Best Practices with Practiceminders

by BOOKMINDERS®

The official newsletter of Practiceminders

This issue's feature:

Fortifying Nonprofit Clients: Practiceminders' Guide to Combat Theft and Fraud

Fortifying Nonprofit Clients: Practiceminders' Guide to Combat Theft and Fraud

In recent years, reports of financial abuses within nonprofit organizations have underscored the critical importance of robust fraud prevention measures. In October of 2023, a former senior fiscal officer at a Brooklyn-based nonprofit, Company-1, was accused of embezzling more than $2.3 million through falsified invoicing. In 2022, the former Executive Director and a Project Manager of Chicago-based nonprofit, Center for Community Academic Success Partnerships, were charged with misappropriating $1.8 million largely through checks written to a fraudulent vendor the pair controlled.

“With approximately $40-50 billion lost to nonprofit fraud annually, it's imperative that organizations remain attentive in safeguarding their financial integrity.”

The embezzlement scandals at Company-1 and the Center for Community Academic Success Partnerships serve as stark reminders of the theft and fraud risks facing nonprofits today. With approximately $40-50 billion lost to nonprofit fraud annually, it's imperative that organizations remain attentive in safeguarding their financial integrity.

The costs of fraud go beyond the potential monetary losses; permanent loss of organizational reputation and goodwill threaten to undermine the public trust in nonprofits as entities worthy of support. Given the risks, your nonprofit clients must be increasingly vigilant about the status of their financial controls and security measures. As experienced consultants to firms across the accounting industry, the Practiceminders team understands the challenges nonprofits face and is committed to providing guidance and support to mitigate the risks of theft and fraud.

Help Clients Understand the Risks and Implement Solutions

Fraud can occur any time assets are managed without a system of “checks and balances”. Many nonprofits operate with minimal overhead, causing overlap of duties and resulting in weakened controls. As organizations grow in size and complexity, more sophisticated systems are required to address the increasing variety and volume of financial transactions.

While it’s not feasible to eliminate the possibility of fraud, there are ways for organizations to minimize their exposure. Guiding your client through implementing the following procedures will aid in establishing an environment where tight fiscal controls are the norm:

1. **Do not delegate e-bill approval or check signing responsibility.** Top management is responsible for the finances and should always retain authority for approving payments. Signature stamps are problematic by nature and should be prohibited.
2. **Implement electronic safeguards.** Make sure clients aren’t unintentionally giving check signing privileges to those who aren’t authorized. Employees with debit cards and electronic access to transfer funds essentially have the same authority as a check signer.
3. **Use Third Party Payable Platforms.** Paying bills through Third Party Payable Platforms, like Bill.com, protects the client’s checking account information from being transmitted through the mail and reduces the of payment alteration. A system reliant on handwritten checks is more vulnerable to document manipulation and misuse.
4. **Protect Physical Check stock.** Clients should refrain from maintaining a supply of blank check stock, or if unavoidable, require it be kept in a locked cabinet/safe. Payments made by check stock should require signature from two or more individuals.
5. **When appropriate, let vendors draft routine payments.** Allowing certain companies to

(continued on next page)

5. (cont.) automatically withdraw their payments is the most efficient way to pay a bill, while also eliminating the chance that your client's bank account and routing number will fall into the wrong hands.
6. **Use two people when processing payments by mail.** If the organization receives cash, check or credit card payments, these duties need to be separated and handled by at least two staff members.
7. **Always give customers a receipt for point-of-sale (POS) transactions.** Since cash registers are most often operated by one person, the receipt serves to verify proper posting of sales. If receipts can't be printed, then have the client ensure the display on the cash register faces the customer so the sale can be verified.
8. **Outsource or automate customer payments.** A variety of services allow donors and members to make payments by credit card via the web or mobile device. Encourage the client to use a bank lock box if they can't establish separation of duties for payments received by mail. If possible, eliminate all cash and check payments for small transactions.
9. **Monitor revenue.** Membership, donor management, and POS systems provide reports to help identify irregularities. Coach clients to acquire familiarity with key revenue metrics and review these regularly.
10. **Know the numbers.** Clients who have a firm grasp of their financial results are rarely subject to malfeasance. When a client's management is hands-off, the organization is much more vulnerable to on-going theft.
11. **Encourage Communication.** Statistically, fraud is most often discovered as the result of a tip. Your client must foster a culture where all stakeholders are encouraged to keep a watchful eye. It is imperative that everyone understands their respective stake in protecting an organizations' assets.

It's important to help clients understand that financial statement audits are not intended to detect fraud but instead, to validate the accuracy of the financial statements. Although fraud may be discovered during an annual audit, that alone is not an effective measure for prevention.

Relying on outside vendors' vigilance is another common error in many nonprofit client's fraud prevention planning. A misperception exists that banks closely monitor checking accounts. Banks may catch the occasional unauthorized, forged, or missing signature(s), but help your clients understand that this is not a reliable method for preventing fraud. Conducting random reviews of bank account activity is the best way to deter felonious activity.

These basic precautions can help you protect your nonprofit clients from financial losses and perhaps permanent destruction of their organization's credibility. Finally, if you or your client are still concerned about their degree of vulnerability, encourage them to seek an independent review.

Want to learn more? Download this and other reference guides online at bookminders.com/the-practiceminder.