Fraud in Non-Profit Organizations: What You Need to Know NOW!

Reports of fraud in today’s world of finance are in no short supply. It seems almost daily we read about a newly defrauded organization which suffered significant financial losses due to a rogue employee’s dishonest actions. Unfortunately, non-profit organizations are not exempt from this disturbing trend. According to a global fraud study conducted by the Association of Certified Fraud Examiners, 10.8% of fraud cases investigated between January 2012 and December 2013 involved not-for-profit organizations who reported instances of fraud with median losses landing around $108,000. For many not-for-profit organizations, those kind of losses can mean the difference between thriving and floundering.

Understanding Fraud

So what is fraud? The ACFE defines fraud as “The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets”. While siphoning cash is the primary goal of most fraudsters, it is not the only fraud target. Non-financial assets are also subject to abuse.

One of the tools most frequently utilized by fraud experts is the Fraud Triangle, which illustrates the three main underlying themes generally present in a fraud case: perceived opportunity, perceived pressure, and rationalization.
Perceived Opportunity – This is the area of the fraud triangle where organizations have the most control. Opportunity allows for the ability to commit fraud. Most opportunities are seized through weak internal controls, poor management oversight, and/or through use of one’s position and authority. Limiting the opportunity for fraud to occur is a key method an organization can use to reduce its fraud risk.

Perceived Pressure – This is what drives a person to commit fraud. Most of the time, pressure results from significant personal financial needs. However, there are some situations where the pressure to commit fraud comes simply from an excessive level of greed on the part of the fraudster. While an organization doesn’t necessarily have a lot of control over this area, being aware of the pressures that may exist will help to identify the red flags that indicate the possibility of fraud.

Rationalization – Most people have a hard time going against the societal norms of decency and trust. In order to perpetuate fraud, most individuals with intact moral standards will feel the need to create excuses for their behavior. Some common rationalizations for committing fraud are:
- I was only “borrowing” the money and planned to repay it.
- The company won’t even realize this amount is gone; it’s not that much.
- My boss does it all the time.
- I’ve been working with the company for 15 years. They owe it to me.
- I’ll stop once I pay off my debts.
- I deserved this after the way the company has treated me.

Rationalization can be reduced by promoting a strong sense of ethical behavior amongst employees and by creating a positive work environment.

Understanding these three elements of the Fraud Triangle will provide a better understanding of fraud, which will in turn increase your chances of identifying the fraud risks that exist within your organization. Identifying the risks will allow you to outline a roadmap you can use to implement stronger preventative procedures.

Common Non-Profit Frauds

There are many different types of fraud that can occur within any organization. The three most prevalent in non-profit organizations include billing schemes, check tampering schemes, and expense reimbursement schemes. The objective of all of these schemes - and the majority of other fraudulent disbursement schemes - is the same: how to get money out of the organization. However, in addition to fraudulent disbursement schemes, non-profits are uniquely susceptible to fraudulent donations. Limiting the opportunities for each of these frauds to exist is the best way to prevent them from happening.

Fraudulent Donations can exist in a variety of forms. One that is relatively new is the work of hackers and the dangers of stolen identities and credit card information. Thieves who purchase stolen information frequently use non-profits and their online donation function as a medium for processing a large amount of credit card information for the sole purpose of determining if the credit cards are still active. The scheme includes processing a donation on the stolen credit card for small dollar amounts, usually around $2 - $3. If the charge goes through, the thief will use the active card to make larger purchases.

The application of a “Captcha” to the online donation process is designed to help deter this type of fraud. In addition, non-profits must perform sufficient due diligence when accepting contingent donations, certain restricted donations, and the source of significant high dollar donations. A donation acceptance policy will help establish a framework which an organization can use in the donation acceptance process. An example of a donation acceptance policy is included as Exhibit A.

