PROTECTING ★ THE ★ UNPROTECTED

Avoiding Theft

Protecting the Integrity of Your Nonprofit

Ohio Attorney General Dave Yost's office works to ensure that donations are used as they are intended. Learn strategies to prevent theft or misappropriation in your nonprofit organization.

DAVE YOST
OHIO ATTORNEY GENERAL

Dear Nonprofit Leader,

The public's trust is pivotal to the mission of a nonprofit. Although such organizations provide a diverse range of services to Ohioans, the public frequently thinks of "nonprofits" as a giant entity. When the reputation of one nonprofit suffers, so do those of the rest. We are here to help you avoid pitfalls.

The Charitable Law Section of the Ohio Attorney General's Office is committed to honoring the important role of nonprofits throughout the state. Oversight is critical: One of the section's most important tasks is to make sure that funds are used for charitable purposes, not misdirected to private interests. This duty, rooted in common law and reinforced through many statutory provisions, is one of the attorney general's oldest responsibilities.

This Avoiding Theft guide can help you establish provisions to prevent embezzlement or misappropriation within your organization or guide you in evaluating the safety net already in place. If you become aware of questionable actions, please contact my office. We will investigate suspected fraud, theft or other activities that diminish or threaten the valuable work of nonprofits.

When nonprofit leaders like you step up to do good things the right way, our communities grow stronger. I thank you for making the effort.

Very respectfully yours,

Dave Yost
Ohio Attorney General

RECOGNIZING THE POTENTIAL FOR PROBLEMS

Charities rely on the good-faith efforts of invaluable volunteers and, in some cases, paid staff members. Most people are honest and committed, but even longtime volunteers can find themselves in situations that tempt them to steal from the organization.

Theft happens in large and small organizations alike, and it often involves individuals who are widely respected and valued within the nonprofit. Such transgressions might happen during a period of financial hardship for the individual, or out of spite, for revenge or because of addiction issues. Other times, the only explanation is greed.

Regardless, one truth is well-known: The No. 1 contributing factor to theft is access to assets.

Unfortunately, well-meaning organizations — and, ultimately, those they serve — suffer from such incidents. The Association of Certified Fraud Examiners reports that a typical organization loses 7 percent of its annual revenue to fraudulent activity. Applied to the $410 billion that Americans donated to charities in 2017, that rate translates to $28.7 billion in potential losses.

DEVELOPING ANTITHEFT PROCEDURES

The adoption and regular review of written policies help protect the organization, board members, staff members and volunteers. All should find the development of such procedures a comfort, not a threat.

It is important to keep the focus on the processes, not the people. Nonprofits should implement and/or examine their procedures without considering the trustworthiness of the specific individuals involved. The procedures should be based on objective standards about how best to protect the organization's interests.

Although it is impossible to guarantee the prevention of theft, nonprofits should take steps to reduce the likelihood of problems and ensure a quick response if problems do arise. Some charitable boards rely solely on an annual audit to safeguard the organization from fraud. In truth, though, an audit's primary goal is to ensure that financial statements provide an accurate fiscal picture, so audits rarely uncover fraud. Fraud is often uncovered through diligent oversight, whistleblowing, an internal audit or sheer luck.

Among the most important duties of board members are developing internal controls, implementing audit processes, and establishing written policies and procedures — and making sure they are being followed. In fact, failure to address these issues can constitute a breach of fiduciary duties and jeopardize the organization's future. Board members who recklessly and intentionally fail to act even risk personal liability.

Lawyers, accountants, business leaders and other community leaders are often willing to provide guidance on the creation of internal controls and board-governance policies. Numerous books, resources and training organizations can also provide assistance. Board members must take the time to analyze the specific needs and goals of the organization and work to constantly improve activities in these areas.

LIMITING EXPOSURE

Nonprofit organizations should consider a range of steps to limit their exposure to theft. Some of these steps center on the importance of the separation of duties so that no one person has sole access to and control over the collecting, depositing and reporting of financial information — the root problem in most instances of theft. Others reinforce the importance of regular and effective oversight by the board or audit committee. The board is responsible for ensuring that an effective system of checks and balances is in place.

An organization's size and complexity should be considered when assessing needs. There is no single fool-proof formula to eliminate theft, but the surest recipe for disaster is to ignore the issue.

