CharityEngine®
Powering the good to be great.

# Nonprofit Payment Processing

## Understanding The Basics

# Contents

# 1 Nonprofit Payment Processing Understanding The Basics

## Introduction

Your nonprofit relies heavily on donations in order to succeed. You probably recognize that payment processing services take a small percentage of your donation profits. But have you ever really stopped to consider why that is? Knowing the basics of payment processing for nonprofits can help you better understand what happens when you receive a donation and make decisions when investing in software solutions. This guide will help organizations like yours make the best decisions regarding online donations.

### 3 Keys To Nonprofit Payment Processing

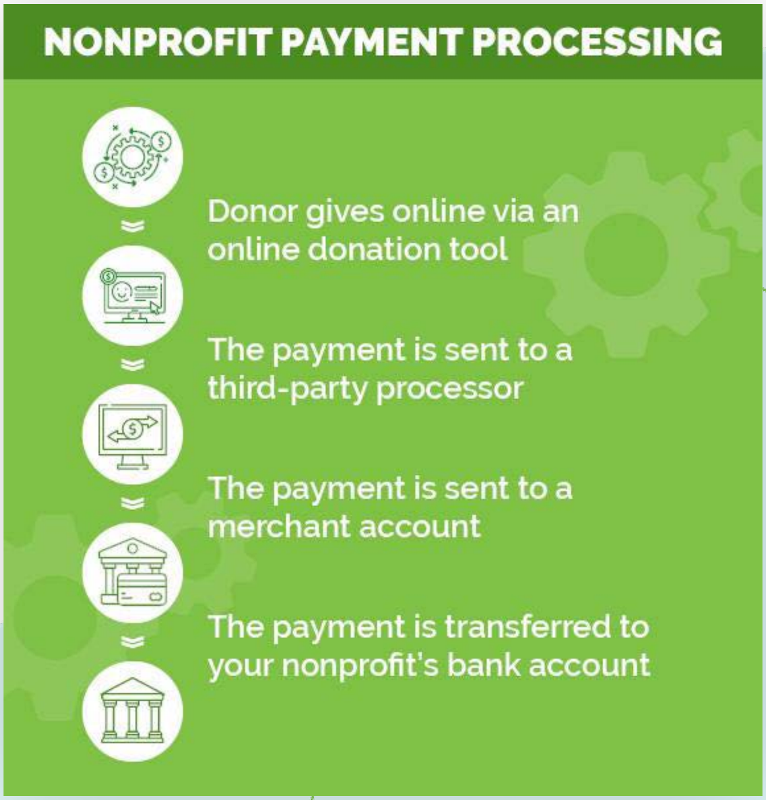
- Nonprofit Payment Processing Glossary
- VERSUS: Comparison Of Elements
- Ensuring Security Of Donations

## Let’s Start With the Obvious Question

What is nonprofit payment processing? Nonprofit payment processing describes each step that occurs from the time when a supporter provides their credit card information until the money is deposited into your nonprofit’s bank account.

**This process looks something like this:**

- First, your donor gives online via an online donation tool.
- Next, the payment is sent to a third-party processor or aggregator.
- Then, the payment is sent to a merchant account.
- Finally, the payment is transferred to the nonprofit’s bank account.



NONPROFIT PAYMENT PROCESSING

Donor gives online via an online donation tool

The payment is sent to a third-party processor

The payment is sent to a merchant account

The payment is transferred to your nonprofit’s bank account

## Ready To Dive A Little Deeper?

Let’s define some key terms related to payment processing for nonprofits.

# Nonprofit Payment Processing Glossary

**Merchant Account**: A merchant account is an in-between account where funds are transferred from the donor's account after they give but before being deposited into your nonprofit's account. This account is one of the key aspects of payment processing that allows organizations to accept donations.

**Aggregator**: An aggregator is a type of payment processing service. This type of service processes payments through a single merchant account for all contributions. This means that all nonprofits who use the same aggregator also use the same merchant account. They provide ease-of-use, but not much customization, flexibility, or speed. PayPal is a very common example of an aggregator.