Billing Schemes are a type of fraudulent disbursement scheme which allows a perpetrator to steal funds without actually handling cash or checks while at work. This type of scheme is a popular form of fraud because it offers the prospect of large rewards. There are three main categories of billing schemes: invoicing via shell companies, invoicing via non-accomplice vendors, and personal purchases with company funds.
• **Invoicing via shell companies** – this scheme involves a fictitious entity that may be nothing more than a fabricated name and a post office box. Once the shell company is formed, the corrupt employee begins billing the employer. Creating invoices is not too difficult, especially with today’s technology. The most difficult part in this invoicing fraud is getting the fraudulent invoice approved. In most fraud schemes of this type, the fraudster is in a position of authority to approve the fraudulent invoice. It is for this reason that the separation of preparation and approval of invoices is important.

• **Invoicing via non-accomplice vendors** – this scheme involves the use of invoices of legitimate third-party vendors without their knowledge or participation in the fraud. Also known as a “pay and return” scheme, this type of fraud can be perpetrated in different ways. One way is to purposely double-pay an invoice, then call the vendor and request that one of the checks be returned (usually to the attention of the fraudster). Another way is to intentionally pay the wrong vendor. For example, an employee will send Vendor A’s check to Vendor B. After the checks are mailed, the employee calls the vendors to explain the “mistake” and requests that they return the checks to his or her attention. When the checks arrive, the employee converts them and keeps the money. To ensure that the vendors eventually get paid, the employee will usually run the invoices through the accounts payable system a second time. Similar to invoicing via shell companies, this fraud is most easily committed by an employee with approval authority. Again, in order to prevent this type of fraud, it is important that preparation and approval of invoices is separated.

• **Personal purchases with company funds** – instead of running false invoices through the accounts payable, this scheme is most easily committed by making purchases on company credit cards or on running accounts with vendors. Unlike invoicing schemes, this scheme does not require prior approval as the approval is granted with the issuance of the card. Review of the credit card statement by somebody other than the card user may detect fraudulent purchases. It is also highly recommended to implement a check card and credit card use policy that clearly defines the rules and procedures governing the check card and credit card. Example policies are included as Exhibits B and C.

**Check Tampering Schemes** are fundamentally different from billing schemes in that the corrupt employee takes physical control of a check and makes it payable to himself or herself through one of several methods. Most check tampering crimes fall into one of four categories: forged maker schemes, forged endorsement schemes, altered payee schemes, and authorized maker schemes. Regardless of the type of check tampering, concealment is one of the most important parts in making the fraud a success. Therefore, it is highly advisable to separate the check writing function from the approval and signing functions and the bank reconciliation function from the reconciliation review function.

• **Forged maker schemes** – this forgery involves a type of fraud where an employee fraudulently affixes the signature of an authorized check signer. To successfully accomplish this scheme, an employee must have access to a blank check; they must be able to produce a convincing forgery of an authorized signature, and they must be able to conceal their crime. Since possessing the check is a key factor in this type of fraud, it is generally committed by employees in accounts payable, office managers, bookkeepers, or other employees whose duties typically include the preparation of organization checks.

• **Forged endorsement schemes** – this type of fraud exists when an employee intercepts a check intended for a third party and converts the check to cash by forging the endorsement in the third party’s name. A key factor in this fraud is the employee’s ability to gain access to the check after it has been signed. Therefore, anyone who is allowed to handle signed checks may be in a good position to intercept them. Separating the check preparation, the check signing, and the check delivery functions is a good practice in preventing this type of fraud.
• **Altered payee schemes** – this is another type of intercepted check scheme where an employee gains access to a signed check. It differs from a fraudulent endorsement scheme in that instead of endorsing the check in the third party’s name, the employee alters the payee designation so that the check can be endorsed and converted by the employee or an accomplice. One of the most egregious examples of poor internal controls is when an employee prepares a check, leaves the payee designation blank, and submits it to an authorized signer who signs the check and returns it to the employee. Common sense should prevent anyone from giving a signed, blank check to another person, but implementing strict controls to ensure the prevention of this possibility is advised.