Take care with payments

Requiring multiple signatures on checking and investment accounts for checks written above an established amount can provide some measure of control. The approved signatories should be individuals who are independent of each other, so avoid selecting individuals who are family members, close friends or related by supervisory structures. Having blank checks signed in advance for convenience's sake poses a risk. Organizations should also consider using safety checks that cannot easily be scanned or altered. For handwritten checks, gel pens are safer than ink pens. If your organization pays its bills electronically, consider granting online access to the accounts to someone not authorized to pay bills.

Reconcile bank statements

Someone who is not authorized to sign checks should reconcile all bank statements monthly. Each check should be compared against appropriate purchase orders and receipts to verify that the expenditures were authorized and the goods or services received. Arrangements also could be made to have the bank send multiple bank statements, one to the charity office and one to the home address of the board treasurer. Such a process can reduce the risk of bank-statement tampering to hide fraudulent activities.

Restrict use of cash

Cash is particularly tempting, and the more that organizations can limit the need to handle it, the better. For many charitable organizations, however, this is not possible. Two people should count cash at events, and a third should deposit the money in the bank. Counts should be recorded, verified and reconciled. Ensuring that cash deposits are routinely made – that the money is not just left in the office – is vital. Cash and checks should be safely locked up if not immediately deposited. If the group sells refreshments, for example, consider a ticketing system in which vendors do not handle cash, just tickets – an approach that centralizes the cash-collection process.

Establish check-handling procedures

A common theft scheme in charities involves volunteers or staff members diverting checks made out to the organization into other accounts they have opened personally. Though somewhat-costly, lockbox services — in which donors mail checks to a lockbox at a bank, for example — allow the checks to be automatically processed without going through volunteer or staff hands.

Another important consideration is developing internal systems to monitor and track incoming mail that might contain checks. Checks could be stamped as "Deposit Only" but avoid including bank-account numbers on those stamps. Some individuals who receive canceled checks have been known to fraudulently make use of the bank-account data.

It's also important to set up a segregated system for recording and depositing all checks that are received regularly. Checks should be safely locked away when immediate deposit is not possible.

Work from vendor lists

A ruse used by some insider thieves is to submit phony invoices. To guard against this, organizations should consider making purchases only from an approved list of vendors. Before a vendor can be added to the list, the business should be researched thoroughly to verify its legitimacy. Consider including a "right-to-inquire" clause in the contract so that a vendor's internal records can be inspected when fraud is suspected.

Develop payroll controls

This common scam involves ghost employees. Nonprofits should coordinate human-resource and finance functions to ensure that, when employees leave, they are removed from the payroll. Only the names of current employees should be on a payroll, with limits placed on the number of people authorized to add or eliminate names from the payroll. Outsourcing this function to a payroll processor can help curtail this threat.

Establish expense reimbursement policies

Expense reimbursement is an area ripe for abuse in all organizations, making the need for policies especially vital. Pre-approval of expenses should be encouraged, and reimbursement should require the accompaniment of receipts and other forms of documentation. The issuance and use of corporate credit cards should be discouraged, as they often become a source of problems. If cards are permitted, they should be closely reviewed to ensure legitimacy and documentation by someone not authorized to use them. The board or one of its committees should regularly review the expenses of the executive director.

Match physical and recorded inventories

Many organizations suffer losses in the form of resources, such as equipment or other goods. Physical inventories should be taken regularly and matched against recorded inventories. Such efforts should include computers, cellphones, office equipment and similar items.

Set and follow budgets

All organizations should have an annual budgeting process. Although staff members often prepare the budget, the board must review, approve and monitor it. Often a finance committee of the board is best positioned to do this. Budgets should encompass the entire organization as well as any segments that operate separately. At each board meeting, the board should review revenue and expenses and evaluate actual results compared with the projected budget levels. Some variations can be expected, but the board needs to understand the variations and develop plans to address any that are problematic. Board members should also ensure that funds whose uses are restricted — by grants, for example — are used only for those purposes.

Employ competitive bidding

Board members face serious risks when they fail to exercise a duty of loyalty to the nonprofit. When charitable contracts are routinely sent to specific businesses, including those that board members are involved with, consumers can legitimately question whether decisions are being made to further the personal interests of board members. In fact, conflict-of-interest policies are not only crucial but also can protect board members from possible criminal and civil action. Competitively bidding out services and purchases above a certain threshold can reduce problems. It is also important to ensure that vendors are not engaged in collusion and that insiders are not seeking kickbacks.

