Fraud and Not for Profits

By Joanne Ironside for ACFE Vancouver Chapter for March 2021

Not-for-profit (NFP) organizations serve to benefit the lives of people all over the globe. Are non-profits and charities any more vulnerable to fraud or more likely to perpetrate outright fraud under the guise of being a charity? How susceptible to deception are they be? The answer, unfortunately, is more than one expects. How do we manage, mitigate, and prevent fraud in these vital sectors of our social economy? This paper will examine types of fraud, discuss cases, and provide common-sense solutions.

No one can take trust for granted. As reported by the New York Times, 40-45 billion dollars disappeared due to internal and external fraud in not-for-profit organizations. Non-profits consisting of educational, religious, social service, and charity institutions improve the broader

community. One might assume that not-for-profit organizations are less likely to be involved in fraudulent activities. Unfortunately, fraud frequently occurs in not-for-profit organizations.

Fraud cases include corruption, employee and board misconduct, theft, embezzlement, and misrepresentation of financial statements, to name a few. Others are cybersecurity, vendor fraud, asset theft, and outright cash skimming.

The Importance of the Fraud Triangle:

NFP Management and Boards should familiarize themselves with the fraud triangle. The fraud triangle is credited to Steve Albrecht and refers to a framework for spotting high-fraud situations and the circumstances that would lead to fraud. The fraud triangle states that fraud occurs when pressure, opportunity, and rationalization collide. The pressure is the financial or emotional force pushing towards fraud. Opportunity is the ability to execute the plan without being caught. Rationalization is how someone justifies their dishonest actions.

Interestingly, most fraud is detected through a tip or by accident. Scams have many early warning signals. The higher an individual's position is in a not-for-profit organization, the greater their ability to commit fraud. Interestingly, according to the 2020 Report to the Nations Fraud study, only 4% of scams are detected during an external audit.

Key Warnings:

Essential warnings or red flags can be organized into four categories and can help design internal controls and monitoring procedures. These categories include data, documents, lack of rules, and behavior. Data may consist of transactions conducted at unusual times of the day, or during days of the week, or in a season when transactions do generally not occur. It could include figures in accounts with large round numbers or transactions with unknown parties, including related parties or unrecognized vendors. Data may also include improperly classified transactions in the financial records. Documents may consist of missing or altered records. It could include evidence of backdated documents, missing or unavailable originals, copies that conflict with one another, questionable or missing signatures.

Lack of Internal Controls is a standard red flag. There are inconsistent or non-existent monitoring controls, inadequate segregation of duties, lax rules regarding transaction authorization, and a failure to reconcile bank statements promptly. It also includes a low tone from senior leadership. Behavior that suggests fraud includes financial difficulties or living beyond one's means. Divorce, family problems, or addiction problems. Past employment-related or legal issues. Unexpected charitable behavior, a very close relationship with suppliers or parties receiving grants and services, and an unwillingness to share duties. Other concerning behaviors could include refusing to take vacation, defensiveness, complaints about working conditions, pay and leave, and complaints about a lack of autonomy.

It is crucial to respond quickly to fraud; avoiding the situation in the first place is the best plan of all. It is unrealistic to eliminate the risk of fraud; however, the governing body and executives in a non-profit organization play a vital role in minimizing the risk. By establishing an environment of ethical behavior, closing gaps in internal controls, and developing a proactive fraud identification and response program, non-profits can reduce the financial and reputational damages associated with the fraud.

Anti-Fraud Policies:

Some fundamental ways to refine the anti-fraud control policies include forming an empowered audit and finance committee. It is most valuable that the committee has independence from management. A committee with up to five members is generally workable and optimal for most non-profits. At least one committee member should be a financial expert, but individuals with non-financial skills and expertise can provide a valuable perspective.

A combination of internal and cultural controls forms the foundation of an anti-fraud program. Internal controls restrict opportunities to hide the fraud trail and can discourage all but the most determined fraudsters. Standard tools include security and access controls, such as dual authority or dollar authorization limits, audits, inspections, and transaction monitoring. Beneficially, the presence of anti-fraud controls correlates with a decrease in the cost and duration of fraud schemes.

Mechanical compliance with internal controls is not sufficient to prevent fraud. Senior NFP leadership must promote a culture of integrity and ethics, motivating employees to play a more active role in stopping fraud. A stable, ethical environment encourages self-policing, simple adherence to internal control methods.

