A Violation of Trust: Fraud Risk in Nonprofit Organizations

By Jonathan T. Marks, CPA, CFF, CITP, CFE, and Pete A. Ugo, CPA

Resource Type: Articles

Topic: Fraud and Financial Oversight

The risk of fraud is a serious concern for all types of enterprises, but fraud can be particularly damaging to a nonprofit organization, for which a damaged reputation can have devastating consequences.

The Costs of Fraud in Nonprofit Organizations

According to the most recent global fraud study by the Association of Certified Fraud Examiners (ACFE), the typical organization loses an estimated 5 percent of its annual revenue to fraud. While fraud in nonprofit organizations resulted, on average, in a smaller net loss than fraud in commercial enterprises, the nonprofits in the study reported a median loss of $100,000—an 11 percent increase from the previous study and a significant loss to any charitable organization.

Beyond the immediate financial loss, however, an even greater potential cost of fraud to nonprofit organizations is the reputational damage that can occur. Because most nonprofits depend on support from donors, grantors, or other public sources, their reputations are among their most valued assets. In addition, fraud in nonprofit settings often garners unrelenting negative media attention.

Vulnerability to Fraud

Nonprofits can be particularly attractive targets for fraudsters. Executives who are passionate about their agencies and their missions are naturally trusting of others who share their interest- or who pretend to. Moreover, board members and executives who are dedicated and talented in their particular fields may not be well versed in financial issues and internal controls.

In addition, nonprofits of all sizes may have only limited resources available to address internal controls. This makes them vulnerable to an employee who could recognize this lack of controls and use it as an opportunity to commit fraud.

As the Center for Audit Quality has noted, “fraud cannot occur unless an opportunity is present. Opportunity has two aspects: the inherent susceptibility of the [organization’s] accounting to manipulation, and the conditions within the [organization] that may allow a fraud to occur.” In addition, the opportunity for fraud is also affected

by an organization’s culture, a factor that is often overlooked.

The very nature of some nonprofits also makes them tempting targets. Many nonprofits distribute grants, scholarships, awards, or other types of financial aid to outside agencies or individual recipients. This opens yet another door for potential abuse or misappropriation and requires even more oversight to make sure funds are not being misappropriated. In addition, nonprofits tend to have large amounts of cash and checks coming in from various sources, making them vulnerable to skimming (when an employee accepts payment from an outside party but does not record the sale and instead pockets the money) or cash larceny (when an employee steals cash and checks from daily receipts before they are deposited in the bank).

Struggling agencies also frequently experience relatively high staff turnover, making training and adequate segregation of duties more difficult. Finally, many nonprofits depend heavily on volunteers and other community members, which can further complicate efforts to establish or maintain internal controls. It is important to remember that internal controls provide only reasonable—not absolute—assurance that the objectives of an organization will be met. As a result, no organization, even one with the strongest internal controls, is immune to fraud.

How Fraud Occurs and Why

While nonprofit organizations present particular temptations to fraudsters, the actual fraud schemes they might face are common to all types of organizations. Fraud schemes in nonprofits can include check fraud, embezzlement, ghost employees, expense fraud, misappropriation of funds for personal use, fictitious vendor schemes, kickbacks from unscrupulous vendors, and outright theft of cash or assets—to name a few.

One area in which nonprofit organizations seem particularly vulnerable is billing schemes, in which an employee fraudulently submits invoices to obtain payments he or she is not entitled to receive. According to the most recent ACFE survey, billing schemes were among the most common fraud methods in the cases studied for the 2012 report.

Billing schemes often involve the creation of a shell company. In such a fraud, a dishonest employee sets up a fake identity that bills for good or services the organization does not receive. In some instances, goods or services may be delivered but are marked up excessively, with the proceeds diverted to the employee.

Other scams include pay-and-return schemes that cause overpayments to legitimate vendors. When an overpayment is returned, it is embezzled by the employee. Another favorite is simply ordering personal merchandise that is inappropriately charged to the organization.

Common warning signals or red flags of potential billing fraud include but are not limited to:

- Invoices for unspecified or poorly defined services
- Unfamiliar vendors
- Vendors that have only a post-office-box address
- Vendors with company names consisting only of initials (many such companies are legitimate, of course, but fraudsters commonly use this naming convention)
- Sudden increases in purchases from one vendor
- Vendor billings issued more often than once a month
- Vendor addresses that match employee addresses
- Large billings that are broken into multiple smaller invoices that will not attract attention
- Internal control deficiencies such as allowing a person who processes payments to approve new vendors

These warnings or red flags can be organized into four general categories:

Data

- Transactions conducted at unusual times of day, on weekends or holidays, or during a season when such transactions normally do not occur
- Transactions that occur more frequently than expected — or not frequently enough
- Accounts with many large, round numbers or transactions that are unusually large or small
- Transactions with questionable parties, including related parties or unrecognized vendors

Documents

- Missing or altered documents
- Evidence of backdated documents
- Missing or unavailable originals
- Documents that conflict with one another
- Questionable or missing signatures

Lack of Controls

- Unwillingness to remediate gaps
- Poor “tone from the top”
- Inconsistent or nonexistent monitoring controls
- Inadequate segregation of duties
- Lax rules regarding transaction authorization
- Failure to reconcile accounts in a timely manner

Behavior

- Financial difficulties or generally living beyond one’s means
- Divorce, family problems, or addiction problems
- Past employment-related or legal problems
- An unusually close association with vendors or recipients of grants or services
- Control issues and a general unwillingness to share duties
- Refusal to take vacations
- Irritability or defensiveness
- Complaints about inadequate pay
- Complaints about lack of autonomy or authority

It is also worth noting that fraud is not about obstruction; rather, it is about deception, deflection, and persuasion. When fraudsters or white-collar criminals are profiled, they often are found to be anxious, secretive, moody, hot-tempered, friendly, outgoing, and passionate. They often are good salespeople and will say what people want to hear in order to build rapport and gain trust. Moreover, often there are other warning signs or red flags hidden in plain sight…such as living beyond one’s means, having financial difficulties, maintaining an unusually close association with vendors, or exhibiting excessive control issues, which generally will not be identified by traditional internal controls. It is important to maintain a healthy level of skepticism and always remember that trust is a professional hazard; if you do not verify information, you could become a victim.

