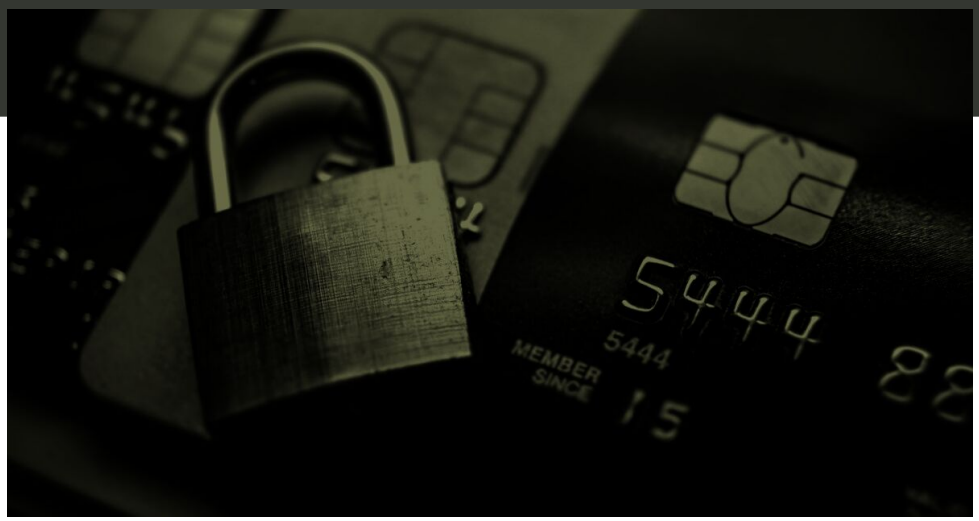
GENERAL

Tips to Protect Your Nonprofit from Credit Card Fraud

04.19.19 | Linda J. Rosenthal, JD



More than a few nonprofit organizations operate on the assumption that they are relatively safe from fraud or theft not just by outsiders but from trusted insiders as well. As statistics show each year, this belief is incorrect and dangerous.

In more than a handful of previous blog posts, we've highlighted this persistent danger. See for example: **Charity Embezzlement: Thwart It With Good Controls**; **Nonprofits Beware: Pfishing Trips**; and **Charity Fraud: Secret Billing Schemes**. Nonprofit groups must learn about fraud prevention with special emphasis in the ways that criminals target the charitable sector.

Credit Card Vulnerabilities

A particular area of risk that persists is the use of credit cards. Despite the introduction several years ago of the chip technology now featured on most cards, there are **still vulnerabilities**.

Chip-based cards and the accompanying card readers are, indeed, **safer** than before. They are "dynamic" and data is changed with each use. The earlier magnetic-strip cards that remain in a static stage are more prone to copying.

According to credit-card giant Visa, the introduction of the newer card technology has resulted in a **70 percent decrease** in fraud, but the effect is restricted to in-person payments. The benefit of the chip technology evaporates in the case of **online credit card transactions**.

The popularity of online financial transactions is accelerating; more consumers are making this choice. This trend, as well as an alarming number of **security breaches** in all sectors has created a

significant jump in the prevalence of online credit card fraud.

In recent years, partly as a result of demand from savvy donors, more and more organizations have created and encouraged online, electronic, charitable giving opportunities.

There are **two particular vulnerabilities** in connection with this new donation route. First, a credit card hacker will use stolen information to make a donation on your website for various reasons including "card testing." A "bot" may spam your donation page with transactions "every few seconds, looking for a credit card hit." The numbers being tested may be just "random number combinations and sequences" instead of numbers from stolen credit cards. The card-testing method is used so that the criminals can search for information "pending the acceptance of the card payment. If the credit card payment is accepted," it is tagged as a valid card number that can be sold to others for use in unrelated fraud schemes.

Second, a criminal can engage in "refund fraud," where a significant online contribution is made with a stolen credit card, followed by a call to the organization that the donation was a mistake. For instance, the caller says that he or she "accidentally donated $2,000" when the intent was to give just $200. Then a request is made to refund the erroneous amount to a different card.

Safeguards Against Credit Card Fraud

There are important precautions that can be put in place to minimize a nonprofit organization's risk of online fraud, including adopting systems safeguards and careful monitoring practices.

System Controls

Adopting practices that permit the organization to uncover and prevent fraud can dramatically minimize risk. There are **payment systems** available that monitor and decline transactions that are suspicious; one example is the **Advanced Fraud Detection Suite** from Authorize.net.

In addition, the organization should **ask for the security code** for any credit card offered. Known as "CVV," it is the familiar 3- or 4-digit number on the front or back of most credit cards. "This helps to show that the cardholder is actually physically possessing the card at that moment."

Another important safeguard is to **use an "address verification system"** known as AVS. It verifies that the person using the credit card is aware of the correct address. But legitimate donors using their own cards can make mistakes and AVS doesn't work well for addresses outside of the United States. An extra level of protection is to have "error messaging specific to AVS issues" on the organization's donation page.

Another important practice called "rate throttling" is to **"limit the number of transactions"** that can be sent by a single computer in a designated period of time; for instance, in an hour. This minimizes card testing in which bots may submit many contributions from the same computer in rapid succession. Similarly, use "hold transactions for review," especially for any that exceed the maximum number of allowable donations; include an on-screen message to that effect. That way the card testers won't know if the card being tested is accepted or declined, and should discourage them from targeting your organization further.

Monitoring Vigilance

As a complementary safeguard to the systems controls, to the extent feasible, **monitor your organization's credit-card processing**. This includes setting up email alerts about suspicious transactions and designating a staff member to follow-up. "A word of caution: make sure to respect the balance between vigilance and paranoia, as you do not want to frustrate your legitimate, innocent donors."

*Extra **Step***

For organizations that are plagued by relatively heavy card-testing attacks, "deploy **reCaptcha** as **another safety measure**" at least on an intermittent basis. But avoid the types of reCaptcha features that seriously annoy most people – like offering a hard-to-read code that is difficult to duplicate. You don't want to have donors give up in frustration.

Conclusion

Nonprofits may be **unaware of the types of threats** that online credit card use may pose to them, particularly if they are a small group with limited personnel and budgetary resources. But the consequences of this pernicious type of fraud are significant enough that they should adopt adequate safeguards commensurate with the threat.