• **Authorized maker schemes** – this is one of the most difficult check tampering schemes to defend. This scheme is one where an employee with check signing authority writes fraudulent checks to his or her benefit and signs his or her own name. There is no alteration or forgery involved in this fraud. The only obstacle in successfully committing this fraud is obtaining a blank check. However, since most authorized check signers are owners, officers, or otherwise high ranking employees, obtaining a blank check even if policy prohibits the handling of blank checks by check signers is not going to be too difficult.

**Expense Reimbursement Schemes** exist when an employee manipulates an organization’s expense reimbursement procedures to generate fraudulent disbursements. This type of fraud can be successfully perpetrated by mischaracterizing personal expenses and calling them business related expenses, overstating the true cost of legitimate business expenses, fictitiously creating an expense and submitting it for reimbursement, or submitting a legitimate expense for reimbursement multiple times. Most expense reimbursement schemes are successful because of a lack in the review procedures over expense reimbursement reports. It is not enough to have the detailed reports submitted if they are not reviewed. A policy requiring the periodic review of expense reports, paired with examining the appropriate detail, will help deter expense reimbursement frauds.

**Preventative Practices**

**Audit Committees**

Nonprofits are frequently criticized for having weak internal controls due to understaffing, poor training, and lack of segregation of duties. To compensate for the common control weaknesses, many nonprofits have taken to forming an audit committee.

A critical function of the audit committee is to serve as not only the financial watchdog but also to oversee the organization’s internal controls and risk-management procedures. The audit committee is an extension of the board in order to assure that proper financial management is in place. To have an effective audit committee, at least one member should be considered “financially literate”. Being financially literate can mean a lot of things, but the general criteria for the audit committee member is that the person must:

- Understand financial statements
- Understand financial risks
- Understand the impact of organizational decisions on the financial statements
- Be able to identify balance sheet risks
- Understand revenue recognition issues on the financial statements

The creation of an effective audit committee will assist a non-profit in being more accountable, and will benefit the organization with improved financial practices and reporting; better deterrence to fraud, and enhanced external and internal audit functions. An audit committee charter will establish how many members are on the committee, what is considered a quorum, how often the committee should meet, etc. An example of an audit committee charter is provided as Exhibit D.
Hotlines

Tips account for approximately 42% of fraud detection. Of the tips reported, nearly 50% of them come from employees. Clearly the significance of having an available channel for employees to communicate fraudulent or unusual behavior is incredibly high. A hotline is nothing more than a method for employees to anonymously report potential fraud, ethical issues, and other concerns. If the organization does not have the resources available to establish an internal fraud hotline, then strongly consider using an external vendor to provide this service.

Internal Reviews

Most organizations are not large enough to have a complete separation of internal controls, so to consider a separate internal audit function is out of the question. However, non-profits have a unique feature that for-profit entities do not: volunteers. The board of directors - more specifically the executive committee of the board (or even your newly formed audit committee) - is a perfect medium to use for spot checking records and performing periodical reviews of accounting records such as checks, invoices, bank reconciliations, and employee expense reimbursement reports.

The frauds of today have not changed significantly from the frauds of the past. Most frauds can be prevented by taking away opportunities for them to exist. The best way to remove the opportunity for fraud is through strong internal controls, which don’t always have to be expensive. There’s no guarantee that implementing internal controls and segregation of duties will prevent a fraud from occurring 100% of the time, but a sure way to keep fraud risk high is by doing nothing.
Gift Acceptance Policy Example

Acceptance of any contribution, gift or grant is at the discretion of the Organization. The Organization will not accept any gift unless it can be used or expended consistently with the purpose and mission of the Organization.

No irrevocable gift, whether outright or life-income in character, will be accepted if under any reasonable set of circumstances the gift would jeopardize the donor's financial security.

The Organization will refrain from providing advice about the tax or other treatment of gifts and will encourage donors to seek guidance from their own professional advisors to assist them in the process of making their.

The Organization will accept donations of cash or publicly traded securities. Gifts of in-kind services will be accepted at the discretion of the Organization.

