



IDENTIFYING & MITIGATING NONPROFIT FRAUD

A comprehensive guide to understanding, spotting and preventing fraud at your organization.

It's tough enough to bring in the funding needed to fulfill your organization's mission. Throw fraud into the mix, however, and you have a real problem. In 2020, nonprofit fraud cases resulted in an **average loss of nearly \$640,000***. Even worse, 97% of those cases were **perpetrated by someone within the organization.**

How does this happen? Nonprofits often lack the **personnel** needed to properly monitor accounting and financial operations. So these duties tend to fall to executive directors, managers or board members, all of whom have other responsibilities. As a result, internal controls can easily get overlooked—and that makes these organizations more susceptible to fraud.

You can help prevent fraud within your organization by understanding the form it takes and the warning signs that it might be an issue. You should also have a basic familiarity with your nonprofit's accounting and implement effective internal controls to hold everyone accountable.

The good news: **It's all easier than you might think!**

* = According to the Association of Certified Fraud Examiners 2020 report

Types of Fraud

Fraud at your nonprofit can generally fall under two categories.

CASH FRAUD

As its name implies, cash fraud involves stealing funds from an organization.

- » **Skimming** occurs when money is taken before it's entered into your accounting software. For example, a thrift shop employee makes a sale but doesn't record it and pockets the cash.
- » **Embezzlement** is when money is stolen after it's been recorded in your organization's books. Examples include submitting falsified expense reports, stealing checks and depositing them into a personal account, and making payments for nonexistent vendor services.

FINANCIAL STATEMENT FRAUD

This is the deliberate misrepresentation or omission of financial statement data, with the intent to mislead board members, bankers, funders or others about the organization's financial performance. Examples include delaying the payment and recording of expenditures, adjusting journal entries, improper revenue recognition, and overstatement of assets.

Why do people commit nonprofit fraud?

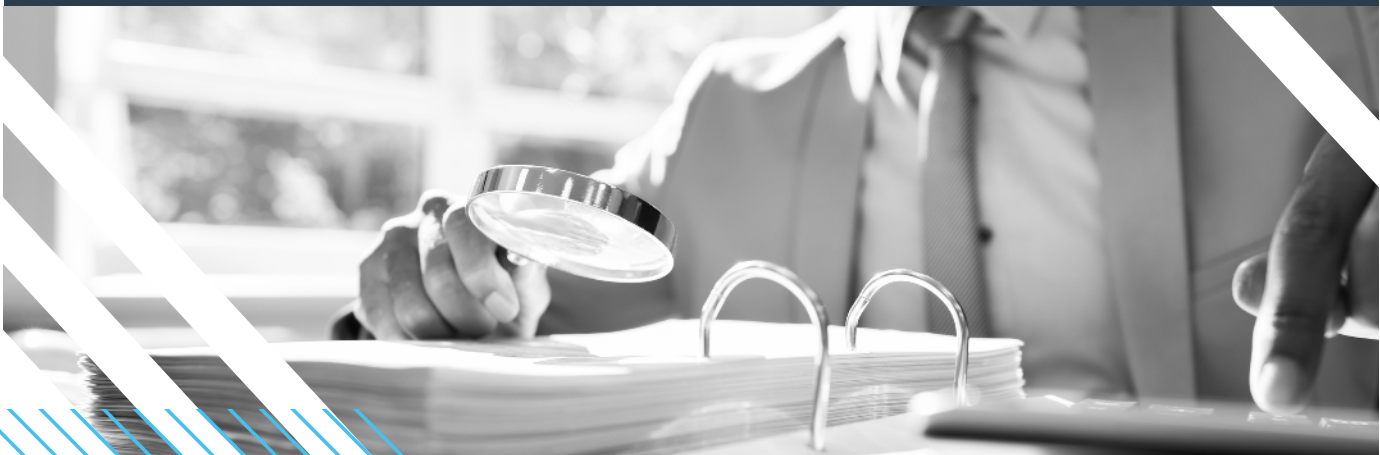
There are limitless reasons why people participate in fraudulent activity. But they can generally be boiled down to these three factors:

- » **Motivation** - Economic factors such as personal financial distress or overspending might prompt someone to commit fraud.
- » **Rationalization** - Sometimes people find a way to justify committing fraud. This can include perceived lower-than-deserved pay or the idea that they're simply "borrowing" from the organization and intend to return the money eventually.
- » **Opportunity** - If someone's access to assets and information convinces them they can get away with fraud, they're more likely to commit it.

