White Paper

Credit Card Fraud Protection for Nonprofits

iATS payments by deluxe

CONTENTS

Donors Should Be Able to Donate Securely | **3**

Types of Fraudulent Credit Card Transactions | **4**

Increasingly Sophisticated Fraud Attempts | **7**

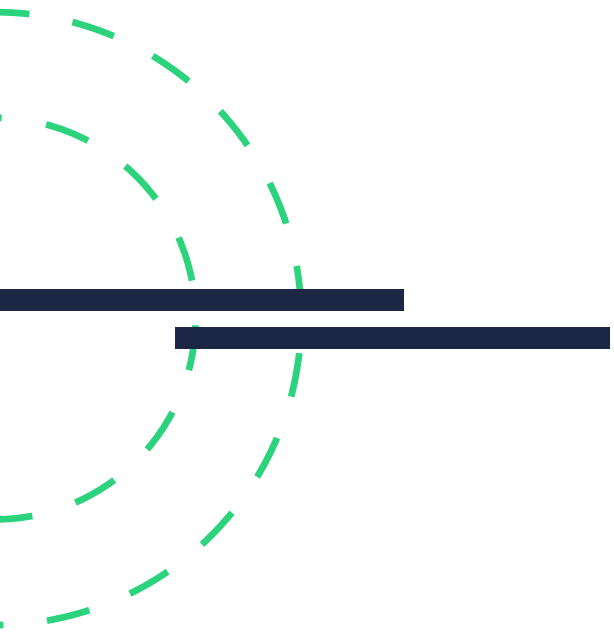
Impact of Credit Card Fraud on Nonprofits | **8**

PCI Compliance and Its Role In Preventing Fraud | **9**

Steps You Can Take To Minimize Risk | **10**

Choosing the Right Payment Processor | **13**

About iATS Payments | **14**



iATS payments by deluxe

DONORS SHOULD BE ABLE TO DONATE SECURELY

Nonprofits try to have a positive impact in their communities by directly serving their missions and raising awareness for causes.

To do so, they need robust online fundraising efforts. However, these efforts can be undercut by fraudulent activity.

The growth of online fundraising is accelerating each year. **68% of total charitable giving** in 2018 in the U.S. came from individual donors, and over half of donors worldwide preferred to pay online via credit card. In 2020, overall revenue raised online **grew by a further 23%**.

Without online donations, your nonprofit would not be able to function. For this reason, your donors should be able to donate securely.

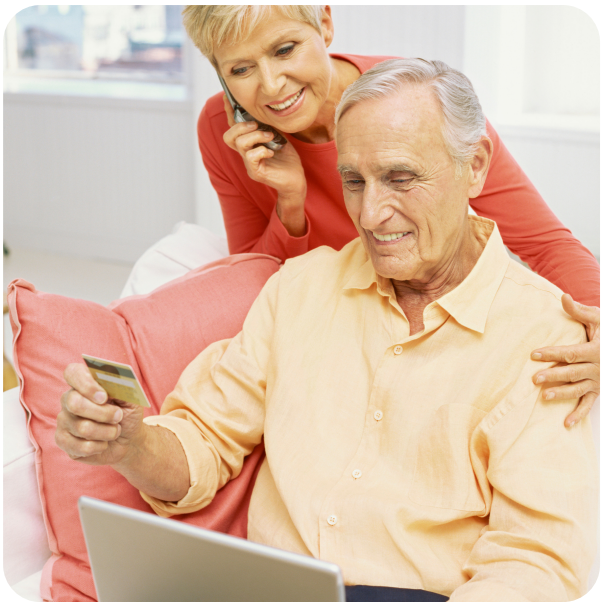
Organizations can experience significant losses of funds meant to support people in need if affected by malicious attempts to steal money. They can also suffer from long-lasting reputational damages, making it difficult to attract new donors.

Given the economic damage done by the pandemic, maintaining good relationships with donors has become even more critical.

69% of nonprofits think fraud is a significant risk to the nonprofit sector, and 85% think they are doing everything they can to prevent fraud, but almost **50% do not** have best-practice protections.

As a nonprofit, it is your responsibility to make sure safety measures are in place.

