The Not-for-Profit’s Guide to Fraud Prevention

A Tale of Two Organizations and How To Create Your Own Happily-Ever-After Story
INTRODUCTION

TALE 1: LACK OF CONTROLS LEADS TO SIGNIFICANT LOSSES 1

TALE 2: WHISTLEBLOWER POLICY UNCOVERS COLLUSION 2

INTERNAL CONTROLS CAN SAVE THE DAY 3

6 RISKS SPECIFIC TO NON-PROFITS 3

REDUCING THE RISK OF FRAUD 5

PROFILE OF A FRAUDSTER 6

KEY QUESTIONS TO DETERMINE YOUR RISK 6

IMPLEMENT CONTROLS TO MITIGATE RISKS 7

PUTTING POLICY INTO ACTION 9

LIVING HAPPILY-EVER-AFTER AND FREE OF FRAUD 10
It’s an all-too-common moral of a story: The one we trust the most is the one who betrays us.

Such violations of trust often occur in not-for-profit organizations due to a lack of resources or knowledge necessary to implement preventive or detective controls. And when occupational fraud is revealed, not-for-profits often feel pressure to keep it quiet in order to avoid a scandal and protect donations.

The costs of fraud extend far beyond financial losses. Also at risk is the organization’s reputation (which is a vital element to current and future funding), and even the personal reputation and assets of the board members and executives who have fiduciary responsibility.

But this ending is not written in the books yet. You, as an executive or board member within a not-for-profit, hold your fate in your own hands.

While the Association of Certified Fraud Examiners (ACFE) estimates that all organizations lose, on average, about 5% of revenues to fraud every year, the presence of anti-fraud controls is correlated with significant decreases in the cost and duration of those occurrences.

Consider the following tale of two not-for-profits and note how a few preventive measures made all of the difference.

**Tale 1: Lack of Controls Leads to Significant Losses**

It started small. Doris, who had been the bookkeeper for a local charity for 15 years, had recently gotten a credit card on the charity’s account – even though she didn’t handle purchasing for the organization. Her husband had recently lost his job, so she used the card to buy a few personal things, telling herself that she would pay it back next month. But the charity’s board and executive director were focused on fundraising, so she was the only one who reviewed the credit card statements each month. Rather than bring her actions to their attention, she just kept quiet.

The next time she used the credit card, Doris told herself that she deserved it. She had worked hard for the organization for a long time and for relatively little pay. So what if she treated herself to some “perks” now and then? The good she was doing outweighed the bad – right?

Doris covered her tracks by spreading the credit card charges out across several different expense accounts so that anyone who happened to review the financial statements wouldn’t notice anything funny. Not that it was necessary, she reasoned, since she was the only financial staff person and no one else even bothered to review the financial statements. To keep anyone else from taking over her duties, she avoided taking sick days and passed up her annual vacation. But
the stress of her husband’s unsuccessful job hunt and the weight of keeping her secret finally caught up to her. As she was in bed with a nasty case of the flu, the charity’s credit card statement arrived. When the executive director opened it, he was shocked to find charges to department stores and an auto mechanic. After a call to the credit card company, the executive director discovered that Doris had been perpetrating her scheme for more than a year and racked up a total of $50,000 in personal expenses.

The executive director reported Doris to the police, and as part of her judgment she was ordered to pay the charity about $100 per month. However, at that rate, it would take her more than 40 years to pay the full amount. In the meantime, the local charity had lost $50,000 that could have furthered its mission.

Tale 2: Whistleblower Policy Uncovers Collusion

Jack and Larry thought they had a foolproof plan. The CFO and controller, both of whom had been with the metro area symphony for more than five years, already approved one another’s expense reports. Who would know if they used their corporate credit cards to pay for weekend getaways with their wives? On top of these lavish weekends, the two also were close to several of the symphony’s major sponsors. Leveraging their positions, they skimmed a portion of those sponsorship payments off of the top, and again they colluded to hide the scheme from the CEO and board of directors.