Implementing Controls

As with all risk issues, the ultimate responsibility for identifying gaps and developing fraud controls rests with management. To meet this responsibility, management should avoid complacency and not assume that if fraud occurs “the auditors will catch it.” Although having an annual audit is a good anti-fraud control, by the time an audit uncovers a fraud scheme, it is usually too late to prevent the financial and reputational damage that will follow.

Most board members and executives of nonprofits do not think as fraudsters do, which is a good thing. Unfortunately, this can make it difficult for them to develop controls that help reduce their organizations’ exposure to fraud risk. A critical step in the process of developing an effective fraud risk management program is assessing the board’s own skills and capabilities and deciding where professional help is most needed. The board is ultimately responsible for oversight of the organization’s risk management efforts, which senior management is then charged with carrying out.

Anti-Fraud Principles

Here are some important principles to keep in mind as you work to refine the anti-fraud control policies at your nonprofit:

- Form an effective and empowered audit committee or equivalent. One of the most important attributes of

the audit committee is complete independence from management. In addition, the committee should be authorized to hire outside counsel and other advisers to assist it in discharging its responsibilities. Although your circumstances may warrant a larger committee, a committee of three to five members is generally workable and optimal for most nonprofits. At least one audit committee member should be a financial expert, but individuals with nonfinancial skills and expertise are also needed to provide additional perspective.

- Establish and enforce a system of effective controls. Combinations of internal and cultural controls form the core of an anti-fraud program. Internal controls limit opportunities to hide the fraud trail and can discourage all but the most arrogant fraudsters. Common tools include security and access controls, such as dual authority or monetary authorization limits, as well as audits, inspections, and transaction monitoring. The recent ACFE survey pointed out that the presence of anti-fraud controls is notably correlated with significant decreases in the cost and duration of occupational fraud schemes.
- Establish the right tone from the top. Mere mechanical compliance with internal controls can still leave the organization vulnerable, which is why the attitude and actions of management are so important. Actively and visibly promoting a culture of integrity and ethics will embolden honest employees to put a stop to fraud. Most organizations find that a strong ethical environment encourages self-policing, thereby increasing the level of oversight far beyond what internal control methods alone provide.
- Provide a clear process for reporting suspicious behavior. Over the years in which the ACFE has been conducting its global fraud studies, the most effective means of detecting fraud has always been tips. In the most recent study, tips were responsible for uncovering nearly three times as many frauds as any other form of detection such as management reviews, surprise inspections, audits, or surveillance devices. While some nonprofits use a third-party hotline service for reporting suspicions about fraud, creating a culture where employees know that the nonprofit's reputation and mission depend on their willingness to report suspicions of fraud is less costly and may be equally effective.
- Develop a response plan in case deterrence fails. In spite of everyone's best efforts, fraud still can occur. In many cases, the initial reaction of executives or board members is to confront the suspected fraudster outright or, if there is doubt, to begin collecting paper or electronic evidence. All too often, these are exactly the wrong things to do and could compromise an organization's ability to prosecute. Confronting a suspected fraudster without adequate evidence is not only awkward and legally dangerous; it can also alert the suspect to cover his or her tracks. On the other hand, surreptitiously examining computer links and email archives could compromise the evidence and imperil the integrity of a formal investigation, making conviction and recovery more difficult. To avoid these various unintended consequences, nonprofit organizations should develop appropriate strategies in advance to deal with specific types of fraud or other misconduct. The protocol for dealing with an employee suspected of cheating on an expense report is different from that for an executive involved in a conflict of interest.
- Confront the issue openly and directly. Perhaps the most common impulse when fraud is detected is to dismiss the offender, limit the damage, and hope the story can be kept quiet. This too is likely to fail. Eventually, word of the fraud gets out and the associated rumors are likely to be exaggerated, causing even more reputational damage than would have been done if the board had simply been forthright.

A Combination of Deterrence and Detection

As important as it is to respond quickly to fraud, avoiding the situation in the first place is the best plan of all. Although it is unrealistic to expect to completely eliminate the risk of fraud, the governing board and executives in a nonprofit organization can take effective steps to minimize the risk.

By establishing an environment in which ethical behavior is expected, closing gaps in internal controls, and developing a proactive fraud identification and response program, nonprofits can significantly reduce the financial and reputational risks associated with fraud.

This article was excerpted from an article published by Crowe Horwath in August 2012.

Jonathan Marks is a partner and leader of Fraud, Ethics, and Anti-Corruption Services with Crowe Horwath LLP in the New York office. He can be reached at 212.572.5576 or jonathan.marks@crowehorwath.com. Pete Ugo is a partner with Crowe in the Indianapolis office. He can be reached at 317.208.2509 or pete.ugo@crowehorwath.com.