Mitigating fraud risk in nonprofits

Forensics Today

PwC perspectives on the newest risks drawing investigator scrutiny

pwc

- Nonprofit organizations can be vulnerable to fraud because they often have high-trust environments, more deferential boards, less mature antifraud controls and limited awareness of fraud risk, which can allow schemes to go unnoticed for months or even years.
- The impact can be devastating, as fraud diverts vital resources, disrupts operations and damages an organization's reputation — which, in turn, can undermine donor confidence and fundraising.
- To manage this risk, nonprofits should assess their vulnerabilities and implement strong antifraud controls, training, monitoring and response protocols.

Fraud is a growing threat across all industries but especially the nonprofit sector. Why? Nonprofits usually operate in environments of high trust with less oversight, they have the lowest rate of fraud awareness training compared to other sectors and their antifraud programs, if any exist, are often inadequate. Moreover, their employees' duties are sometimes not segregated, which can mean a single person has total, unsupervised control over a given process.

That can make them uniquely vulnerable to fraud. And once targeted, nonprofits typically suffer disproportionate harm, as their insufficient defenses allow fraudsters to continue operating undetected for longer periods. Losses include diversion of mission-critical funds, disruption of operations and damage to the organization's reputation. This, in turn, can threaten donor trust and the nonprofit's ability to raise funds.

Effective fraud defenses are therefore essential to a nonprofit's mission, governance and financial viability. To achieve resilience, nonprofits should implement adequate antifraud capabilities across their organization, including monitoring, training for board and staff, audits, crisis management planning, communications and incident response.

An array of fraud schemes and sources

Fraud touches organizations of all sizes, in all sectors. It originates both internally and externally, and can take many forms: embezzlement, corruption, financial statement fraud, procurement scams and – in the case of nonprofits – grantee fraud. In PwC's Global Economic Crime Survey 2024, nearly half (47%) of all organizations reported that they experienced fraud in the past two years.

Nonprofit fraud often occurs internally, sometimes on a small-scale involving theft or corruption by employees (skimming, check tampering, expense falsification, collusion with grantees, inappropriate interactions with foreign government officials and so on), but more advanced schemes by senior executives also happen. In rare cases, entire organizations have been corrupted so fully they've become a fraudulent enterprise that preys on donors.

Example: A large nonprofit perpetrated a massive telefunding fraud scheme for over ten years, collecting and misappropriating more than $110 million from donors nationwide. The defendants — owners, senior managers and related companies — bombarded consumers with 1.3 billion deceptive fundraising calls, most of them illegal robocalls. Federal and state authorities secured a settlement permanently banning the defendants from conducting fundraising activities and telemarketing of any kind, and imposing a $110 million judgment.

Fraud can also originate externally, through third parties such as vendors, suppliers or grantees.

Example: A nonprofit organization discovered a large drop-off in donations and a spike in donor complaints. After investigating, it learned that an overworked bank employee was discarding donations to the nonprofit that required manual processing (versus by a machine), resulting in over $50 million of uncashed donations over six months. The nonprofit relied on the bank to process a heavy volume of donations without conducting regular oversight and discovered the problem only after reviewing historical donation activity.