Tips:

Leadership must provide a process for reporting suspicious behavior. The 2020 ACFE Report to the Nations Global Fraud study states that tips are *the most effective* way to detect fraud. In the 2020 survey, tip-offs were responsible for uncovering 43% of incidents of occupational scams. Tips are three times greater than other detection forms, such as management reviews, surprise inspections, audits, or surveillance devices. It is critical to the employees to know that the non-profit's reputation and mission depend on their willingness to report suspicions of fraud.

Response Plan:

Despite an influential audit committee and adequate controls, fraud can occur. When the organization suspects that scam is happening within their organization, they can choose to do nothing to avoid the bad publicity or hope that the problem will disappear on its own. They investigate the issues themselves or engage outside experts to probe the subject more deeply.

It is critical to developing a response plan for when deterrence fails. The initial reaction of leadership and board members is to immediately confront the suspected fraudster and collect documents and electronic evidence. Unfortunately, moving too quickly could compromise the not-for-profit's ability to prosecute. Engaging a suspected fraudster without adequate evidence is both uncomfortable and legally dangerous. It could alert the suspect to destroy her records. Secretly, examining computer links and email archives can make the evidence inadmissible. An improper process may make it more challenging to achieve a conviction and recover lost funds. To avoid unintended consequences, non-profit organizations should develop appropriate strategies in advance to deal with specific types of fraud or other misconduct.

Fraud Detection:

When fraud is detected, the most common impulse is to dismiss, limit the damages, and hope the story can be kept quiet. Eventually, word of the fraud gets out. The ensuing rumors are likely to be exaggerated, causing even more reputational damage than would have been done if the Board had been forthright. Reputational damage can only hurt the charity, as it may impact its ability to source new donations or detract from its' ability to complete its stated mission and purpose.

Managing the Fraud*:*

It is often wise to engage a team of forensic experts. These teams may include a lawyer and an experienced fraud & forensic investigator. These professionals can help identify how the loss occurred, identify "leakage" or other areas not initially considered an issue, preserve any available evidence, quantify the loss, control the flow of information and, in many cases, help stem the loss. The forensic team will then aid the Board of directors or governing body to improve their governance and fraud risk management programs to help protect and preserve the organization.

Cyber-Security Threats:

According to Proofpoint, a leading cyber-security firm, schools and universities face four times as many phishing attacks as the average organization. Educational institutions are amongst the most vulnerable sectors. In 2018, Proofpoint cyber-security researchers discovered that the frequency the education sector is being targeted increased by 120% year-over-year, with most fraudsters looking for cash versus corporate secrets. Cybersecurity is a significant threat to the education sector. Because schools and universities handle large amounts of personal data, they typically lack sufficient resources to ensure information is dealt with responsibly and that defense mechanisms are adequate.

Defense against Phishing Emails:

Phishing is a cyber-attack with email. Its' goal is to deceive the email recipient into believing that the email contains information the reader wants or needs — a request from their bank, for instance, or a note from someone in their company — and click a link or download an attachment. In theory, phishing scams are easy to prevent. They are just emails, and if one

ignores the message, they pose no danger whatsoever. However, when the wrong file downloads or a link innocently clicked, then there are problems. Staff responds because criminals make them believe that is not an option. The message may tell the reader that they urgently need to download a file from their key supplier or that they need to give payment details for something they ordered. Phishing emails create a false sense of urgency. The key to successfully defend against phishing emails is to learn to question the message and manipulation.

Payroll:

The payroll administrator is one of the most trusted employees. Payroll staff has access to confidential information, bank account numbers, Social Insurance numbers, and compensation. These valued employees are often among the ones who embezzle. Payroll frauds last an average of 30 months, which is one of the longest-lasting fraud schemes. The most common payroll fraud schemes involve ghost or non-existent employees, incorrect wages, and commission schemes.

Simple internal control to reduce the likelihood of payroll fraud occurring include having a third party distribute the payroll cheques or electronic payroll notifications. Payroll ledgers and payroll disbursements should be reviewed every month by someone other than the payroll administrator. This review includes reconciling the payroll bank statements with the payroll records. The payroll processing company should remit statutory remittances directly to the government. Review payroll accounts monthly for fictitious employees or employees no longer employed. Task the payroll system to produce exception reports that are reviewed by a senior employee. Exception reports should include changes in pay rate, excessive hours worked, overtime hours worked, excessive amounts paid, the system overrides, and personnel data changes (such as address changes). All accounting personnel, including the payroll employee, are required to take a vacation. Cross-train employees to process the payroll in the absence of the payroll administrator. Payroll bank statements should be reviewed and reconciled by an accounting employee independent of the payroll function. An employee, separate from the payroll function, should verify timely statutory remittances to the Canada Revenue Agency or applicable government agency.

