Five steps to help reduce fraud in not-for-profit organizations

Prepared by:

Patrick Chylinski, *Director*, McGladrey LLP
213.330.4605, patrick.chylinski@mcgladrey.com

When many people think about fraud, their thoughts usually turn to banks, investment firms and large businesses. But don't be fooled. Not-for-profit organizations – including many charities, colleges, religious entities and trade groups – are often easy targets for sophisticated fraud schemes.

In its 2012 Report to the Nation, the Association of Certified Fraud Examiners (ACFE) said that frauds occurring in not-for-profit operations make up about 10 percent of all reported cases. While that's well behind the 28 percent of frauds reported to law enforcement from public companies, the median losses are relatively close ($127,000 for public companies, $100,000 for not-for-profit entities). However, that impact of fraud losses is often far greater on charitable and service organizations because many of these entities do not have strong cash reserves to cover unexpected shortfalls.

Unfortunately, a typical fraudster is not always easy to spot. The ACFE notes that most employees or others who commit fraudulent acts are first-time offenders, meaning that normal background checks often won't flag a potential threat. However, the ACFE reports that 77 percent of all frauds are committed by people working in one of six business units: accounting, customer service, executive management, operations, purchasing and sales. Fraudsters with longer time on-the-job typically cause greater losses, as do higher-ranking perpetrators.

Where does fraud occur in a not-for profit environment? According to Report to the Nation, billing scams are the most frequent crime (52 percent of reported cases), followed by check tampering (33 percent) and fictitious expense reimbursement schemes (31.5 percent). All of these acts are considered an on-the-books asset misappropriation fraud, because they involve illegal transactions that are ultimately recorded in financial records. For example, an employee may create a fake vendor account, which bills the not-for-profit firm for products or services never received. Or, an employee on a business trip chooses to add personal travel activities onto an expense reimbursement report filed with the not-for-profit entity. These schemes are popular among fraudsters, because the individual does not have to physically take cash or merchandise in order to receive an economic benefit.

Key vulnerabilities

While large not-for-profit entities can operate much like their for-profit cousins, there are a handful of distinctions that may open the door to opportunistic fraudsters. These include:

Trust - More than most conventional businesses, not-for-profit organizations can confer a higher level of trust in executive leaders and founders. However, blind trust in such individuals can allow for management override of control systems, which the ACFE says is the most important contributing factor in nearly 20 percent of all reported fraud cases. In a recent research paper, Management Override of Internal Controls: The Achilles' Heel Of Fraud Prevention, the American Institute of Certified Public Accountants (AICPA) defines the threat as follows:

Management may override controls to intentionally misstate the nature and timing of revenue or other transactions by:

- Recording fictitious business events or transactions or changing the timing of legitimate transactions, particularly those recorded close to the end of an accounting period;
- Establishing or reversing reserves to manipulate results, including intentionally biasing assumptions and judgments used to estimate account balances, and
- Altering records and terms related to significant or unusual transactions.

Oversight - This may be the area where not-for-profit groups are most open to attack. For example, many small and midsized not-for-profits have volunteer boards of directors, many of whom may not have the skills, training or time to provide adequate financial oversight. From an operational viewpoint, lean not-for-profit budgets often translate to fewer workers juggling more jobs. As a result, key functions like finance, bookkeeping, and accounting are often concentrated with a few individuals, making segregation of duties a more challenging task.

Volunteer - Not-for-profit groups often thrive on the strength of volunteers. While the vast majority of these people are honest and committed to an organization's mission and values, a small percentage can use their inside access to pursue illicit activity. For example, the nature of many non-financial charitable contributions – such as vehicles, boats, or household goods – can provide easy pickings for fraudsters who wish to steal, mismanage or use such assets for non-intended purposes.

Five steps to help identify and minimize fraudulent activity

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a framework for effective internal controls. The framework features five interrelated components, which include:

Control environment

As a general rule, not-for-profit boards and senior leadership can help reduce potential fraud activity by setting clear ethical boundaries and demonstrating consequences for behavior outside of those areas. This big picture of what is – and is not – acceptable in the organization's culture should also be emphasized in all vision, values and mission statements.

Risk assessment

If the control environment is the heart of a fraud prevention approach, the risk assessment is the brains. This review should begin with a candid discussion of existing antifraud programs and controls, followed by an evaluation of potential internal and external fraud risks. A sound assessment should also rate the likelihood of various fraud risk scenarios and consider how each potential occurrence could affect an organization's reputation with key stakeholders. Ideally, the assessment should be conducted annually, since organizational priorities, leaders, employees, vendors and other stakeholders regularly change.

Control activities

As defined by COSO, control activities are policies and procedures that help ensure that management directives are carried out. In an AICPA forensic accounting brief titled, Internal Controls and Fraudproofing, control activities are defined at both the basic and supervisory levels. Basic controls include limiting physical access to valuable assets or sensitive information, creating (and enforcing) specific job descriptions that reinforce segregation of duties and performing regular reconciliations of bank accounts, accounts receivable and accounts payable. At the next level, the AICPA suggests that supervisors and leaders take time to review and spot check the validity of accounting and financial documents submitted for approval.

Information and communication

In the larger sense, this step helps ensure that all steps taken to control fraud are clearly communicated to employees, customers and other stakeholders. A well-designed communications system can reinforce a strong tone at the top and provide specific avenues through which internal and external parties can address or report fraud. These avenues may include management and employee training programs to spot fraud, tip hotlines and whistleblower rewards. At the same time, communications systems must be created to identify, capture and relay regular information to key leaders about the success of antifraud controls.

Monitoring

While common sense suggests that all control activities need to be monitored, no two organizations handle that task in the same fashion. If a not-for-profit entity's risk assessment calls for several new control activities, frequent success evaluations are warranted. On the other hand, an organization making little or no changes to internal antifraud efforts may simply maintain a regular monitoring schedule to assess if tools are working properly.

800.274.3978
www.mcgladrey.com