To protect your organization and donors, you need to be aware of the risks your nonprofit could face from different types of fraud.



TYPES OF FRAUDULENT CREDIT CARD TRANSACTIONS

Your nonprofit can fall victim to several different and unique types of fraud, including external risks and fraudulent activity that occurs from within the organization.

In fact, the American Certified Fraud Examiners (ACFE) found nonprofits experience a **median loss of $75,000** from fraudulent activity.

In this white paper, we focus on payments fraud that affects online transactions. You need to look out for the following types of credit card and ACH fraud:

→ ACH Fraud

Also called direct debit payments, ACH payments are an alternative to credit card payments that remove money directly from an individual's bank account.

ACH payments offer the following advantages to nonprofits:

- **Lower overhead**

There are fewer fees associated with processing ACH payments than with credit card payments. When you conduct an ACH transaction, your organization incurs a single flat fee. When donating with a credit card, you are charged a flat fee and a percentage of the transaction, both of which vary based on the type of credit card used.

- **Convenience**

All you need to conduct an ACH payment is an individual's bank account routing number. Nearly everyone has a bank account. When soliciting donations, it is important to appeal to as many potential donors as possible, so it makes sense to **accept payments** via a medium most people can use.

- **Recurring donations**

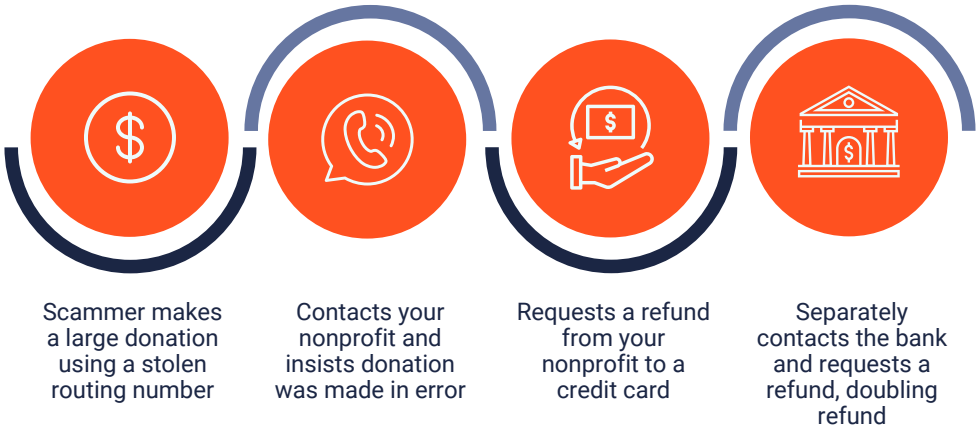
ACH payments are especially popular with nonprofits because they can easily be used to set up a recurring donation schedule. Because of their low overhead and convenient setup, many nonprofits are now encouraging recurring donors to give via ACH payments.

However, because nonprofits are increasingly using ACH payments **for fundraising**, scammers have taken note. Fraudsters can steal an individual's bank account routing number through phishing or database hacking. This is how the scam typically plays out:

- First, they will make a large donation using the stolen routing number.
- The next day, they will contact your organization and insist that the donation was an error. For example, they might say they intended to donate $10 but accidentally wrote $1000 or say that they did not authorize a donation at all.

ACH Phishing Scams

A step-by-step guide



- After making their claim, they will request a refund to a credit card or via check.[3]
- They will also contact the bank associated with the routing number and state that the nonprofit withdrew an unauthorized donation, requesting a refund.

This way, they have doubled the amount of the fraudulent refund. Because it can yield such high returns, nonprofit ACH scamming has become popular with online thieves, and you need to take note of it when protecting your organization against fraud.

→ Donation Form Fraud

Many scammers use online donation forms to test out stolen credit card numbers. Because some nonprofits prioritize ease of use over cybersecurity when creating donation forms, they inadvertently make it easier for thieves who want to test multiple stolen numbers in quick succession.

Donation form fraud involves requesting refunds for false donations made by the scammer. The con typically plays out like this:

- First, thieves will use your donation form to verify the validity of the card number they have stolen. They might attempt dozens of small donations using different cards; once one goes through, they know they can use it to complete their scam. This process is known as card tumbling.
- Next, they will make a false donation and request a refund in the same way an ACH fraudster would.