According to the fraud triangle, employee theft requires a motive or pressure, rationalization, and opportunity. The explanation may be gambling, an expensive lifestyle, frequent travel, divorce, or drug addiction. Perhaps the employee will rationalize that he will pay it back soon or tell himself that he does not get paid enough and deserves more compensation. Finally, the opportunity presents itself with weak internal controls. Tightening an NFP's internal controls reduces the opportunity side of the triangle.

Fraud hotline for whistleblowers:

One remedy to weak governance is a hotline to encourage and facilitate reporting of fraud and tips. The purpose of charter schools is to create a unique environment for children to learn. Lacking the proper oversight and efficient internal controls, these schools cannot provide the promised education. As more schools come online, the risk of more significant losses looms larger without improved oversight and accountability.

Imposter Scams:

While regulators and the Canada Revenue Agency (CRA) battle impostor telemarketing, fraud happens everywhere. According to a recent article from the Independent School Manager's association, impostor scams are the third most common consumer complaint. Schools are frequent targets for such scams. Schools can avoid costly mistakes using some of the following tips.

Do not rush. There is always time:

If a caller is purporting to be a Board member, the bank, law firm, or the CRA phones threatening immediate repercussions should you fail to act, find a way to stall. Pressuring potential victims into making hasty decisions is a clear warning sign, and it is always worth taking the extra time to verify this is an authentic request.

Do not trust names, emails, or caller identification:

Today, scammers can impersonate everyone from the CEO, Board Chair to the CRA collection department. It is always better to phone the source using an alternative communication method, such as calling the vendor directly instead of using the number the suspected fraudster provided.

Question suspicious syntax:

Are there odd capital letters? Are there unexpected opening lines, unlike routine correspondence such as Hello Sir/Madam or Dear God's Chosen? Consider word choices that are unlike regular communication. These red flags should have you assume the message is spam.

Be Careful with Wire Transfers:

Wire money transfers, once completed, are almost impossible to reverse. Ensure that wire transfers must be approved by more than just one person and are going to the correct recipient.

Double Check the Financials:

While every school and not-for-profit operates on trust, not double-checking the bank accounts and accounting records can have severe consequences. Embezzlement and other forms of financial fraud could damage the school's community, hurt the financial budget, and even force bankruptcy. The negative publicity will discourage prospective families, donors and create serious cash flow issues.

There are "warning signs" that it may be time to examine the financials more closely. Of course, these can all indicate dedicated employees and entirely innocent, but it does not hurt to explore these discrepancies.

· Petty cash disappears quickly.

· Expense reports seem extravagant (travel, office supplies, etc.).

· The employee avoids taking all of his vacation days. There is no opportunity for another employee to take over some of the functions. Make vacations mandatory by implementing a "use-it-or-lose-it" policy. Regular breaks not only reduce employee burnout but can also aid in

uncovering fraud. Frequently, once a non-vacation-taking employee takes time off, evidence of fraud surfaces. Some individuals work non-stop for fear of being discovered.

· An employee demonstrates personal spending—vacations, new cars, expensive clothing that his/her level of family income cannot support.

· Significantly, remember to reconcile the monthly bank statements promptly with financial reports. Mistakes get found before they cause more significant problems. Issues are proactively addressed well before a "trusted employee" siphons off two million dollars.

Conclusion:

Non-profits exist to serve and improve the lives of people living in the communities they support. It is critical to understand funding, donations and verify the budget. Effective governance, the right culture, and adequate financial controls are vital to protect donors and ensure the organization's economic viability. Thus, it is essential to stay alert and act on all fraudulent behavior. The mantra for all must be "see something, say something." No one can afford to take fraud for granted.

Joanne Ironside is a current student of the Graduate Certificate Program in Forensic Investigation of Financial Crime at the British Columbia Institute of Technology.

If you are interested in speaking at one of our Chapter events or submitting an article for our monthly newsletter or weekly fraud insights post, please contact me directly anytime at president@cfevancouver.com. This is a great professional development opportunity. Lastly, I encourage everyone to make continuous learning a part of their lives and wish you all the very best in 2021.

Most sincerely, Steve Wilson, President, ACFE Vancouver Chapter, www.cfevancouver.com