Chargebacks Can Put Your Organization at Risk: How to Prevent Online Credit-Card Fraud

Be sure you have the right precautions in place.

By Drew Sementa

Despite attempts by banks to make online transactions safer, as much as 60-70% of credit-card fraud still occurs online. And it seems that no sites are sacred. Unscrupulous hackers are increasingly stealing from well-meaning nonprofit organizations and even running transactions on insecure nonprofit websites to test stolen cards, costing nonprofits 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. Since new legislation which came into force in October 2015, it's now the organization's responsibility to repay chargeback funds if they can't prove fraud occurred – a liability that has the potential to devastate small nonprofits.

So to avoid these costly situations, let's delve into three ways you can prevent fraud so you can spend your funds where it really counts:

Check the billing address and CVV code

Many nonprofits have pretty basic websites, and that's okay. When it comes to accepting payments, however, it's vital to have professional systems in place. Having poorly protected payment systems could land you in hot water by ruining the trust of donors and costing you extensive chargeback fees.

A key first step to preventing fraud is to check the CVV (Card Verification Value) codes and billing addresses associated with credit cards being used for every donation offered. Upon payment, ask the donor to supply the CVV – the three or four-digit number on the front or back of all credit cards. Also be sure to use an Address Verification Service (AVS),which compares the billing address a customer provides with the address the card has on record. If these don't match up, the transaction shouldn't be accepted.

And while this may seem complicated, 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, donors 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's tough to prove the transaction wasn't valid. Having the right systems in place reduces the risk of having to pay the charge and return the funds.

Be suspicious of multiple small donations

When fraudsters use nonprofit sites as testing platforms, they usually don't spend large sums of money – to keep their heads low and avoid being noticed. Being aware of this, it's important to be on the lookout for multiple small donations.

If you discover small donations that are out of the ordinary, you need to speak to your payment processor for advice on how to handle the situation – that is, if the processor doesn't contact you 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 in the first place, you might want to consider blocking small contributions altogether. For example, you may decide not

> "If the addresses don't match, the donation shouldn't be accepted."

to accept donations of less than $2 on your website – an amount that doesn't count for much after processing fees, anyway. A payment processor would happily speak to your webmaster and put such a change in place.

Require the donor to make an account on your site

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

To discourage fraudsters from testing donors' credit cards, consider asking donors to make online accounts on your website before they make a donation. A genuine donor is unlikely to have a problem sharing a bit of their information with a nonprofit they'd like to help. But a fraudster? Well, upon being faced with making an account, they'll likely just move on to another insecure nonprofit website that doesn't require one.

Not only do these account requirements help prevent fraud, but they also provide a rich set of data about your donors. On the sign-up page for each account, you have the opportunity to ask donors their gender, interests, concerns, city, name, and e-mail address to help develop donor personas – basically, profiles that represent the types of people you want to market to. Such profiles will help you convey content that really makes an impact and get more donations coming in. You can also use this information for targeted marketing campaigns and share the results of campaigns with the people who supported them.

Drew Sementa is CEO of Tidal Commerce (tidalpay.com), a merchant solutions company that focuses on helping small and medium-sized organizations grow. Drew has years of industry experience in the Merchant Services and Fintech industries and started his business in his own basement back in 2003. Since then he's grown Tidal Commerce into a leading merchant provider.

Be Vigilant to Protect Your Assets

For more ways to ward off fraud, see these articles (NonprofitWorld.org):

Wire Transfer Fraud: It Could Happen to You (Vol. 35, No. 3)

Preventing Embezzlement in Your Organization (Vol. 37, No. 2)

Can Your Organization Afford to Lose $100,000? Safeguards Every Nonprofit Needs to Implement (Vol. 30, No. 3)

Don't Get Caught by Phishing Schemes (Vol. 35, No. 2)

Want to Avoid Fraud? Look to Your Board (Vol. 28, No. 5)

Mitigate Cyber Risks with the Right Security Controls (Vol. 36, No. 1)

please get in touch...

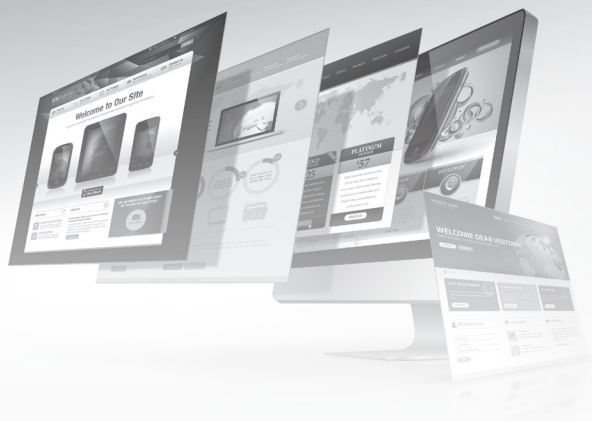
We would love to hear your response to anything in **Nonprofit World**, your comments about any aspect of the nonprofit sector, and your concerns about your daily work. Please get in touch in any of the following ways:

Drop us a note at: Letters to the Editor, Nonprofit World, P.O. Box 44173, Madison, Wisconsin 53744-4173.

E-mail to: muehrcke@charter.net

Please include your name, organization, address, phone number, and e-mail address. If you'd like your comments to appear anonymously, please let us know. We look forward to hearing from you!

Also, we hope you'll join the discussion on the Nonprofit World Discussion Forum. Just go to NonprofitWorld.org, sign in as a member, and click on the Nonprofit Forum link.



WHAT'S UP ONLINE?

Would you like to discuss some of the issues addressed in ***Nonprofit World*** with other nonprofit professionals? Do you have questions to ask or expertise of your own to share?

Society for Nonprofits is actively engaged on LinkedIn, Facebook and Twitter. Find us on your favorite social media platform by visiting **social.snpo.org**

If you have any questions, contact Jason Chmura at jchmura@NonprofitWorld.org