A growing sector with unique risks

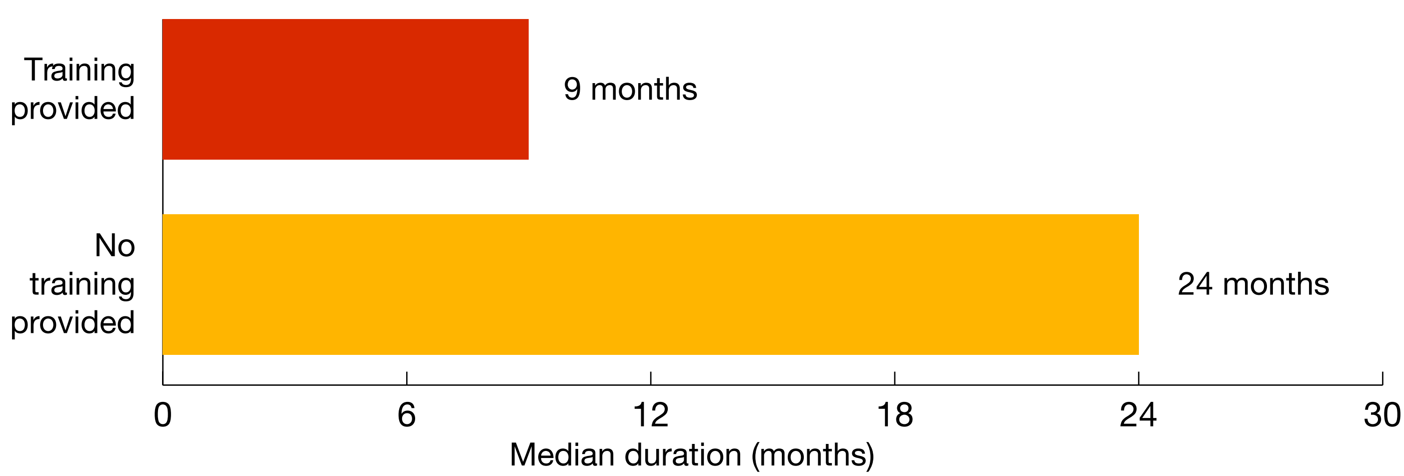
The United States is home to roughly 1.8 million nonprofits, according to a study by the Urban Institute. This number includes 501(c)(3) public charities, private foundations and a variety of membership and professional organizations. With expenditures of $1.94 trillion, charitable 501(c)(3) nonprofits account for roughly 75 percent of revenue and expenses in the sector.

The nonprofit sector is a major US employer, with an average annual workforce of nearly 12.8 million as of 2022, according to a report from the Center for Nonprofits, Philanthropy, and Social Enterprise at George Mason University's Schar School of Policy and Government. This amounted to 9.9% of non-government employment. Nonprofits added nearly 277,500 jobs between 2017 and 2022.

Why is this important to note? Board members of nonprofits — although fiduciaries — are also volunteers with careers, families and other time commitments that can make it difficult for them to stay engaged at a level to help the organization detect and mitigate fraud risks. This may be the first time they've served on a board and are still learning how they operate, including how to recognize warning signs of fraud or financial mismanagement. In many cases, they're volunteers and donors who place considerable trust in the organization's leadership teams and may not yet know how to properly question management or scrutinize financial activity or operational details to the same degree as a for-profit, compensated board. These conditions can foster a control environment that's more susceptible to fraud.

Another vulnerability can be the lack of fraud risk awareness. According to a report by the Association of Certified Fraud Examiners, nonprofits have the lowest implementation rate of fraud awareness training across all sectors. This training helps organizations uncover fraud quickly and limit the damage. Those without it experience nearly double the losses compared to their trained counterparts. Significantly, the report noted, fraud schemes in nonprofits typically go on for 14 months before detection.

Nonprofits that provided fraud awareness training uncovered frauds more than 2.5X times faster than those that didn't



Source: Occupational Fraud 2024: A Report to the Nations.

Fraud's ripple effect on nonprofits

The consequences of fraud can extend far beyond financial losses for nonprofits, striking at the heart of their mission and the trust volunteers and employees work so hard to maintain. Breaching this trust can devastate the organization. Each dimension of impact reveals the critical vulnerabilities nonprofits face.

