Nonprofit Observer

Payment Card Industry Data Security Standards
Are you up to date on PCI compliance?

Tips for raising your board's financial literacy
Balance sheets and income statements made easier

Why fraud hotlines are critical for nonprofits

The good news about volunteers

SPRING 2025

Seward and Monde

Certified Public Accountants and Consultants

Over 100 Years of Service & Growth

Payment Card Industry Data Security Standards

Are you up to date on PCI compliance?

The Payment Card Industry Data Security Standards (PCI DSS) are designed to secure credit and debit card transactions and protect cardholder data. These standards apply to all organizations handling credit card information, including nonprofits that accept credit cards for donations, merchandise sales or other purposes.

The latest version of PCI DSS became effective in 2024, but most of the new requirements became effective on March 31, 2025.

Wide-ranging security standard

The PCI Security Standards Council is an independent organization established nearly 20 years ago by major credit card networks, including American Express, Discover, JCB International, MasterCard and Visa. Its primary goal is to enhance payment account data security and promote the global adoption of consistent data security practices.

PCI DSS standards apply to all entities storing, processing or transmitting cardholder or sensitive authentication data. This includes organizations of all sizes, regardless of the volume of transactions they handle.

12 core requirements

The current standards (PCI DSS v4.x) consist of 12 core requirements, each encompassing more specific rules, testing procedures and guidance. The core requirements dictate that covered entities must:

1. Install and maintain network security controls (firewalls) to protect cardholder data,
2. Employ secure configurations for all system components (replacing vendor-supplied defaults with unique passwords and settings),
3. Protect account data through encryption, truncation, masking and hashing,
4. Defend cardholder data by encrypting its transmission over open or public networks,
5. Protect all systems and networks from malicious software (for example, with anti-malware programs),
6. Develop and maintain secure systems and software,
7. Restrict access to system components and cardholder data based on "need to know" (staffers should be restricted to the least data necessary to perform their jobs),
8. Identify users and authenticate access to system components through unique identifiers and associated authentication factors, such as passwords, smart cards or biometric elements,
9. Restrict physical access to cardholder data and systems that store, process or transmit cardholder data,

10. Log and monitor all access to system components and cardholder data,

11. Regularly test the security of systems and networks to ensure security controls continue to reflect the changing environment and

12. Support information security with organizational policies and programs that inform all personnel of the sensitivity of cardholder data and their responsibilities for protecting it.

The latest updates added 64 new sub-requirements, including 51 that took effect on March 31, 2025.

Card network enforcement

Although the PCI Security Council promulgates the standards, it doesn't enforce them. That's generally left to the card networks. The networks establish their compliance requirements in terms and conditions, typically based on the number of transactions processed. The greater the number of transactions, the tighter the provider's requirements will likely be.

Noncompliance can prove costly. The network may impose substantial penalties or even prohibit you from processing card payments. Moreover, noncompliance could lead to data breaches, resulting in steep legal and mitigation costs, hefty fines and devastating reputational damage.

Best practices

Nonprofits often manage compliance by outsourcing it to online payment platforms or payment service providers — such as PayPal, Stripe or Square — and incorporating compliance in their service agreements. It's important to know that card networks will hold nonprofits liable for noncompliance if a provider falls short. In addition, nonprofits may need to submit a Report on Compliance (ROC) or complete a Self-Assessment Questionnaire.

Conduct thorough due diligence before selecting a provider to reduce the risk of noncompliance. Request examples of PCI ROCs and monitor a provider's compliance with its contract's security and compliance provisions and audit requests.

What if you don't use a provider for your credit card transactions? Be careful. If you handle cardholder data on your website or servers, you're responsible for complying with the PCI requirements issued by your card networks. Make sure your IT professionals are up to date on the new requirements.

Other standards

The PCI DSS may not be your nonprofit's only data security requirement. Organizations must also comply with other laws, regulations, and formal or informal standards that set parameters for protecting individuals' personal information. Of course, your nonprofit can only benefit from adopting more stringent safeguards than those mandated. ●

LOOK FOR 'SECURE-BY-DESIGN'

Credit card transactions aren't the only potential vulnerabilities nonprofits must address to safeguard their and their supporters' data and finances (see main article). Hackers and cybercriminals can exploit weaknesses in various software systems. Rather than focusing solely on whether your software providers satisfy various compliance standards, determine whether they adhere to the "secure-by-design" approach. This can reduce risk.