**Payment Processor**: A dedicated payment processor is similar to an aggregator because it helps facilitate payment processing. However, a dedicated payment processor sets up a different merchant account for each of its customers. They typically provide faster processing and more flexibility for users.

**Payment Gateway**: While the terms payment gateway and payment processor are frequently interchanged in conversation, they are different steps in the process. A payment processor collects and transmits payment information, while a payment gateway uses a series of encryptions to securely authorize the transaction before it moves forward.

**PCI Compliance**: The Payment Card Industry created a series of standards for companies to uphold in order to process payments safely. PCI-compliant processing services adhere to these guidelines and internally check their processes with a self-assessment to avoid violations.

**PCI Certification**: A step above compliance, PCI certification requires a rigorous process and a comprehensive audit by a qualified security assessor to ensure all of the proper security measures are taken while processing payments.

**Virtual Private Network**: A virtual private network (or VPN) uses encryptions to ensure internet security during payment processing. It's used to keep payment data in the hands of the right people and to prevent fraudulent payments.

# A Comparison Of Elements

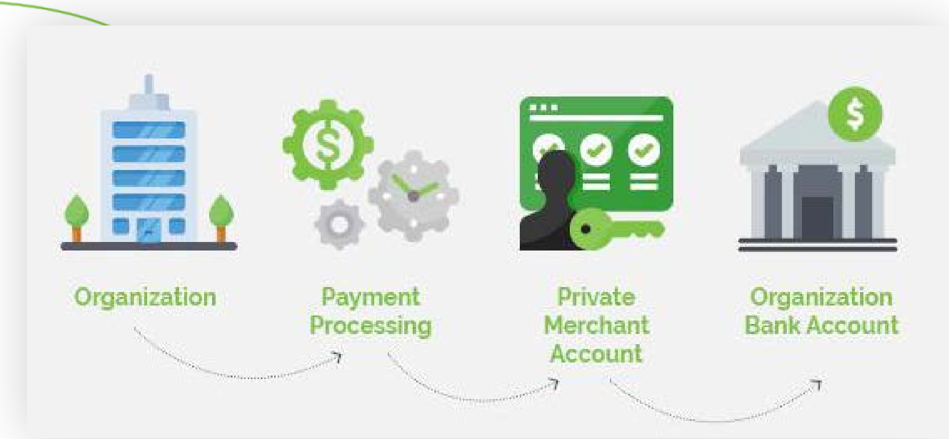
Some of the terms above can seem somewhat similar to one another. And they even serve similar purposes! So making the distinctions between these similar terms is key for your nonprofit to make the best decisions when investing in software.

The comparisons we'll cover include payment processor vs. aggregator, PCI compliance vs. PCI certification, and payment processor vs. online giving tool. Let's get started.

## Payment Processor vs. Aggregator

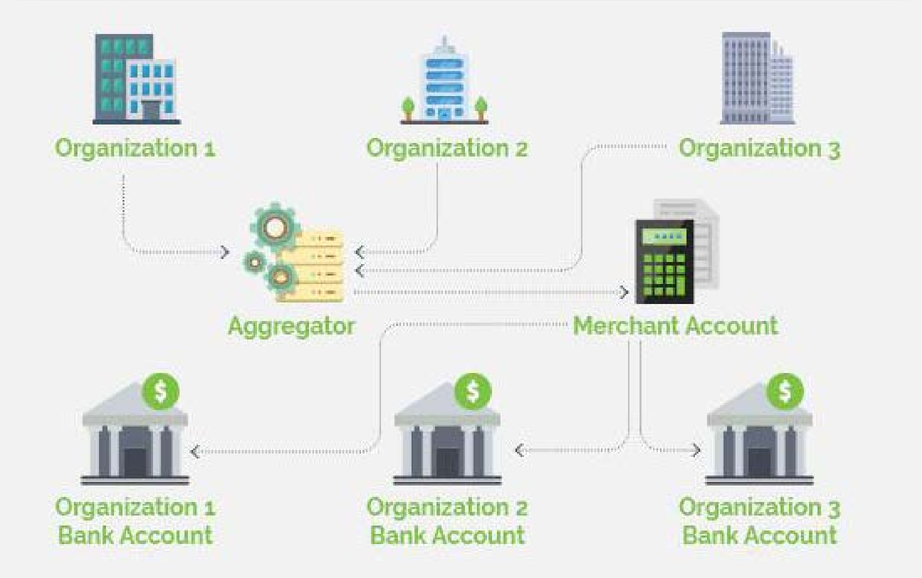
Payment Processors and Aggregators both work as the intermediary to transfer data and funds from your donor's bank account to your nonprofit's bank account.

