Theft and Embezzlement: A Diligence Checklist

By Sarah E. Mooney and Joan M. Renner

Recent media attention to fraud in the nonprofit community has provided a wake-up call for associations that may need to get better at protecting their assets. For those that have been fleeced and those that want to avoid becoming the next news story, these steps can help shore up critical financial controls.

Late last year, a problem that many in the tax-exempt sector have experienced but that is rarely discussed openly made headlines in *The Washington Post*. A *Post* investigation found that hundreds of nonprofit organizations reported to the IRS that they had experienced theft of their assets.

Investigative journalists at the *Post*, with assistance from Guidestar, analyzed public Form 990 information returns filed with the IRS between 2008 and 2012 and found that more than 1,000 tax-exempt organizations answered "Yes" to a relatively new question: "Did the organization become aware during the year of a significant diversion of the organization's assets?" The *Post* also created an easy-to-search database of organizations reporting asset diversions with a shortcut to the explanation each organization provided.

The 990 instructions state that a "Yes" answer triggers a required explanation on Schedule O, including the nature of the diversion, dollar amounts and other property involved, corrective actions taken, and pertinent circumstances. The instructions note that the person or persons who diverted the assets should not be identified by name.

A "diversion of assets" as defined in the 990 instructions includes any unauthorized conversion or use of the organization's assets other than for the organization's authorized purposes, including embezzlement and theft. A diversion is considered "significant" if the gross value of all diversions discovered during the organization's tax year exceeds 5 percent of the organization's gross receipts for its tax year, 5 percent of its total assets as of the end of its tax year, or $250,000.

The issue is an important one and can pose dire consequences. A diversion of assets to an insider (someone who can exercise substantial influence over the organization's affairs) could be considered inurement of the organization's net earnings and result in revocation of its tax-exempt status. It could also lead to a costly and time-consuming state attorney general investigation or lawsuit. In the case of a 501(c)(3) or 501(c)(4) organization, it could also be an excess benefit transaction subject to significant excise penalties.

Reporting and Investigation

If an organization makes the unfortunate discovery that it has been the victim of fraud or embezzlement, its leaders need to take several important steps. This diligence checklist can serve as a guide.

Inform the board. The board of directors, which has a fiduciary obligation to oversee the organization's finances, should be immediately informed of any credible reports of fraud, theft, or unauthorized use of the organization's assets. If a diversion is reported by an outsider and involves a board member, in many cases the state attorney general may already be involved in an investigation.

Investigate the alleged fraud, theft, or misuse. The board or a committee of the board (typically the audit committee) should convene an investigation, likely with the assistance of law enforcement (the local police, the district attorney's office, or the FBI), forensic accountants (depending on the nature of the fraud), and legal counsel. The board or committee may designate the executive director or chief financial officer to manage the day-to-day investigation and may require periodic reports.

Notify the insurer. Most insurance policies require immediate notification to the carrier upon discovery of a theft or a situation that could result in a loss of money or other property. In addition, a police report may be required for purposes of filing an insurance claim if the organization has special crime coverage or employee dishonesty coverage.

Make reasonable efforts to recover any stolen or misused assets. The organization will need to cooperate with any investigation or criminal prosecution. Depending on the amount of money or property at issue, the organization may want to explore a civil lawsuit to recover the stolen or misused assets.

Disclose the asset diversion on your Form 990 and on a state return if required. Reporting a significant diversion of assts to the IRS is not optional. The agency treats an incomplete return the same as a return filed late, and significant penalties could be imposed. Some states that require charitable organizations to file annual reports may also request diversion information. For example, in California, organizations required to register with the attorney general's office are also required to file Form RRF-1 annually and report any diversions on this form. In New York, organizations are encouraged to report embezzlement to the attorney general's Charities Bureau.

Prevention

As fiduciaries, the board should make sure that adequate financial controls are in place to prevent fraud and theft of the organization's assets. Management should produce timely and accurate income and expense statements, balance sheets, and budget status reports, and board members should ask questions. The board should also work with its outside accountants to evaluate whether tighter internal controls are needed.

One of the most important components of an organization's system of controls against error or fraud is the tone set by leadership. Making adequate internal controls a board priority reduces the risk of loss to embezzlement or fraud. Some boards dismiss internal control procedures as unattainable or inefficient, presuming that organizations should just do the best they can with available resources. This approach can leave the organization open to fraud. All boards are expected to carry out their fiduciary duty, even in situations where resources are limited.

Implementing an annual assessment of controls can help the board fulfill its fiduciary responsibilities. In the assessment, management inspects the organization's transaction processes, identifies any new risks, and updates the organization's controls, enlisting the assistance of outside accountants as needed. Management reports the results to the treasurer or appropriate committee. This assessment should include a review of the organization's procedures in each major financial area, including income, disbursements, payroll, investments, credit cards, and expense reports.

An assessment of controls should do the following:

- Summarize how transactions are carried out in each area.
- Identify weaknesses and risks that could allow embezzlement to occur. Ask: If an individual wanted to embezzle in this area, how would he or she do it? The answers point to your organization's risks.
- Consider how embezzlement could be detected. Ask: If unauthorized transactions happened here, how would we know? The answer points to your new control procedures.

The chart below lists common transaction types and their risks, along with potential controls:

Transaction and Risk	**Control Procedure**
Transaction: online bill paying *Risk:* unauthorized payments	Dual password approval. This system allows one person to prepare online payments but not release them and another to review and release online payments. OR Regular online review of bank transactions by the treasurer or another independent individual who will request documentation for any unapproved items.
Transaction: remote deposit; scanning of incoming paper checks *Risk:* diverted incoming checks	Scanning of incoming checks by an independent individual before checks are distributed to accounting department or to others in the organization.
Transaction: online contributions through the organization's website *Risk:* diverted receipts	Regular comparison, by an independent individual, of a statement of website activity to amounts deposited in the organization's bank account.
Transaction: online payroll with direct deposit of employees' paychecks *Risk:* unauthorized payment dates or amounts	Dual password approval. This system allows one person to prepare paychecks but not release them and another to approve and release paychecks. OR Review by an independent individual of payroll activity accessed directly from the payroll system compared to approved payroll.

Transaction: all accounts payable applications *Risk:* fake vendors	Separate password access, independent of other accounting duties, for setup of new vendors. Log of changes to vendor master file.
Transaction: outgoing wire transfers and electronic payment of credit cards or other bills by Automated Clearing House (ACH) *Risk:* unauthorized transfers out of bank account	Dual authorization for outgoing ACH payments and wire transfers, where one person creates the transfer and a second releases it.
Transaction: refunds of credit card transactions *Risk:* unauthorized refunds to unauthorized credit cards	Password-protected refund function that restricts the ability to issue refunds; independent review of credit card refunds debited to the organization's checking account verifying that the credit card receiving the refund is the same card that was used to make the sale. Some payment gateways offer credit card and refund fraud protection.
Transaction: fraudulent attempts by outsiders to draw on association's bank account *Risk:* unauthorized checks or bank withdrawals	Fraud protection services offered by your bank, such as Positive Pay check verification and ACH verification filters.

The procedures appropriate for any individual organization will depend on its specific facts and circumstances. Regardless of the details, by assessing internal controls and updating the assessment annually, management can take advantage of new efficiencies and modify the organization's controls as needed over time to keep assets safe.

Sarah E. Mooney is a partner with the law firm Webster, Chamberlain & Bean, LLP, in Washington, DC. Email: smooney@wc-b.com. Joan M. Renner is a CPA with Renner & Company in Alexandria, Virginia. Email: joanrenner@rennercpa.com.

* * *