Certain other gifts, real property, personal property, in-kind gifts, non-liquid securities, and contributions whose sources are not transparent or whose use is restricted in some manner, must be reviewed prior to acceptance due to the special obligations raised or liabilities they may pose for the Organization.

The Organization will provide acknowledgments to donors meeting IRS substantiation requirements for property received by the charity as a gift. However, except for gifts of cash and publicly traded securities, no value shall be ascribed to any receipt or other form of substantiation of a gift received by Organization.

The Organization will respect the intent of the donor relating to gifts for restricted purposes and those relating to the desire to remain anonymous. With respect to anonymous gifts, the Organization will restrict information about the donor to only those staff members with a need to know.

The Organization will not compensate, whether through commissions, finders' fees, or other means, any third party for directing a gift or a donor to the Organization.

**Revision History**
On ___(Date)___ the Board of Directors of the Organization adopted this Gift Acceptance Policy.
Debit Card / Credit Card Use Policy Example

POLICY

The corporation will not authorize the use of debit cards for any purposes. The Board will determine whether there is a compelling need for the corporation to obtain one or more credit/debit cards. If the Board determines that credit/debit cards are needed, the Board will authorize specific individuals to utilize a corporate credit/debit card. A corporate cardholder may use the credit/debit card only for official purposes directly related to the needs of the organization. The cardholder may not use a corporate credit/debit card for personal purposes, even if he or she plans to reimburse the organization.

The following purchases are not allowed on the corporate credit/debit card:

- Personal purchases
- Cash advances or loans
- Payroll advances
- Purchased for other organizations
- Alcohol
- Personal entertainment
- Fuel for personal vehicles
- Purchases from a business you own or operate unless pre-approved by the Board
- Any item inconsistent with the mission and values of the organization

An individual purchase shall not exceed $____________. Aggregate monthly purchases shall not exceed $____________.

PROCEDURES

In order to use the card, the cardholder must follow these procedures:

1. **Cardholder Agreement.** Upon issuing a corporate card to a cardholder, the cardholder must sign a statement that the cardholder has read and understands this Credit Card policy and will reimburse the corporation for any personal charges on the card.

2. **Advance Approval.** The Board must give advance written approval to make a purchase whenever practical. The cardholder’s purchase request should describe the purchase and cost.

3. **Original Receipts.** The cardholder must keep the original receipt that describes each purchase made on the card. The credit card receipt is not sufficient.

4. **Notification of use of the credit card.** The cardholder will email the Treasurer after each use of the corporate credit card noting the date, vendor, and amount of each charge made. This is will allow the Treasurer to be aware of the cash that will be required to pay the credit card bill and alert the Treasurer to potential unnecessary use of the credit card.
5. *Expense Form.* Within 5 days after the end of the billing cycle, the cardholder must prepare and sign an expense detail form and attach original receipts and a copy of the purchase request. In the case of meals, the statement must include the names of all persons at the meal and a brief description of the business purpose, in accordance with IRS regulations.

6. *Approval by Treasurer.* The cardholder must give the expense detail form to the Treasurer for approval. The Treasurer shall review each purchase to ensure that it was reasonable, necessary and the best value for the organization. The Treasurer will reconcile the expense detail form to the credit card billing statement, authorize payment and follow up on any inconsistencies.

7. *Notification of Loss/Theft.* The cardholder must notify the bank and the organization immediately in the event that the card is lost or stolen.
Exhibit C

Credit Card / Debit Card Acknowledgement Form Example

I have received the organization’s [Visa / American express] credit card (Card), Account Number: _______________

I take responsibility for all expenses charged to the Card, and I agree to:

• Use the Card, for business-related travel, meals and entertainment, hotels and car rentals. My personal expenses will NOT be charged to the Card.

• Personally pay all items charged to the Card when billed. I will promptly follow up with [Visa / American Express] to resolve any disputed charges.

• Submit a Monthly Expense Report for reimbursement of Card charges to Accounting, with accompanying receipts and Supervisor approval.