What mainly differentiates donation form fraud from ACH fraud is that it is easier to spot before it happens but can cost you more if a thief slips through the cracks. After the refund is processed, you will likely be charged a chargeback fee once the bank realizes the transaction was fraudulent.

→ Creation of Clone Charities

Another way fraudsters target nonprofits is by creating a clone of a legitimate charity, setting up accounts in their name and soliciting donations to this illegitimate copy of the actual organization.

The result is donors give to what they think is the legitimate organization, but the money goes to the account of the fraudster, who typically disappears soon after. The legitimate charity suffers the consequences of the fraudulent activity because the organization's reputation is damaged.

This is an especially common type of fraud, and similarly, criminals also set up fake charity auctions. Since donors pay for these items themselves, they cannot always be reimbursed, and items may or may not have a return policy.

While annual audits can help nonprofits uncover major cases of fraud, most of the time, this is not the case. Charities need to establish a rigid system of checks and balances to ensure they do not fall victim to internal or external fraud.

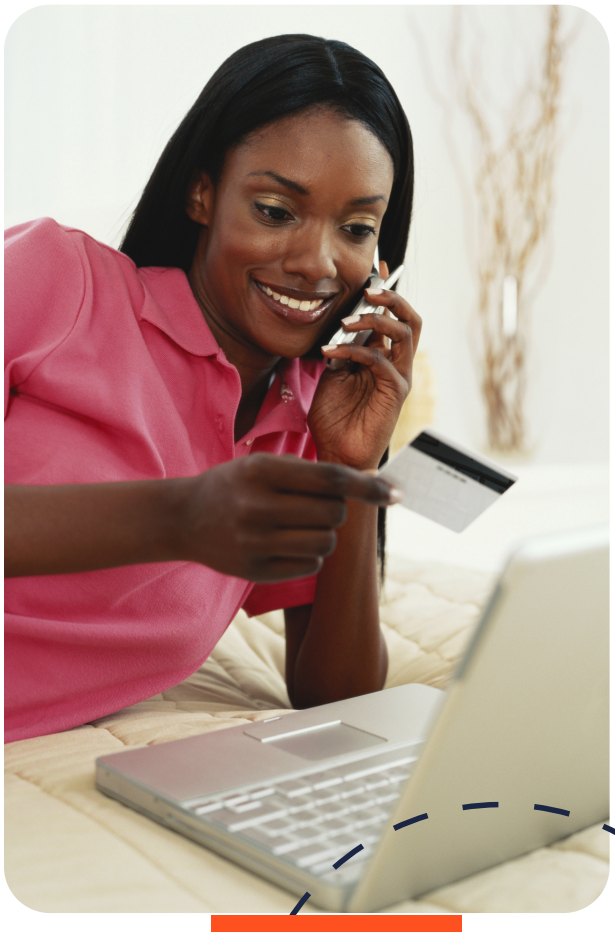
Processing suspicious transactions

Your nonprofit may be contacted by someone who claims they will make a large donation, but only if you send half the donated amount to another charity, which turns out to be a personal bank account.

This involves your nonprofit in money laundering, and the transaction is typically made with a stolen or compromised credit card. In addition to lost funds, your nonprofit could potentially encounter high litigation costs to defend itself against money laundering charges.

Warning signs of this type of activity include unusually large amounts, the 'donor' setting conditions of how the gift will be made, complex transfer arrangements and a donation that is actually a loan.

If the donor starts asking for an atypical donation process, the transaction should be flagged as potentially fraudulent. Your nonprofit should never move its own funds to another bank account to receive a large donation.



INCREASINGLY SOPHISTICATED FRAUD ATTEMPTS

Card tumblers gain information by focusing on the rules and math of how credit card numbers are created. Typically, once they have a credit card number, they test them online for validity and if one works, they use it on sites that don't verify information such as the name and security code on the card.

However, increasingly sophisticated card tumbling methods mean that fraudsters don't even need card details anymore. Hackers can write algorithms to create thousands of possible credit and debit card numbers from scratch. Your donors' credit card numbers can be targeted completely by chance.