The primary difference between these two nonprofit payment processing methods is the use of the merchant account. Therefore, the processes look somewhat different. Also, organizations that use the same aggregator also share the same merchant account.



## Payment Processors

First, the donor provides their credit or debit card information on your nonprofit's online giving page. Next, that data is sent through the payment processor's gateway to the individual merchant account that the processor has set up for your nonprofit. Then, the merchant account holds the donation amount while the payment processor verifies the payment information. Finally, the donation is transferred from the merchant account to your nonprofit's bank account.


Organization 1
Organization 2
Organization 3
Aggregator
Merchant Account
Organization 1 Bank Account
Organization 2 Bank Account
Organization 3 Bank Account

## Aggregators

First, the donor provides their credit or debit card information on your nonprofit's online giving page. Next, that data is sent through a payment gateway to an aggregator-controlled merchant account. This account is shared by all of the aggregator's clients. Then, the merchant account holds the donation amount while the aggregator verifies the payment information. Finally, the donation is transferred from the merchant account to your nonprofit's bank account.

# Our Preference?

## Dedicated Payment Processors

Both types of payment processing systems will get your donations from point A (your donor) to point B (your nonprofit).

*However, we tend to recommend dedicated payment processors for most organizations.*

## Why?

**Dedicated payment processors offer more personalized services.**

For instance, if something were to go wrong and there was a data breach regarding your aggregator (scary, we know), the aggregator will have all of their clients to respond to, limiting the one-on-one attention your organization receives.

However, if something were to happen to your account, you're more likely to get personalized assistance from a dedicated payment processor because you have an individual account with them rather than a shared merchant account.

Plus, dedicated payment processors have fewer interruptions to their processing activities for your nonprofit's donations, speeding up the process.

**This leads to a faster payout and less room for error.**

# PCI Compliance and PCI Certification

PCI compliance and PCI certification standards have the same objective in mind: to keep payment information and donor data safe. Both standards are set by the Payment Card Industry to best handle credit card data. However, there are certain differences your nonprofit should know about before you make your investment in a payment processing solution.