What they didn’t count on was the efficacy of the organization’s internal controls. When Lisa, the accounts payable clerk, received the statements for processing, she noticed that some of the charges looked fishy. She remembered that the CEO had spoken during the annual retreat about the need for everyone to stay alert for signs of fraud. Lisa pulled out the written copy of the symphony’s whistleblower policy. As a result of Lisa’s anonymous tip, the symphony caught the perpetrators within just three months. While the two fraudsters had already caused losses of almost $100,000, the symphony was able to cut short what could have been an even more devastating scheme.

The High Costs of Ignoring Fraud Risks By the Numbers

$23.2\%$ of frauds that cause more than $1 \mbox{ million in losses.}$

$10.1\%$ of all frauds affect NFPs with a median loss of $100,000.

$12\%$ of victim organizations that make a full recovery.

Source: Association of Certified Fraud Examiners (ACFE) 2016 Report to the Nations on Occupational Fraud and Abuse
INTERNAL CONTROLS CAN SAVE THE DAY

These two examples, while fictional, are representative of fraud cases that strike not-for-profits every year. In the first example, the charity failed to take even simple precautions that could have avoided the theft. First, the bookkeeper had no reason to have a credit card on the charity’s account, since she wasn’t responsible for purchasing or paying bills. Second, the executive director or a board member should have been reviewing the credit card statements on at least a periodic basis.

In the second case, the existence of strong controls saved the day. Even though the CFO and controller bypassed the first control (segregation of duties) through collusion, the strong tone at the top and written whistleblower policy allowed the organization to stamp out the scheme before it proceeded too far.

6 RISKS SPECIFIC TO NON-PROFITS

We’ve all heard the myths when it comes to fraud in not-for-profit organizations: “It can’t happen here. All of our volunteers and staff members are honest and committed to our mission, and besides they’ve been with us for years. If someone was stealing from us, we would have found it by now.”

But the fact is that not-for-profits account for 10.1% of all frauds (ACFE 2016 RTTN) and face specific risks that make them particularly susceptible.

1. Inadequate resources for financial oversight

Most non-profits are akin to small businesses. Of the roughly 1 million public charities in the United States, about three-quarters have annual expenses of less than $500,000. (http://www.independentssector.org/scope_of_the_sector) Like Doris’ charity, small not-for-profits often lack the resources for strong internal controls such as segregation of duties.

2. Excessive control in one person

Especially in small not-for-profits, the founder or executive director may be responsible for almost everything – from writing checks to approving vendors. This lack of segregation of duties creates a seedbed for fraudulent behavior. Tenure and level of authority also positively correlate with the magnitude of the fraud. Executives commit frauds with a median loss almost 10 times those caused by employees, and employees with more than 10 years of tenure are responsible for median losses 2½ times those caused by employees with less than five years of experience, according to ACFE’s 2016 Report to the Nations.

True Stories of Million-Dollar Fraud

Atlanta’s Woodruff Arts Center was already struggling with mounting debt when it discovered that the facilities director, Ralph Clark, had embezzled more than $1 million over the course of seven years, in part through issuing invoices for bogus vendors. Clark would pick up the checks for the vendor himself and deposit them into accounts for which he had signatory authority. Clark also required a maintenance vendor to pay him kickbacks on inflated invoices. Clark is facing a maximum prison sentence of 10 years and a fine up to $250,000.
3. All-volunteer boards with little or no financial oversight

The risk of too much control concentrated in the hands of the executive director indicates a need for objective oversight from a financially literate board of directors. To meet their fiduciary duty of care, all board members need to understand how to read financial statements and be alert to warning signs of errors, fraud, or abuse. However, unlike many for-profit corporations and larger not-for-profits, smaller NFPs tend not to recruit board members with experience running organizations and overseeing financial responsibilities. In those smaller organizations, like Doris’ charity, board members’ roles typically are focused on fundraising, and the organizations may not include financial oversight in their list of responsibilities.

4. Volunteers privy to confidential information

In addition to the board members, volunteers perform many financial functions in not-for-profits, including collecting donations, rental fees, and other payments. In many cases, these volunteers have not been vetted thoroughly, opening the door to a potential fraudster.