Software designed under the secure-by-design standard prioritizes customers' security as a core business requirement — rather than treating it as just a technical feature. Software makers that implement secure-by-design principles in the earliest design phase of a product's development lifecycle reduce the number of exploitable flaws before the product is introduced to the market for widespread use. Out-of-the-box software, for example, should include multifactor authentication, logging and single sign-on for no extra fee.

Tips for raising your board's financial literacy

Balance sheets and income statements made easier

A nonprofit organization's board of directors might include accountants, bankers or investment managers. It also might consist of business or community leaders with expertise in your nonprofit's niche or fundraising, marketing and publicity. How can you best share your financial results with those board members who aren't necessarily financial experts? We answer some common questions.

What are our primary information sources?

Generally, a nonprofit's financial situation is represented in two documents: a *statement of financial position* (balance sheet) and a *statement of activities* (income statement). However, providing long lists of numbers can dizzy readers. Remember, *how* you present the numbers to the board is just as important as the numbers themselves.

Instead of using a numerical format, employ graphs and pie charts to relay information. Whether through a bar graph, ratio or other means, there are effective ways to present financial data to nonfinancial board members.

What about the statement of financial position?

A statement of financial position shows an organization's:

- Assets (cash, accounts receivable, and property and equipment),
- Liabilities (accounts payable and long-term debt), and
- Net assets (with and without donor restrictions on resources).

You can use a pie chart to depict assets so board members can easily understand what portion

of total assets can quickly be converted to cash (such as cash equivalents and investments) vs. the portion that can't be rapidly converted (including property and equipment).

How should we present income statement information?

A statement of activities (or income statement) generally starts with total revenues and support. Then, program, management general expenses and fundraising costs are deducted to determine the overall change in net assets. A bar chart is a good way to present this information. It can compare current revenues and expenses with those of previous periods in a single image. By adjusting the bar graphs on, say, a monthly basis, nonfinancial board members can regularly compare revenues and expenses to the budget.

For example, you can create a bar chart showing how your annual event was funded last year with money from attendees, sponsors and general funds. This tool can help a board make quicker and better-informed decisions — in this case, about setting or readjusting funding expectations for this year's annual event.

What if revenues have decreased?

Your annual budget assumes a particular level of revenues and support. If you don't obtain specific grants or take in less for program services than anticipated, your board will need to revisit anticipated expenses and adjust figures accordingly. A graphic image is one way to call "heads-up" quickly.

Even though COVID-19 is mainly in the rearview mirror, the economy is still recovering from some of its effects. You may experience cuts in grants due to the lingering effects of COVID and other factors. Comparing ratios for the current year to the prior year can reveal whether these costs have been cut effectively. You can also compare total support and revenues to management and general expenses, program services, and fundraising expenses.

These ratios allow your board to see if your organization's costs and revenues are in line with its expectations, as expressed, for example, in your budget. Suppose your management and general expenses are $100,000 for the coming year, and your organization's total support and revenue is $1 million. That's a highly impressive (though not typical) ratio of 1:10 — 10% of every dollar earned is spent on administrative costs, with the remaining 90% available to fund programs.

What else?

To help your board with financial literacy, try bringing in outside speakers, such as investment advisors, bankers and accountants. Or, if you have financial professionals on your board, you might ask them to share tips and answer other board members' questions as they arise. If your board could use more financial expertise, contact us for potential recommendations. ●

Why fraud hotlines are critical for nonprofits

Nonprofits operate under intense scrutiny from many sources, including donors, regulators, watchdog groups and the communities they serve. A single instance of fraud can damage an organization's reputation, erode donor confidence and divert precious resources away from critical missions. Anonymous fraud reporting hotlines are, therefore, essential.

Discreet — and effective — option

According to the Association of Certified Fraud Examiners (ACFE), nonprofits lose an average of 5% of their annual revenue to fraud. In the 2024 ACFE *Report to the Nations,* the median loss when a not-for-profit experiences fraud is $76,000. Implementing proactive measures to prevent and address fraudulent behavior is paramount. The ACFE report says that adding a confidential hotline cuts the median loss of a fraud scheme in half and reduces its duration by about half.

Hotlines are effective because they provide a discreet way for employees, volunteers, donors and stakeholders to report suspected unethical or fraudulent activities. Unlike traditional reporting channels that may be hindered by fear of retaliation or organizational hierarchy, hotlines encourage whistleblowers to come forward without fear of retribution.