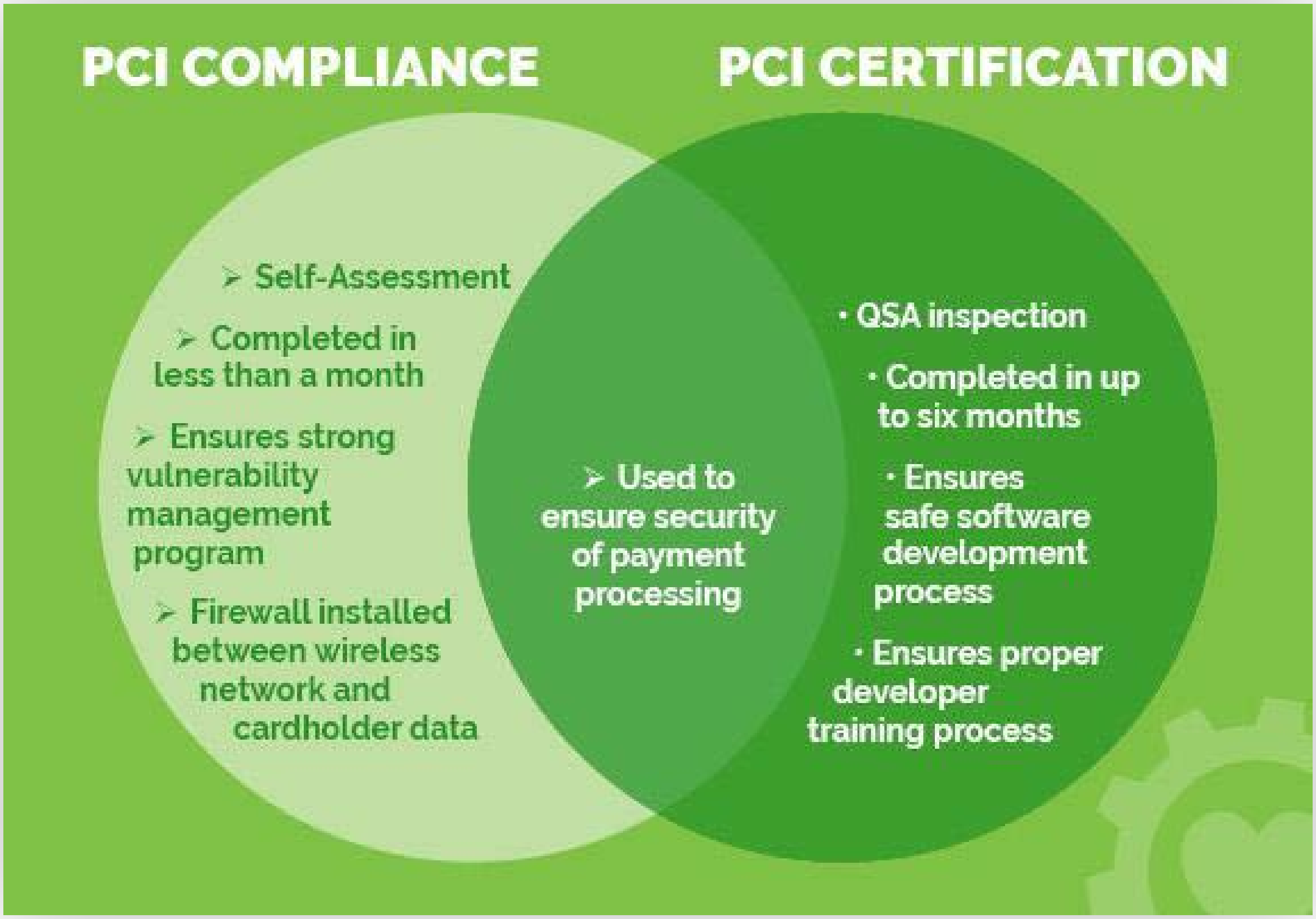
Because the PCI-certification process is so rigorous and stringent about the guidelines that must be met, we recommend looking for a solution with this security classification.

**If your payment processor is PCI-Compliant:**

- It has taken a self-assessment to ensure it follows all of the guidelines.
- It installed a firewall between the wireless network and the cardholder data.
- It has implemented a strong vulnerability management program.
- The security qualifications likely took less than a month to complete.

**If your payment processor is PCI-Certified:**

- A Qualified Security Assessor (QSA) has inspected and approved the software and the security measures taken to protect payment data.
- The QSA has looked into how the software solution was developed.
- The QSA checked the training process of the software developers.
- The security qualifications could have taken up to six months to complete



PCI COMPLIANCE

PCI CERTIFICATION

- ➢ Self-Assessment
- ➢ Completed in less than a month
- ➢ Ensures strong vulnerability management program
- ➢ Firewall installed between wireless network and cardholder data

➢ Used to ensure security of payment processing

- QSA inspection
- Completed in up to six months
- Ensures safe software development process
- Ensures proper developer training process

Make sure that any software solution you use that touches donor payment data is at least PCI-compliant. However, if you have a choice between the two, PCI-certified software is always the way to go. **Your nonprofit can rest assured that a PCI-certified payment processing system is trustworthy and will keep payment data safe.**

# Payment Processor vs. Online Donation Tool

Your nonprofit may ask the question: *"If I invest in an* **online donation tool***, is that tool also a* **payment processor***? How do I know?"*

## These are two different tools that have two different functions.

An **Online Donation Tool** is the front-end tool. This is what helps your nonprofit set up online pages that supporters will see in order to make donations. It helps you organize the necessary data collection forms that you need to learn more about your supporters. Plus, this is generally where you can streamline donor data to your CRM for future engagement.