5. Nonreciprocal transactions

A donor typically does not receive anything of value in exchange for the contribution except for a letter acknowledging the transaction. In many cases, that contribution is in cash. Both of these facts make it all-too-easy to divert those funds.

6. Susceptible to negative publicity

In the 2016 ACFE study, more than 40% of fraud cases were not reported to the police, and the most commonly cited reason was fear of negative publicity. For many not-for-profits, negative publicity and the subsequent hit to donations could sink the organization. That knowledge exerts pressure on many executive directors to keep the fraud quiet, and the very fact that so many of these cases go unreported is an incentive to fraudsters. Because there is no record of their malfeasance, subsequent employers are none the wiser. Of the repeat offenders who perpetrated major embezzlements in the last five years, about one in six stole from not-for-profits or religious organizations.

True Stories of Million-Dollar Fraud

New York State Attorney General Eric Schneiderman found evidence of “stunning” negligence on the part of the board of Educational Housing Services (EHS).

Board members must pay a collective $1 million from their own personal funds and are forever banned from sitting on the board of any New York charity after Schneiderman found that they breached their duties of loyalty and care by contracting with Student Services, Inc. (SSI), a corporation founded by founder and former board president George Scott and his wife.

SSI charged Educational Housing millions of dollars for intermediating cable, phone and Internet services, which Schneiderman asserts provided no meaningful benefit. Board members were also receiving consulting contracts that provided “little value” to EHS, Schneiderman says.

In addition to the $1 million to be paid by the board, Scott was ordered to make restitution of $2.5 million and waive SSI’s rights to an additional $2 million expected under the company’s contract with EHS.
REDUCING THE RISK OF FRAUD

Due to these unique risks, if your not-for-profit organization hasn’t already suffered an instance of fraud, then there is a decent chance that you will discover one soon. And, if so, it likely has been going on for months or even years.

But you can change the ending of this story. According to the ACFE, 29.3% of fraud cases are due to a complete lack of internal controls. Choose your own adventure by instilling a strong anti-fraud culture and a set of controls that are targeted to your organization’s unique risks.

Start by identifying the types of fraud that could be perpetrated by your employees, board members, or volunteers. Some of the typical types of fraud experienced by not-for-profits include:

- **Billing fraud**, including credit card abuse and creation of fictitious vendors. Frequency: 25% of all fraud cases, according to ACFE.
- **Skimming**, in which funds are diverted before they are ever recorded on the books. This fraud is most likely to happen when the funds are in the form of cash. Frequency: 19.2% of fraud cases.
- **Expense reimbursement fraud**, in which an employee claims reimbursement for fictitious or inflated business expenses. Frequency: 25%.
- **Check tampering**, a scheme in which an employee intercepts, forges or alters a check. Frequency: 25% of fraud cases.
- **Payroll manipulation**, which includes fraudulent timekeeping, fictitious employees, and continued payment of terminated employees. Frequency: 13.5%.
- **Corruption**, in which an employee abuses his or her influence in a business transaction. This situation includes board members or executives with conflicts of interest, as well as bribing. Frequency: 28.8% of fraud cases.
PROFILE OF A FRAUDSTER

Detecting fraud is all the more difficult because the typical fraudster doesn’t look like a crook. In fact, it may be the person you least suspect. Consider the perpetrators in our two case studies. Doris is a long-time, trusted bookkeeper; Jack and Larry hold high-level positions in the symphony. All three of them are respected members of society with spotless records prior to their crimes.

These characteristics align with the common profile of an occupational fraudster:

- Married
- Educated
- In their 30s or 40s
- First-time offenders
- Hard workers (like Doris, they may never take vacations)
- In a position along the financial chain, such as a bookkeeper or controller

Certain characteristics correlate with higher median losses. For example, in the ACFE study, men were responsible for median losses roughly twice the amount stolen by women.