- **Financial damage:** Fraud incidents can deplete resources that are important to achieving philanthropic goals. Funds meant for beneficiaries are siphoned away, forcing organizations to redirect time and money toward damage control rather than mission-driven work.
- **Operational disruption:** Fraud can halt ongoing projects and imperil long-term strategic plans. The recovery process — investigating the incident, addressing regulatory concerns and implementing new safeguards — diverts attention and resources away from core objectives.
- **Reputational harm:** A single fraud incident can undermine the trust of donors, beneficiaries and partners, often taking years to rebuild. Nonprofits rely heavily on their reputation to secure funding and support, making any loss of trust particularly devastating.
- **Fiduciary exposure:** Another risk is potential personal liability for board members who fail to exercise adequate oversight. Even without direct involvement, ignoring red flags or failing to ask probing questions may be seen as a breach of fiduciary duty, as all board members share collective responsibility for governance.

In addition to all this, nonprofits face increasing regulatory scrutiny. Heightened oversight and potential penalties from regulators underscore the importance of adopting strong antifraud measures and bolstering compliance alongside operational integrity.

Fraud not only threatens the financial stability of nonprofits but also jeopardizes their ability to fulfill their missions and serve communities. Addressing these risks is imperative.

A framework for fraud resilience

To combat this growing threat, nonprofits should consider a holistic framework that integrates both proactive and reactive measures to prevent, detect and respond effectively to fraud incidents. The following steps apply to organizations of all sizes and sectors, though nonprofits are less likely to have implemented them.

Proactive measures: Building a strong foundation

- **Conduct risk assessments:** Understand where your vulnerabilities lie by performing regular risk assessments to identify weak spots within your operations and across your grantee networks. These assessments should inform targeted strategies designed to address specific risks and reinforce overall resilience. Targeted risk assessment areas may include, for example:
    - » Access to, handling and managing cash
    - » Procurement and vendor selection
    - » Disbursements to grantees, vendors and other third parties
    - » Conflict of interest management
- **Establish guidelines and controls:** Develop clear guidelines and internal controls by setting transparent expectations for fund use, documentation and oversight. Build accountability into your processes and periodically review processes so they remain effective.
- **Implement fraud awareness training:** Empower your staff to act as the first line of defense by educating them to recognize potential fraud scenarios and understand the consequences of engaging in fraudulent activity. Board members, too, should receive targeted antifraud training to strengthen oversight and reinforce their role in detecting red flags.
- **Encourage whistleblower reporting:** Create a speak-up culture in which employees and stakeholders feel safe reporting suspicious activities without fear of retaliation. Provide a reporting hotline or mechanism that's accessible to employees and others external to the organization (e.g., donors). Periodically review employee and external complaints for patterns or red flags that may be indicative of fraudulent activity.
- **Strengthen monitoring practices:** Leverage forensic data analytics to flag irregularities in real time. Conduct regular site visits to confirm that grantees are adhering to agreed-on terms.
- **Develop a crisis action plan:** Designate a core response team composed of internal and external specialists, including legal counsel, forensic accountants and PR professionals. This team should be ready to act swiftly and decisively when fraud is suspected.

Reactive measures: Responding to fraud incidents

- **Manage incident triage:** Your crisis response team may need to temporarily pause operations after an incident to secure evidence, notify stakeholders and gather facts. Identify an incident coordinator to oversee these steps and create a focused, organized response.
- **Conduct thorough investigations:** Prioritize transparency throughout your investigation and adhere to ethical standards while also preserving attorney-client privilege when applicable. Engage external professionals when needed to help maintain credibility and objectivity.
- **Communicate with stakeholders:** Provide clear and transparent communication throughout the incident investigation process. Inform donors, regulators and the public of the situation and the steps you're taking to address it. Honest messaging can be key to rebuilding trust and demonstrating accountability.

Contact us

Ryan Murphy
Partner, Global Investigations & Forensics Leader, PwC US
ryan.d.murphy@pwc.com
LinkedIn

Amanda Cox
Principal, Financial Crimes Practice Leader, PwC US
amanda.cox@pwc.com
LinkedIn

Shea Fowler
Partner, National Higher Education & Nonprofit
Risk & Regulatory Leader, PwC US
shea.m.fowler@pwc.com
LinkedIn

www.pwc.com