Possible benefits include:

Privacy and secrecy. Hotlines may reduce the fear of speaking up by offering tipsters the chance to report issues anonymously.

Early detection. Organizations that provide hotlines can minimize damages to their finances and reputation by halting schemes early on.

Demonstrating a commitment to responsible operation. A hotline represents a commitment to fraud prevention and ethical conduct.

In addition to a phone-based hotline, you may consider offering email and web-based reporting tools.

5 implementation tips

To maximize your fraud hotline's effectiveness, be sure to:

1. **Use a reputable service provider.** Third-party hotline services are available and offer neutrality and confidentiality of reports.

2. **Train employees and volunteers.** Staff, volunteers and others should learn how to use the hotline and the types of incidents or suspicions to report. Also, post signs in break rooms and other high-traffic areas publicizing your hotline.

3. **Set clear policies.** Procedures for investigating reports, protecting whistleblowers and addressing confirmed instances of fraud should be communicated.

4. **Get the word out.** Promote your hotline to other stakeholders, such as donors and vendors, by including information on your website and in newsletters.

5. **Review any reports and act swiftly.** Regularly review hotline reports, investigate them thoroughly and take appropriate corrective actions.

You may want to engage a forensic accountant to conduct interviews and collect evidence of fraud.

Real-world success

Several nonprofits have successfully leveraged hotlines to detect and deter fraud. For instance, a large international humanitarian organization uncovered misappropriation of funds in a remote regional office after a tip was submitted via hotline. Swift action resolved the issue and reinforced the organization's commitment to accountability.

In another case, a hotline report led a small nonprofit to identify fraudulent expense reimbursements by a staff member. Timely intervention saved the organization thousands of dollars and prompted a review of internal controls.

Bottom line

Fraud hotlines are invaluable for nonprofits seeking ways to protect their assets and uphold public trust. By providing a safe, anonymous channel for reporting, you can enhance your organization's fraud prevention strategies, strengthen stakeholder confidence and help ensure staffers remain focused on your mission.

The good news about volunteers

Most nonprofit organizations operate on lean budgets, making volunteers essential. But what's one hour of volunteer time worth? The latest research by Independent Sector and the Do Good Institute produced a *Value of Volunteer Time* report, which estimates that one hour of volunteer time is worth $33.49. That's a 5.3% increase from the previous year, 2022.

VolunteerMatch, a member of Independent Sector, offers a study that provides additional perspective: Each volunteer contributes an average of 52 hours annually. Multiplying the average annual hours by the estimated value per hour ($33.49) equates to nearly $1,741 per volunteer each year. Of course, specialized volunteers, such as accountants or attorneys, can deliver even greater value.

On the rise again

The COVID-19 pandemic significantly impacted many aspects of life, including volunteerism, as nonprofits paused efforts to recruit in-person help. However, volunteerism is rebounding. According to AmeriCorps and the U.S. Census Bureau's publication *Volunteering and Civic Life in America,* charitable engagement has risen sharply. Although just over 60 million Americans volunteered in 2021, that number soared to nearly 76 million in 2023 — the most significant increase in over 20 years.

In 2023, 28.3% of Americans volunteered, contributing close to 5 billion hours through organizations. According to AmeriCorps, the federal agency for national service and volunteerism, this effort carried an economic value of $167.2 billion.

Lowdown on virtual help

The latest research from AmeriCorps includes something new: Virtual volunteering was measured for the first time. During the review period

(September 2022 through September 2023), 13.4 million individuals engaged in virtual or hybrid volunteering. These volunteers tend to be a bit older, averaging age 49, as opposed to in-person volunteers, whose average age is 46.

Also, the virtual and hybrid volunteer participation rate among those with disabilities was 20%, compared to 18% for others. This suggests that people with disabilities prefer virtual and hybrid services.

Final takeaways

Whether your team consists entirely of unpaid volunteers or includes just a few dedicated individuals supporting your paid staff, each volunteer is invaluable. And let's face it — you could likely use even more help. Not all volunteering is formal. Many Americans lend a hand in informal ways — for example, by helping neighbors — a trend that continues to grow.

The bottom line is to know how people prefer to contribute, whether in person, virtually or through a hybrid approach. This information will help you better tailor your volunteer program to those eager to lend a helping hand. ●