Collusion is another factor that increases the loss – as Jack and Larry’s organization discovered. While lone perpetrators commit most frauds, conspiracy cases account for higher losses. Collusion was responsible for 47.1% of fraud cases in the most recent ACFE report, but median losses were about 3 times those caused by lone perpetrators (approximately $260,000 for 3–4 people vs. $85,000 for one perpetrator).

Level of authority also correlates with larger losses. ACFE reports that the median loss caused by an owner or executive is $500,000 (in the U.S.) as compared with $150,000 median loss caused by managers, and $54,000 median loss caused by employees. Fraud by an executive also took longer to detect: 24 months vs. 12 months for employees.

Tenure also has a positive correlation with the size of the loss. Perpetrators who had worked for their organizations for more than 10 years were responsible for a median loss of $250,000, compared with a median $100,000 loss for those who had been in their positions for one to five years.

KEY QUESTIONS TO DETERMINE YOUR RISK

The perpetrators in our fictional case studies exhibit many of the characteristics of typical fraudsters. If their leaders had been more alert to these signs, then they could have changed the outcome of their stories.

Armed with an understanding of potential types of fraud and the demographics of fraud perpetrators, executive directors and board members should ask and answer some key questions that can illuminate gaps in internal controls. This process is also known as a fraud risk assessment.
The overall question a nonprofit should be asking is: What are the business processes and controls around functions where money is coming in and going out of the organization?

Specific questions include:

- What is the tone at the top with respect to ethical behavior?
- How often is management reviewing financial transactions?
- Do we have a written conflict of interest policy? Are officers, directors, and key employees required to annually disclose interests that could give rise to conflicts?
- Do we have a written whistleblower policy?
- Do we have a written accounting policy handbook that identifies each significant accounting position and describes job responsibilities?
- Does the accounting policy describe processes and internal controls related to each major transaction cycle? Does it spell out who should have corporate credit cards and who can write and sign checks?
- Do we regularly monitor and enforce compliance with each of the above policies?

**IMPLEMENT CONTROLS TO MITIGATE RISKS**

With an understanding of areas where fraud is likely to occur, any organization – even Doris’ small charity – can implement simple controls to mitigate those risks by implementing internal controls that fall in the three primary areas of prevention, detection, and correction.

**Prevention**

The first line of defense includes measures that prevent perpetrators from committing an act of fraud. For example:

- **Segregation and/or rotation of financial duties.** The person who initiates a transaction shouldn't approve that transaction, and the person who approves the transaction should be different from the person who records it. While collusion like Larry and Jack’s can negate this control, a triad of checks-and-balances significantly reduces the chances of fraud.

- **Credit card policies.** Credit card accounts are akin to cash and should only be assigned to employees who have a clear need to use them, such as purchasing managers. Bookkeepers like Doris, with no need to make purchases, should not have credit cards. When individual cards are required, consider credit purchase contracts for employees outlining utilization responsibilities and rules, and restrict accounts with spending limits and merchant accounting codes.

- **Dual signatories.** Requiring two signatures on checks above a certain amount (both of which are from individuals who did not write the check) reduces the likelihood of check fraud.

- **Access controls,** such as strong passwords for accounting systems, restrict access and also increase traceability of actions.
• **Background checks.** In addition to prospective and current employees, also scrutinize vendors and volunteers who are involved with financial transactions.

**Detection**

Due to their limited resources, many small organizations can’t afford to implement robust preventive controls. Ongoing oversight through detective controls can provide the safety net such organizations need. These controls include:

• **Hotline policy.** This control is consistently the most common method of initial detection among frauds reported to ACFE. As shown in our symphony example, more than 47% of frauds reported in the 2016 ACFE report were detected initially through a tip from a whistleblower.

• **Internal audits** of financial statements (comparing actual to budget and investigating any variances), as well as credit card charges, expense reports, payroll records, and petty cash. Internal audits were the second most common method of initial detection (18.4%), according to ACFE. Both organizations in our case studies could have cut short the duration of fraud – or even deterred the fraudsters in the first place – with regular internal audits.

• **Management review** of bank statements, credit card statements, canceled checks, and invoices. Management review was the third most common method of initial detection (12.1%), and it could have saved Doris’ charity from tens of thousands in losses.