Too many organizations, including charities, still do not require three-digit security codes to process transactions and this places them at risk for this type of online payments fraud.

Nonprofit organizations tend to have fewer anti-fraud measures in place, leaving them more vulnerable to payments fraud. If the rightful owner of a card number disputes charges, they must be refunded. This is known as a 'chargeback', and often incurs a fee.

Organizations end up losing revenue for donations they cannot use to support their causes.

IMPACT OF CREDIT CARD FRAUD ON NONPROFITS

Your nonprofit depends on donations to stay in operation and support its cause. This means financial losses from returning funds and paying chargeback fees are especially significant. Any percentage of revenue lost annually is money your nonprofit cannot use to further its mission.

Since nonprofits depend on donor support, the reputational damage from incidences of fraud can be extremely costly. It will be more difficult for charities to attract new donors if they have publicly suffered significant fraudulent activity.

Additionally, fraudulent activity is bad for internal business operations. Credit card fraud can disrupt the inner workings of a nonprofit and lower employee morale. Disengaged workers will not contribute as much effort, which can make it difficult for your organization to get back on track.

PCI COMPLIANCE AND ITS ROLE IN PREVENTING FRAUD

The Payment Card Industry Data Security Standard (PCI DSS) requires all organizations that process, store or transmit credit card information to adhere to a set of guidelines to maintain a secure environment. This creates an actionable framework to ensure safe handling of donors' credit card information.

PCI compliance enables prevention, detection and appropriate handling of incidents, which is highly valuable to nonprofits. Maintaining this certification can help build donor trust in the security of their financial information.

STEPS YOU CAN TAKE TO MINIMIZE RISK

Just because thieves might target your nonprofit for payment fraud does not mean there's nothing you can do to protect your organization and donors. Here are a few core strategies to prevent thieves from successfully targeting you.

Improve Password Security

Your passwords should be unique and securely stored to prevent them from being cracked. Ideal passwords are long and contain symbols, numbers and upper and lower-case letters. You should also enable multi-factor authentication for password resets wherever possible.

You should use password managers, which not only store passwords securely, but can assist in generating strong passwords and ensure you don't reuse passwords across sites. Here are some password managers you could consider.

Beware of Phishing Emails

Emails asking you to click on links or attachments and provide personal information can be used by fraudsters to install malware and gain access to sensitive information. Fraudsters can also pose as your nonprofit and solicit donations from well-meaning constituents. You should take the following steps to mitigate your risk –

- Carefully review the email for poor spelling or grammar and the email address for errors
- Do not click on any links or attachments. You can hover over them to ascertain if they are genuine
- Separately contact the organization that sent the email to confirm its authenticity

Monitor Your Merchant Services Account

To better spot donation fraud, you should check for multiple donations with small, random amounts that occur over a short period. Such transactions are often made using the same name for many different card numbers.

To protect against fraud, your nonprofit could require a minimum donation amount and CVV2 for online transactions. You could even enable Captcha in your online donation form. If you use an online form vendor, work with them to ensure you're protected. iATS Payments works exclusively with nonprofit organizations, and our fraud tools are built to suit your needs specifically. Our free and easy-to-use protection tools prevent over USD 48,000,000 in potential losses from fraudulent transactions every year.

We offer the following free and easy-to-use protection tools -

- Address Verification System (AVS)
- Bank Identification Number (BIN) Blocking
- Card Verification Code Requirement Capability (CVV2)

$48m

Our free and easy-to-use protection tools prevent over USD 48,000,000 in potential losses from fraudulent transactions every year

- Card Number Tumbling
- IP Blocking
- IP Velocity Checking
- Minimum Transaction
- Limit Name Tumbling

Make Sure Donors Have Access to the Card They are Using [3]

Most credit card thieves do not have stolen physical credit cards on hand. In most cases, they gain access to the card number and know very little about the cardholder or their card. For this reason, you can usually weed out fraudulent donations by making it harder to use card numbers illegally:

- **CVV2 verification**

A card's CVV2 number is the short code found on the back of a credit card. Require that online donors input this number when entering their card information, and you will likely eliminate fraudsters who do not have access to the code.