**Payment Processors**, on the other hand, are more of a back-end tool. Your supporters won't see what the payment processor does. Instead, it's the liaison between your supporter's donation and your nonprofit's bank account. It's what helps keep that important payment information secure.

Most online donation tools will partner with specific payment processors to help nonprofits obtain their donations from beginning to the end

**However, the best solution is when the same company offers both your online donation tool and its own payment processing service.**

When both are compiled in the same solution, your nonprofit will save money (because you take out the middleman) and you'll have a more personal relationship with the vendor. CharityEngine does both.

# Security

## One of the worst things that could happen to your nonprofit is a data breach because it damages trust.

Trust is an integral part of the relationship you have with supporters. If they don't trust your organization, they're probably not going to contribute to your cause anymore. Conduct the proper research in order to ensure the safety of your donor's information. Some of the considerations and keywords your nonprofit should look for before investing in new software solutions include:

**PCI Compliance or Certification**. Consider if you're most comfortable with a certified or compliant organization. Then, make sure to look for solutions that hold the standards most important to your nonprofit.

**Tokenization**. Tokenization replaces the payment information entered by your nonprofit's supporters (like their credit card number) with a string of alphanumeric symbols. This is a security standard required to become PCI-compliant or PCI-certified.

**Encryption**. Similar to tokenization, encryption protects supporter information by converting the data into something less legible for hackers. It takes this sensitive data and converts it into *cyphertext* that can only be translated back with a specific "key."

**Internet Protocol Blocking**: If your nonprofit has specific IP addresses that you know are unwelcome, you can block them with IP blocking.

## We are not just PCI-Compliant.

CharityEngine is PCI-Certified! Certification is via a rigorous third party validated review process. See our listing on the VISA® Preferred Services website.

When you start considering software to help your nonprofit accept donations online, conduct the proper research to make sure the providers offer these types of safety features. **If you're unsure, just ask!** Software providers will be happy to talk about the different measures they take in order to keep your donor data safe.

# 2 Protecting Your Nonprofit From Fraud

## Introduction

When you consider fraud, you might think of someone stealing your identity and making purchases on a credit card. And you're right; that's fraud. Nonprofits aren't usually selling valuable goods, so no one is making purchases with a stolen identity. So are you susceptible to this type of deception? Yes, but you can protect yourself.

The consequences of fraud can be damage to your brand, loss of support, and loss of fundraising income. This chapter will explain why nonprofits can be victimized and offer some warning signs. We will give you a real-life example of what nonprofit e-commerce fraud looks like, and we'll give you some tips on how you can protect your organization.

# Nonprofit Fraud

Nonprofits become victims of fraud for a few reasons:

- Nonprofits trust others who appear to share in their missions and efforts.
- A smaller staff focused on serving donors often doesn't have extensive IT resources to combat fraud.
- Nonprofits have money coming in from different sources and for different amounts, so fraud can be tough to spot.
- And finally, a simple, insidious reason: you're a testing ground for more significant fraud. With often recognizable brands and easy-to-use donation forms, your nonprofit is at risk from organized criminal enterprises wanting to test stolen credit card information to use for bigger crimes.

The risk is real, so how can you know if your nonprofit is the victim of fraud? **Some warning signs might alert you.**

# Warning Signs of Nonprofit Fraud

Nonprofit fraud can run the gamut of illegal behavior, from embezzlement to expense to e-commerce fraud. **Here are some general guidelines of warning signs nonprofits should watch for at all times:**

- Invoices and vendors you don't recognize
- Vendors with a P.O. box instead of a physical address
- A company name comprised of only initials, which is a common fraudulent naming convention
- Sudden increase in purchases from a vendor
- Vendors invoicing you more than once a month

What about e-commerce fraud, where extensive, organized criminal enterprises steal credit card numbers and test them using your nonprofit? Called carding or a carding attack, this is a fairly common occurrence and the one we at CharityEngine see the most.

Here are some indicators you might be a victim of a carding attack:

- An abundance of small donations hitting your payment processor at once
- Unusual activity at a time or on a day people aren't usually monitoring software
- Transactions using the same mailing address and phone number
- Email addresses that look strange

While it might seem you need to be on guard 24/7 to recognize an attack, the good news is that technology can help you with fraud protection. But before we get to that, let's look at a real-life case study.