10 Red Flags of Possible Fraud

Financial fraud can easily go undetected and be difficult to prove. However, you can help identify and prevent fraud by watching for these suspicious activities and troubling financial situations.

1. Your organization loses money year after year.
2. Payroll taxes aren't being paid timely.
3. Sales tax payments aren't being made timely.
4. Board meetings often include statements like, "Things always look good in the future." (You won't get a bank loan if you're losing money every year.)
5. All or most of your funding comes from one grant. (What if that one grant accounting for 75% of your business goes away?)
6. You're seeing significant turnover in your accounting department. (This could mean they're frustrated with your financial operations.)
7. Employees are being paid for overtime hours not worked, or timesheets are altered.
8. An employee has an excessive vacation balance. (It could mean they're worried that someone will detect their fraud if they're out of the office.)
9. You're undergoing an audit and can't find requested documents, or the documents appear to be altered or photocopied.
10. You see excessive credit memos in your general ledger and voided checks in your accounting system.



7 Tips for Preventing Fraud

Proper internal control systems give you a better chance of preventing or detecting fraud before it costs your organization big bucks. Implementing the following tips can help you avoid potential problems.

- 1. Conduct background checks before hiring CFOs or bookkeepers who will be responsible for handling the organization's money.** An accountant with a bad credit score is usually not the right person for the job. Thoroughly vet any person or company who touches your finances.
- 2. Implement segregation of duties.** No single individual should be responsible for receiving, depositing, recording and reconciling the receipt of funds. The same goes for authorizing payments, disbursing funds and reconciling bank statements.

When funds are received, have your receptionist or executive director make copies of all the checks. Or you could create a ledger that details the company or individual, check number, amount and date. Provide the ledger or check copies to a bookkeeper for recording purposes, and give them a copy of the bank receipt later for validation.

- 3. Increase controls over credit cards to prevent unauthorized spending.** An employee might use your nonprofit's credit card for personal expenses like gas, personal travel, meals or merchandise. Or maybe they make legitimate purchases for your organization, only to submit the expense for reimbursement (a practice called double dipping).

Fraudulent credit card use is common at nonprofits because it easily goes undetected if you're not vigilant. To prevent it, consider the following controls:

- » Limit the number of credit cards you issue, and make sure all authorized users have their own unique card. When an employee leaves your organization, collect and cancel all cards issued to them.
- » Review the electronic copy of the credit card statement, which cannot be altered. If you prefer paper statements, ensure they're delivered unopened to the person responsible for reconciling charges.
- » Insist on original receipts for all transactions, and compare them to transactions on your credit card statement.
- » Compare expense reimbursement claims to credit card charges.
- » Set the tone at the top. Let your employees know you're monitoring credit cards, and establish clear guidelines regarding their use.

7 Tips for Preventing Fraud (Cont.)

- 4. Use the lock down function in QuickBooks.** While QuickBooks is an effective accounting program, the data can easily be manipulated. However, the software can be set to lock down the prior period statements to avoid changes to these numbers.

Additionally, don't allow your CFO or bookkeeper to export financial reports and data into Excel as a substitute for software-generated financial statements. Data in spreadsheets can easily be manipulated.

- 5. Have a line of credit available for use when necessary.** Organizations with large program expenditures that are reimbursed through grants can easily run into cash flow problems. Having a line of credit will help minimize the potential for fraud when these issues occur.
- 6. Have an approved vendor list—and only allow payments to those vendors.** If you need to add vendors to the list, that process should involve more than one individual at your organization.
- 7. Provide your board of directors with detailed reports on financial activity every month.** Include a statement of financial position, statement of activities and a budget-to-actual report. This should be done for the overall entity and for any grants.

You don't have to be a CPA to have a general sense of your nonprofit's financial picture. If you're spending money, cash should go down; if you've collected revenue, cash should go up. Any deviation from that should be cause for concern (and increased scrutiny).

Paying close attention to your financial position—and implementing the proper checks and balances—will help your nonprofit reduce and prevent fraud.