Monitor grant administration

Organizations can find themselves in trouble with government and private auditors over the improper use of grant funds and designated charitable gifts, which can be expended only in ways defined by the donor. In the area of grants, there are often specific requirements on allowable and unallowable costs, overhead expenses, procurement and record-keeping. The board should ensure that all such requirements are understood and followed.

Consider background and credit checks

Organizations might want to consider requiring criminal-background and credit checks for staff members and volunteers who are in a position to divert resources from the organization. Too often, groups are victimized by an employee or board member who has engaged in theft at another organization. Through a partnership between the Ohio

Attorney General's Office and the Ohio Bureau of Motor Vehicles, Ohio and FBI background checks are available through many BMV sites throughout the state. You can check locations online at **www.OhioAttorneyGeneral.gov/WebCheck**. Additional information is available through Ohio Attorney General Dave Yost's Help Center at 800-282-0515. Background checks are also available through local law-enforcement agencies.

Require vacations and rotation of duties

Problems sometimes are not uncovered because the embezzler never takes a vacation or other time off, so others are unable to get a full picture of the organization's finances. When vacations, mandatory work breaks and rotation of duties are enforced, problems can be discovered more quickly.

Change passwords, combinations and locks

Volunteers and staff members come and go. Be certain to routinely change passwords on bank and financial accounts and routinely change locks and combinations so that people who leave the organization can no longer access valuable data.

Establish whistleblower policies

Boards should develop a whistleblower policy to make it easy for staff members and volunteers to report concerns about fiscal management.

Consider insurance coverage

Many nonprofits obtain insurance coverage to protect an organization's board, staff members and volunteers from liability. Such coverage does not protect board members who intentionally commit fraud or personally benefit from lax policies. As for insurance, even though it might not prevent theft, insurance carriers sometimes provide customers with ongoing training and tips on strengthening internal controls. And if a loss does occur, the coverage might help the organization restore lost funds.

Assess internal controls

An organization's audit committee should consider doing surprise visits or audits to check how well processes and procedures are being

followed. Checking for required documentation on check requests, testing the cash-management policies and examining payroll records can all be helpful. There should be ongoing discussion and consideration of risk assessments to ensure that any gaps are addressed. The board also should ensure that a document-retention and -destruction policy is in place to protect the group's business records. This could become important should investigations occur later.

Recruit new audit committee members

Organizations can benefit from getting new and fresh perspectives on audit committees. This helps prevent or detect schemes that can extend for many years because no new individuals ever served in an auditing role.

Look for warning signs

The board should be alert for warning signs of possible trouble:

- Concerns or questions expressed by people handling the collection of funds and financial reporting
- Changes in record-keeping methods
- Overall complexity of the operations
- Unwillingness to share financial information with interested parties
- Significant changes in revenue and/or expense levels from previous years
- Problematic audit results
- Complaints
- Bounced checks
- Late or nonexistent financial reports to the board
- Unpaid invoices
- Sudden, unexplained changes in lifestyles of employees or volunteers

Develop a fraud action plan

Boards should consider in advance how they will respond if problems arise. Sometimes the clear pronouncement of a policy favoring criminal prosecution for theft serves as a deterrent.

Avoiding Theft in Your Nonprofit

TRACKING YOUR PROGRESS

Use this checklist to keep track of actions your organization has taken to help avoid embezzlement.

- [ ] Require dual signatures
- [ ] Reconcile bank statements
- [ ] Limit use of cash
- [ ] Establish check-handling procedures
- [ ] Work from vendor lists
- [ ] Develop payroll controls
- [ ] Establish expense reimbursement policies
- [ ] Match physical and recorded inventories
- [ ] Set and follow budgets
- [ ] Employ competitive bidding
- [ ] Monitor grant administration
- [ ] Consider background and credit checks
- [ ] Require vacations and rotation of duties
- [ ] Change passwords, combinations and locks
- [ ] Establish whistleblower policies
- [ ] Consider insurance coverage
- [ ] Assess internal controls
- [ ] Recruit new audit committee members
- [ ] Know the warning signs
- [ ] Develop a fraud action plan

DAVE YOST
OHIO ATTORNEY GENERAL

Charitable Law Section
150 E. Gay St., 23rd Floor
Columbus, OH 43215

For more information on charitable law, please visit **www.OhioAttorneyGeneral.gov** or call **800-282-0515.**