Hi, . Here are your Articles for December 26, 2013.

Prevent Fraud by Envisioning How it Could Occur at Your Organization

Every year, millions of dollars are donated to not-for-profit organizations. As one case illustrates (see right-hand box), the money that is supposed to go to an organization's causes can be diverted to thieves. Not-for-profits are not immune to the threat of fraud from their own employees.

Preventing internal fraud within a not-for-profit organization requires many of the same approaches that for-profit companies employ but there are several unique issues.

Here is a list of eight best practices to consider:

1. Follow the money. To prevent fraud, you must first envision how it could happen in your organization. Take a look at the donation process through the eyes of an employee that is intent on embezzling funds. Where are the points of weakness? Are your organization's policies or procedures strong enough to prevent fraud? In some not-for-profit fraud cases, only one employee is responsible for opening the mail and processing donations. To prevent similar frauds, consider the following approach to opening mail that includes donation checks:

- *Assign two employees to the process.* The first employee should open the mail; the second employee should log the amount of the donation. Both employees should sign off on the log once all of the mail has been opened.
- *Open mail in a common area,* not at an employee's desk. Unopened mail should be delivered to one container, opened, logged, and placed in a second container.
- *Have a third employee or manager who is not involved in the mail opening process* retrieve the deposits placed in the second basket, review the log prepared during the process, verify that all donations are accounted for and prepare the bank deposit.
- *Make bank deposits on a daily ba*sis to prevent theft of checks from within the office. While waiting to be deposited, checks should be placed in a safe that requires two unique access codes to open.

Employee Steals Donations in Wire Fraud Case

A 48-year-old Baltimore woman was sentenced to 46 months in prison in 2011 for wire fraud in connection with a scheme to steal more than $375,000 in donations from her not-for-profit employer, according to the U.S. Justice Department.

Dorothy Shields Talbot worked for the United Way of Central Maryland, a non-profit charitable organization located in Baltimore. The organization received charitable donations and disbursed funds as directed by donors to support charities in the area.

For just over a 10-year period, Talbot worked in United Way's finance department and was responsible for opening the mail and depositing donations into a corporate operating bank account.

According to the plea agreement and other court documents, in 2003 or 2004, Talbot was granted signatory authority over a separate account maintained by United Way's Employee Activities Committee, to handle the employee event funds. After a meeting, the committee met and decided to close their account. According to the minutes of that

- *Ensure that a manager level employee reviews the logs,* bank deposit information and entries made in the organizations financial records for accuracy.

2. Force employees to take time off. Most embezzlement schemes require that the perpetrator performs regular maintenance to ensure that the theft remains hidden from co-workers and management.

Employees who refuse to use their allotted vacation may be overly dedicated or prefer work to home but they also may be committing fraud. If you see employees who are obviously sick yet refuse to take time off, there may be cause for concern. Not only will sick employees potentially infect others, they may also be working to ensure that their schemes remain hidden. It is impossible to determine an overly dedicated staff member from an embezzler without further investigation. To simplify matters, require that *all* employees, regardless of function, use their vacation allotment and when appropriate, their sick time.

meeting, Talbot was responsible for closing the account. Instead of closing it, she admitted that from December 2004 through December 2010, she deposited donor checks issued to United Way into that account, rather than into the corporate operating account.

Talbot changed the mailing address for the employee activities checking account from United Way's office to her home. She withdrew $375,232 of the monies deposited into the checking account, through ATM withdrawals, debits and by writing checks to herself and others. Talbot admitted that she used the $375,232 for her own personal benefit, including luxury items for her family.

If your organization has concerns that an employee may be committing fraud, use the time while that employee is on vacation to conduct a review of their work. Make sure that you have a suitably qualified fraud investigator involved to ensure that the investigation complies with your organization's policies -- as well as the law.

3. Engage your donors. From time to time, contact donors to verify how much money they have donated during the year. If your organization uses an accountant to produce financial statements, the verification of donations can be included in that process. If a donor disagrees with the amount of the donations shown in your organization's records, it may be an indication of inaccurate accounting or worse. In either event, discrepancies should be investigated to determine the reasons for differences.

4. Employ data analytics. It is helpful to monitor the amount and frequency of donor contributions over time. Pay particular attention to donors who contribute on a monthly basis and suddenly cease doing so. If the number of checks or the amount of donations changes drastically over the course of a quarter or six-month period, consider contacting the donor to confirm the amounts donated to date.

5. Minimize employee intervention. The theft of donations is relatively easy to complete when employees are directly involved in processing physical checks. If you don't already do so, consider encouraging more donations online. There are a number of cost effective solutions designed specifically for not-for-profits. As an added bonus, the reporting of donations received is less labor intensive than processing donations manually, and normally more accurate.

6. Don't have a culture of too much trust. The spirit with which many not-for-profits operate can produce a culture that erroneously assumes employees and volunteers would never commit fraud. You should apply the same rigor to preventing fraud as for-profit companies.

7. Make sure you know where money is located. It is not unusual for organizations to lose track of how many bank accounts they have. Make sure there is a centralized list of accounts, their purpose, the signatories, and the name of the account officer at the bank. All bank accounts should be reconciled at least every two days to prevent fraud and bank errors from slipping through the cracks. Also, ensure that the bank statements are mailed to your organization's offices and not an employee's home. Leave explicit instructions

with your bank that the mailing address for each bank statement cannot be changed from your office address.

8. Don't go it alone. Periodically, your board should commission reviews of the organization's anti-fraud program. A targeted review of your efforts not only ensures that potential gaps are uncovered, it also shows employees that your organization is serious about preventing fraud. It raises the workplace "perception of detection" that if employees decide to commit fraud, they'll be quickly caught.

2344 Perimeter Park Drive Suite 100 Atlanta, GA 30341