Not-for-Profit Industry
How Nonprofits Can Prevent Online Fraud

Despite attempts by banks to make online transactions safer, as much as 60-70 percent of card fraud still occurs online. And it seems that no sites are sacred. Unscrupulous hackers are stealing from well-meaning nonprofit organizations, and even running transactions on insecure nonprofit websites to test stolen cards, costing groups thousands of dollars in chargeback fees from fake donations.

Traditionally designed to protect consumers from fraud, chargebacks enable card holders to dispute any "mystery" expenses that appear on their bills directly with their banks or credit carriers. Since new legislation which came into force in October 2015, it is now the merchant's responsibility to repay chargeback funds if they cannot prove fraud occurred—a liability that has the potential to devastate small nonprofits trying to do good.

So to avoid these costly situations, below are three ways nonprofits can prevent fraud, so they can spend their funds where it really counts.

CHECK THE BILLING ADDRESS AND CVV CODE

When it comes to accepting payments, it is vital to have professional systems in place. Having poorly protected payment systems can ruin the trust of donors and cost organizations extensive chargeback fees.

A key first step to preventing fraud is to check the CVV codes and billing addresses associated with the card used for every donation. Upon payment, ask donors to supply their CVV codes and be sure to use an address verification service, which compares the billing address a customer provides to the address the card has on record. If these don't match up, the transaction should not be accepted.

And while this may seem complicated for non-tech savvy nonprofits, products such as Visa 3-D Secure, Masterpass by Mastercard, and American Express' expresspay can take care of it all. The platforms not only offer consumers a secure payment experience—that is, they don't have to give their payment information to an unfamiliar website—but it also means nonprofits don't have to worry about being responsible for holding all that card data.

Having these security features on board makes it difficult for consumers to request illicit chargebacks successfully, as it is tough to prove the transaction was not valid. Having the right systems in place reduces the risk of having to pay the charge and return needed funds.

BE SUSPICIOUS OF MULTIPLE SMALL DONATIONS

When fraudsters use charity sites as testing platforms, they usually do not spend large sums of money—they want to keep their heads low and avoid being noticed. It is therefore important for nonprofits to be on the lookout for multiple small donations.

Not-for-Profit Industry
How Nonprofits Can Prevent Online Fraud

If these are out of the ordinary, nonprofits need to speak to their payment processors for advice on how to handle the situation—that is, if the processor does not contact the nonprofit first. A good payment processor will likely send a fraud specialist to the rescue, which is a huge advantage to partnering with a trusted company.

To prevent these fraudulent "donations" from happening, nonprofits might want to consider blocking small contributions all together. For example, a nonprofit may decide not to accept donations of less than $2 on its website, an amount that does not count for much after processing fees, anyway. A payment processor would speak to the charity's webmaster and help get the ball rolling and put the change in place.

REQUIRE THE DONOR TO CREATE AN ACCOUNT ON YOUR SITE

Yes, scammers can be relentless. But they likely will not jump through online hoops in order to commit their crimes.

To discourage fraudsters from testing their cards on your donation site, you should consider asking donors to make online accounts on the website before they make a donation. A genuine donor is unlikely to have a problem sharing a bit of information with a nonprofit they would like to help. But a fraudster? Well, upon being faced with making an account, they will likely just move onto another insecure nonprofit website that does not require one.

Not only do these account requirements help prevent fraud, but they also give nonprofits a rich set of data about their donors. On the sign-up page for each account, nonprofits have the opportunity to ask donors for their gender, interests, concerns, cities, names, and email addresses to help develop donor personas—basically, profiles that represent the types of people the nonprofit wants to market to. This will help nonprofits convey content that really makes an impact—and, hopefully, get more donations coming in. It also means that they can use this data for targeted marketing campaigns and also share the results of fundraising campaigns with the people who supported them.

It is important to have the right online security precautions in place to keep funds out of harm's way and allow nonprofits to spend the majority of their time doing what they do best: helping the community.

The preceding is an article by Drew Sementa, CEO of Tidal Commerce, a merchant solutions and payment processing company. This article first appeared on GuideStar.

Contact Us

If you would like to discuss how Cole, Newton & Duran's not-for-profit team can help your organization with your accounting, tax, or consulting needs, please feel free to give me a call.

Pat Koepke, CPA
Not-for-Profit Practice Leader
734.427.2030
pkoepke@cndcpa.com

CND Cole, Newton & Duran
Certified Public Accountants

Cole, Newton & Duran CPAs
33762 Schoolcraft Road
Livonia, MI 48150
P: 734.427.2030
F: 734.427.3004
W: www.cndcpa.com

www.cndcpa.com
Cole, Newton & Duran CPAs