- **Address verification**

An address verification system (AVS) verifies a donor's billing address with the address their bank has on file. This verification can be done in seconds, and if the thief does not know the correct address, he will not be able to proceed with the scam.

- **Verify the Cardholder's Identity**

Another way to make it harder for scammers to successfully target your organization is to require that donors verify their identity before completing a transaction. Here are a few steps you can take to verify a donor's identity:

- **BIN/IP address verification**

Included in every card number is information identifying the cardholder's bank, called the Bank ID Number (BIN). When processing a donation, compare your donors' regional IP address against their BIN. If they are making their donation from a different country than their IP address, this could be a red flag.

- **2-factor authentication**

You can also confirm a donor's identity using a 2-factor authentication process. Before completing a donation, the user will have to verify their identity via SMS or another communication platform.

- **Make Your Donation Form More Sophisticated**

Many nonprofits shy away from using sophisticated donation forms online because they do not want to make it harder than they have to for donors to complete a donation. However, the more simplistic your donation form, the more likely it will be exploited by scammers.

You can make your donation form more secure by using these two strategies:

- Require a minimum transaction amount
- To prevent refund fraud tactics, you can require a minimum donation amount before completing a transaction. This might seem counter-intuitive, but most donors usually give more than $15 when they donate. If you do not accept small donations, you will not miss out on much.

- **Use encryption/tokenization**

With encryption and tokenization, donors' payment information is turned into a code that only your payment processor can read. If thieves hack your data, they will not be able to extract a donor's information.

- **Enable CAPTCHA**

CAPTCHAs are automated tests designed to block automated bots. Fraudsters sometimes try to use bots to test stolen credit card numbers. Using CAPTCHAs on your online donation forms will give you an additional line of defense against fraud attempts.

Note: Fraud prevention and protection strategies[3] evolve quickly to counter advances made by online scammers. Don't content yourself just with what security measures work now. Think of fraud protection as a continuous process that you can always improve.

While these are measures you can take to protect your nonprofit, there are some things most nonprofits do not have the expertise or resources to accomplish. This makes choosing the right payment processor for you of the utmost importance.

CHOOSING THE RIGHT PAYMENT PROCESSOR

Payment processors are online platforms that facilitate transactions.

Regardless of whether you already have a payment processor (you do if you already accept donations online), it is always helpful to consider what makes a payment processor the right fit for you.

Here are some of the essential fraud protection attributes you should look for in a payment processor:

→ PCI Compliance

These rules and regulations ensure that payments are secure, and that cardholder data is protected from scammers. Failure to abide by these standards can lead to your nonprofit facing fines between $5,000 and $500,000.

→ Data Portability

Whatever data your platform saves on your nonprofit and your donors should be portable, meaning that you can transfer your donor data to a different platform if you choose to leave. You do not want to be held hostage to a platform that you might outgrow or lose all your data if the platform is compromised. Some payment processors, such as iATS Payments, will securely transfer PCI-regulated data like credit card numbers, whereas others will not do so. Failure to transfer credit card data means that your donors will have to register again to donate.

→ 24/7 security assistance

Your platform should provide reliable 24/7 security assistance if an attempt at fraud is ever made on your site. You can put forward all the security measures in the world, but if you do not have a dedicated team to solve issues as they arise, you will still be vulnerable to fraud.

→ Experience with nonprofits

Experience with nonprofits is the most important feature to look for when choosing a payment processor. As discussed before, nonprofits are uniquely vulnerable to online fraud, and your payment processor should be aware of the threats your organization faces.

Working with a payment processor that understands the unique challenges faced by nonprofits saves time and money, allowing your nonprofit to focus on its mission.

While fraud protection for nonprofits is always necessary, now is the time to ensure you have protected your organization's donations and can safely and securely accept donations.

ABOUT iATS PAYMENTS

You work hard to raise money – accepting it should be effortless and secure. With over 20 years of serving the nonprofit sector, we know that the needs of nonprofits are different.

With our technology and deep knowledge of the sector, we provide the totally reliable and secure payment processing your organization needs to run smoothly and efficiently while keeping your donors protected.

LEARN MORE

iATS payments by deluxe