• Return the Card to my Office Administrator or to Human Resources as part of my Exit Interview when I leave the Company, or when I am specifically asked to do so.

• Review the Employee Handbook for details on Use and Return of Company Property, including Company issued credit cards.

I have read, understand and agree to the above-mentioned terms governing the use of the corporate credit card. In addition, I understand misuse or abuse of my Card or willful violation of the terms of this Agreement may result in personal financial liability and disciplinary action, including discharge, per Company Policy No. 35.

_________________________    _________________________
Employee's Signature      Print Name

Employee Number: _________________  Office: _____________________________

Date Card Received by Employee: ___________  Card Expiration Date: ___________

Acknowledgement Form received by Corporate & card info entered in by: _____________________ (initials/date)

Card returned to HR on: ____________________
SAMPLE AUDIT COMMITTEE CHARTER

Mission Statement for the Audit Committee

The Audit Committee shall assist the Board of Director in fulfilling its oversight responsibility with respect to the financial reporting process, the system of internal controls, the audit process and the [Nonprofit]’s process for monitoring compliance with laws and regulations. The Audit Committee shall appoint and manage the outside independent auditor.

a. The Audit Committee shall consist of [at least three board members]. All members of the Committee shall be independent directors. The Committee will be appointed by the board and will elect its Chair from among its members. All members of the Committee should be financially literate. At least one member should have accounting background or related financial management experience.

b. The Committee will meet [twice a year/in January and May] in connection with regularly scheduled meetings of the Board and otherwise as necessary. [Board members who are not members of the Committee may not attend meetings of the Committee except as invited by the Committee for consultation.]

c. A majority of the Committee shall constitute a quorum for the transaction of business at any meeting thereof, and the act of a majority of the members of the Committee present at any meeting at which a quorum is present shall be the act of the Committee.

Roles and Responsibilities

The Committee shall:

A. Provide oversight to ensuring that the [Nonprofit] has an adequate system of internal controls and preparation of financial statements.

B. In fulfilling this responsibility, the Committee shall:

1. Be directly responsible for the appointment, compensation, retention and oversight including evaluation of the work of the outside auditor preparing or issuing an audit or any related work (including resolution of disagreements between management and the outside auditor regarding financial reporting) and the outside auditor shall report directly to the Committee;

2. Review the outside auditor’s qualifications, independence and performance;

3. Review the scope, approach and cost of the audit;

4. Review the [Nonprofit]’s internal audit function, including review of the committee charter, activities, staffing and organizational structure of the internal audit function;

1 No member of the Committee may in the current fiscal year or in the previous fiscal year have been associated in the capacity of employee or of compensated officer of the [Nonprofit]. Nor may any member of the Committee accept, either directly or indirectly, any consulting, advisory, or other compensatory fee from the [Nonprofit].
5. Review significant accounting and reporting developments and issues;

6. Review the annual financial statements audited by the outside auditors;

7. Review suggestions for improvements in internal controls from the internal and outside auditors;

8. Review and monitor the [Nonprofit]’s internal controls and exercise oversight of management’s handling of the [Nonprofit]’s major financial exposures;

9. Review with the outside auditor any audit problems or difficulties and management's response; and

10. Establish procedures for the receipt, retention and treatment of complaints or concerns received by the [Nonprofit] regarding accounting, internal accounting controls or auditing matters, including confidential, anonymous submissions from employees.

C. Exercise oversight of the [Nonprofit]’s process for monitoring compliance with legal and regulatory requirements.

D. Review and make recommendations to the Board with respect to retention of the independent auditor, and the audit functions.

E. Periodically review and assess the adequacy of the Committee’s charter and make recommendations to the Management and Governance Committee of changes.

F. Conduct an annual performance evaluation of the Committee and report its findings to the Chair of the Board.

G. Attend to such other matters as the Board of Trustees may from time to time determine.

H. Maintain minutes of Committee meetings and report regularly to the Board.