# An Example of E-commerce Fraud

Here's a real example from about ten years ago. Unbeknownst to a nonprofit client, they were targeted by a sophisticated international organization. The criminals had deployed a network of bots methodically processing fake donations using stolen credit cards. The donations appeared to be coming from different locations and even different countries.

The nonprofit was large, and the decline ratio of this activity was low relative to the organization's overall donation volume. It took the payment processor about two months to flag this activity as fraudulent.

What's the first thing the payment processor did? They shut down the nonprofit's account and insisted the issue be resolved before it could accept and process credit cards online.

Abruptly, **the nonprofit was told they were a victim of fraud, and they started losing money** with every minute that passed.

This nonprofit came to us frantic about getting answers and developing a plan to proceed.

The first thing we did was look at their payment gateway. The client used one of the largest at the time and had anti-fraud services enabled. So why didn't the system flag the fraud sooner?

There were three reasons this attack was successful:

- The donations were spread over time
- They had a realistic cadence that mimicked donor behavior
- They used accurate donor information

CharityEngine worked with the client to implement some short-term solutions, and then we used our CRM to roll out some longer-term changes that leveraged big data. We could effectively eliminate the risk without affecting the nonprofit's conversion rates.

# How Nonprofits Can Protect Against Fraud

**Leverage technology**. We pound this point into the pavement because we know firsthand how much good technology can make your nonprofit safer and more successful.

If you have access to advanced fraud protection, you might not have to protect yourself at all manually; the software likely does it for you. But here are some steps you can take to ensure you are doing what you can to keep your nonprofit safe:

- Check with your payment gateway, no matter how large or widely used, and ask if they are, at a minimum, performing fundamental, industry-standard **I.P. Pattern Detection Analysis** to block acceleration attacks.
- Implement a solution that goes beyond this pattern detection to tie together analytics and geo-dates. **Analytics-Based Intelligent Analysis** can prevent more sophisticated attackers from targeting your nonprofit.

These next mitigation steps are best-practice methods to block automated attackers, but they can potentially harm your donor experience and reduce conversion rates. Keeping your donor experience easy is always advised, but protecting against fraudulent attacks is critical. You probably experience the following with many, if not most, of your personal online purchases:

- **Address Verification Services** (AVS) are settings at both the gateway and merchant levels. They can be toggled on or off and configured with decline/approval responses based on how closely an address entered matches the address on file with the credit card.
- **CVV Code Validation** is that “three-digit code” you’re constantly being asked to report when shopping online. This, too, can be configured by the gateway or the merchant and set to approve or decline charges depending on the code given.
- **Captcha** is that familiar, annoying box that asks you to select all the pictures with steps or traffic lights. It drives users nuts, but it’s effective at blocking bots.

It’s worth noting that **ACH payments**, or checks and bank transactions, are traditionally less often attacked. But due to new guidelines, all merchants must implement technology that validates bank accounts if they are being used for e-commerce transactions.

This is positive news for nonprofits. If your processor uses a robust ACH account verification service, it will prevent fraud, reduce your ACH return rate, and reduce associated fees.

# 3 Considerations Before Investing

## Considerations before Investing in a Nonprofit Payment Processor

In addition to security, there are plenty of other considerations your nonprofit should make before investing in a payment processing solution.

When you're looking for a solution that will help your nonprofit process payments online, you'll need to consider the fees and your budget, software integrations, and the amount of support your nonprofit will receive.

We'll cover the basics of nonprofit payment processing to help organizations like yours make the best decisions regarding online donations.

**3 Tips For Nonprofit Payment Processing**

- Considerations Before Investing
- How To Get Started Processing Donations
- Our Recommended Software

# Considerations Before Investing

## Payment Processing Fees

In addition to security, there are plenty of other considerations your nonprofit should make before investing in a payment processing solution. When you're looking for a solution that will help your nonprofit process payments online, you'll need to consider the fees and your budget, software integrations, and the amount of support your nonprofit will receive.

Of course, when your nonprofit invests in new software, one of your top priorities is staying within your budget. This means both for the short-term, up-front investment as well as the long-term investment.