• **External audits** of financial statements, as well as of internal controls over financial reporting. These audits may not be cost-effective for many smaller organizations. While an external financial statements audit was the most common anti-fraud control reported by ACFE respondents, only 1.8% of frauds were detected by an external audit. The reason is that financial statement audits are not designed to detect misappropriation of assets, although auditors do assess fraud risks and procedures set-up to mitigate these risks.

**Correction**

Sometimes the best defense is a good offense. If would-be fraudsters know that they will be prosecuted to the full extent of the law, then they will likely think twice about targeting your organization. An effective fraud policy should include the following components:

• **Internal investigation.** A forensic accounting investigation may be necessary to quantify the loss, determine how it was perpetrated, and track the money. This analysis may be necessary to support a prosecution or insurance claim(s).

• **Interviews.** In addition to interviewing the suspect, other employees, board members, and volunteers may need to be interviewed.

• **External investigation.** Pursuing prosecution creates a permanent record that can be discovered by other organizations where the perpetrator may seek employment or volunteer positions in the future.

Be sure to seek legal counsel in establishing any policies, as well as in executing those policies in the case of an actual fraud.
PUTTING POLICY INTO ACTION

We’ve outlined a number of policies that you can use to rewrite your organization’s story. But without action, a policy is nothing more than a fairy tale.

Here is an action plan that any size organization can use to live out a happily-ever-after story:

1. **Set the right tone.** In addition to creating written conflict-of-interest, whistleblower, code of conduct and accounting policies, distribute hard copies of those policies at least annually. Most importantly, talk about the importance of ethical behavior and the consequences of not living up to the organization’s code of conduct and other policies. In our symphony case study, the CEO took time at the annual retreat to discuss the organization’s zero tolerance for fraud, and that simple act influenced Lisa to report a major fraud scheme.

2. **Know your team.** Unfortunately, perpetrators of fraud often go on to commit schemes at other organizations, disproportionately at nonprofit and religious organizations. Conduct background checks of all prospective employees, as well as any volunteers who will be handling financial transactions. Also conduct periodic background checks of current employees and volunteers.

3. **Recruit at least one financially savvy board member** who is capable of overseeing your organization’s fraud risk. Educate that person regarding risks specific to your organization.

4. **Train board members, employees, and volunteers to be aware of and watch for signs of fraud.** Pay attention to rumors of changes in an employee’s behavior or lifestyle. Red flags include living beyond one’s means, gambling problems and other evidence of financial difficulties, an unusually close relationship with a vendor, and control issues. Doris’ unwillingness to take vacations and sick time should have been a red flag for her employer.

5. **Become involved in the financials, with a focus on anomalies.** Frauds discovered by management review and other proactive controls showed the greatest percent reduction in median fraud losses. Both of the schemes described in our case studies would have been potentially deterred if the perpetrators knew an executive or board member was keeping a close eye on the financials.

6. **Create an easy and comfortable method for reporting suspicions.** Lisa’s simple anonymous tip set the ball in motion to bring a major fraud scheme to a halt. Keep in mind that, while employees are the primary source of tips about fraudulent activity, they may also come from outside sources – such as vendors, customers, competitors, and anonymous sources. Create a mechanism, such as an anonymous hotline, that is accessible by any of these sources.

7. **Perform a fraud assessment.** Consider a review of your fraud risks every three years, or more frequently if your organization does not perform regular internal audits.
LIVING HAPPILY-EVER-AFTER AND FREE OF FRAUD

Writing your own happily-ever-after story starts with a thorough assessment of your organization’s unique risks. Your CPA firm is in an ideal position to help you perform a fraud risk assessment and identify the controls that make the most sense for your organization. A CPA can also help you identify and recruit financially savvy board members and train them to spot early signs of fraud.

If you’re looking for help identifying fraud risks and implementing cost-effective internal controls to mitigate those risks, contact CRI’s not-for-profit team to set-up a free 30-minute consultation about your current state and how we can help. But most importantly, don’t wait until a fraudster strikes to start authoring your own story.