There are several different types of fees your nonprofit should be on the lookout for when you invest in payment processing solutions:

- **Transaction fees** are those that your nonprofit pays for each donation you process. This includes fees like the markup from your payment processor.
- **Flat fees** are those that you pay in order to work with a payment gateway, aggregator, or payment processing provider. Generally, these come in the form of a monthly or annual fee.
- **Incidental fees** are charged in response to particular incidents that occur. For example, a chargeback fee is considered an incidental fee.

In addition to these types of fees, your nonprofit should consider who is taking a percentage of your donation (no matter how small it may seem). This is an important consideration because the more parties involved, the more those small percentages that are taken from each donation will add up. The first party to take a percentage of the donation is the donation tool you use. Generally, this tool may ask for a small 1-2% platform fee.

The second party that asks for a percentage of your donation is the payment processor who may ask for 3-5% of the donation. **These small percentages add up over time!**

### Look for a solution that offers both the donation tool and the payment processor in the same software. This cuts out the middleman and combines those percentages to the same small fee.

# Comprehensive Software Ecosystem

When it comes to investing in any solution, one of the considerations your nonprofit should always make is around the idea of software integrations.

## When you invest in software that can *do* more and *streamline* more activities, you'll save time and money in the long run.

Therefore, one of the best things to look for before you invest in *any* software, including your payment processing solution, is how it will connect with the other solutions in your software ecosystem.

This means your nonprofit should ensure your donation tool works with your payment processing system. However, it extends further than that. Your donation tool should also work with your CRM, the payment processor should work with event ticketing software, and all of this should work with your accounting platform.

**The best solution?** Investing in a single software solution that includes every feature and function that your nonprofit needs. In other words, look for an all-in-one solution.

This ensures:

- Updates all occur at once. You don't need to worry about the quality of information transfer when different software providers update at different paces. All updates occur at the same time, from the same provider.
- Every function is guaranteed to work together. While integrations are great, they can limit your software choices. Not every provider integrates with all others. With an all-in-one solution, you're guaranteed that everything is connected given a single investment.

**Single all-in-one software solutions** are the best choice by far, but if you prefer to work with integrations between various providers, try to limit them as much as possible. This means you should look for the best, most complete solutions in any given area of expertise.

## Training and Technical Support

When your nonprofit invests in nonprofit payment processing software, remember that you're looking for more than just a solution. You want a partner for your nonprofit.

### Look for a provider that will stand by your side and help your organization when it comes to training and support if anything were to go wrong.

This is one area where a dedicated payment processor has a major advantage over aggregators. Aggregators work with so many organizations, it's rare that your nonprofit can get individualized support. *Dedicated payment processors are much more likely to help your organization with any issues you may have.*

**When you consider the available training and support of providers, look for:**

- A built-out implementation program
- Dedicated personnel assigned to your nonprofit
- Personal training and access to additional training materials
- Ample access to support via phone, chat, or in-person assistance

Having a good partner for your nonprofit team can make all the difference. Make sure you have the training and support you need from the beginning of the engagement through to the completed implementation and beyond.

# How to Get Started With Nonprofit Payment Processing

Now you know what to look for in a software solution, but where do you start? How do you find the solution that's right for your organization?

## Step 1

First, you need to conduct research about the different nonprofit payment processing solutions available. Some of the resources you should start with include:

- **Cold searches** - Start from ground zero and look up different solutions via search engines.
- **Referrals** - Look for referral lists from other trusted software providers or from well-known comparison websites like Capterra or G2.
- **Ask around** - Ask other nonprofit organizations that you have a relationship with about the software they use for their donation processing.

**Note**: Make sure these solutions appear on Visa's list of registered service providers.

## Step 2

Next, you need to narrow down your potential list of software solutions.

Make a list of the features most important to your nonprofit and consider your budget. Take this list and compare it to your list of potential solutions. Narrow it down to your favorite couple of solutions.

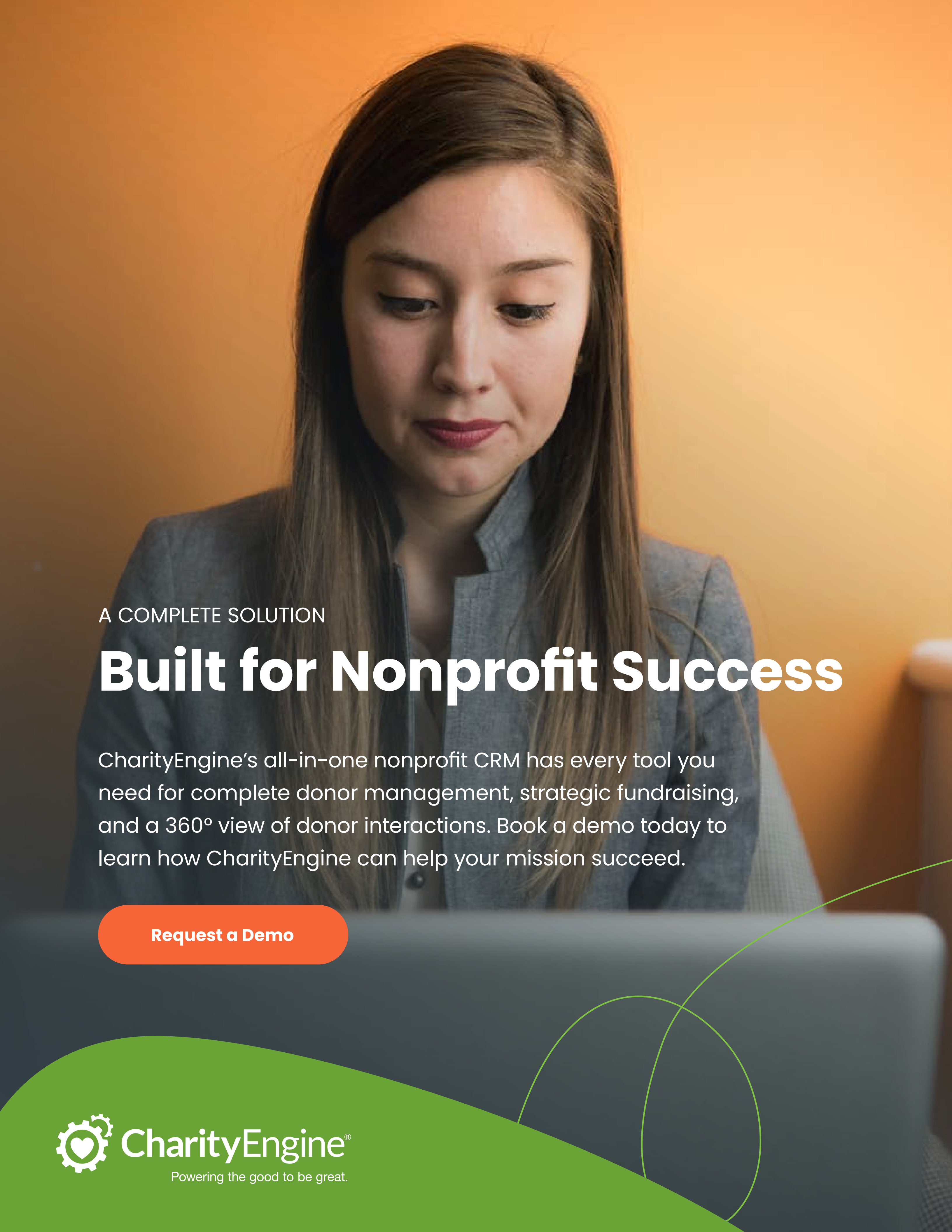
Then, make a list of the questions you still have about each software. This will come handy in the final research step.

## Step 3

Finally, request a demo of your favorite software solutions.

Take the list of questions you made and don't be afraid to ask about them during the demo.

### Make your decision!



A COMPLETE SOLUTION

# Built for Nonprofit Success

CharityEngine's all-in-one nonprofit CRM has every tool you need for complete donor management, strategic fundraising, and a 360° view of donor interactions. Book a demo today to learn how CharityEngine can help your mission succeed.

Request a Demo

CharityEngine®

Powering the good to be great.