iATS payments

CREDIT CARD FRAUD PREVENTION
IN NONPROFITS

TABLE OF CONTENTS

Nonprofits adhere to their missions and try to have a positive impact in local communities and raise funds and awareness for causes. However, these efforts can be undercut by fraudulent activity. Charitable foundations can experience significant revenue 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, which can make it more difficult to attract new donors. Nonprofits need to be aware of the risks they face from different types of fraud to protect themselves and their donors.

FRAUDULENT CREDIT CARD TRANSACTIONS AND IN WHAT WAYS CHARITIES ARE AT RISK

Nonprofits 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 found charities experience a median loss of $85,000. Charitable foundations need to know what to look for to be able to protect themselves from the following types of credit card fraud:

CARD TUMBLING

Card tumblers gain information by focusing on the rules and math of how credit card numbers are created. 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. Many organizations, including charities, do not require three-digit security codes to process transactions and this places them at risk for credit card fraud.

Charities can experience card tumbling if fraudsters use their online sites to test card numbers. Online donations present this risk because they do not involve a physical credit card, and people can make transactions as long as they have a credit card number. If the rightful owner of the card number disputes these charges, he or she must be refunded. This is known in the industry as a "chargeback." Organizations will end up losing revenue for donations they cannot use to support causes.

ONLINE AUCTION FRAUD

In addition to risky credit card donations, nonprofits are vulnerable to criminals using stolen credit card information to purchase items in online auctions. Similar to fraudulent credit card transactions, the charity will need to pay the chargeback fees for the unauthorized charge. Additionally, the nonprofit may lose the donated auction item if it is shipped before the fraud is uncovered. Depending on the value of the item, this can contribute to a significant loss of revenue.

In April 2013, Apple was hosting an online auction for the Robert F. Kennedy Center for Justice and Human Rights, and they discovered the highest bidder for the top item - a coffee date with CEO Tim Cook - was made by someone using a stolen credit card. Fortunately, Apple was able to identify this before the end of the auction.

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. According to data from the Federal Trade Commission, auction fraud accounts for 48 percent of online fraud reports. 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, according to research from the Hauser Center for Nonprofit Organizations at Harvard University. 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

Charities may be contacted by someone who claims he or she will make a large donation, but only if the nonprofit sends half of the donated amount to another charity, which turns out to be a personal bank account. This involves nonprofits in money laundering, and the transaction is typically made with a stolen or compromised credit card. In addition to lost funds, nonprofits could potentially encounter high litigation costs to defend themselves 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. Nonprofits should never move their own funds to another bank account in order to receive a large donation.

IMPACT OF CREDIT CARD FRAUD TARGETED AT NONPROFITS

Charities depend on donations to stay in operation and support their cause, and this means financial losses from returning funds and paying chargeback fees are especially significant. Any percentage of revenue lost annually is money nonprofits cannot use for their missions.

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. Donors will not want to be associated with these organizations because the charities will be perceived as dishonest, and individuals and groups will also worry their financial information will not be secure.

Additionally, fraudulent activities are 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 the organization to get back on track.

IMPACT OF CREDIT CARD FRAUD FOR DONORS

Since many fraudsters test stolen credit card numbers on nonprofits' websites, people may notice suspicious charges on their credit card statements. But unless someone contests this payment, consumers can find themselves the victim of more expensive fraud or identity theft. While many banks and credit card companies do not charge people for transactions they didn't make, consumers may still find their bank accounts temporarily empty.

Although these individuals will be refunded, nonprofit fraud presents an inconvenience for donors. Banks may need to issue fraud victims new credit card numbers, and this can be a hassle for people who have automatic payments, including monthly donations, connected to their cards.

STEPS NONPROFITS CAN TAKE TO MINIMIZE THEIR RISKS

Small and large organizations can feel the effects of fraud, so it's important for charities of any size to establish a system of checks and balances. It can be a good idea to conduct background checks on all potential employees to cut down on the incidences of internal fraud. Organizations need to stay aware of current fraud impacting other nonprofits because it can alert them to individuals who are targeting charities. In addition to boosting internal communication and employee awareness, nonprofits need to increase their payment security to eliminate credit card risks with the following techniques:

- VELOCITY CHECKING: This technique looks at the number of previous payments associated with a credit card number or bank account to identify a common data point, such as a donor name, transaction amount or similar BIN number. Nonprofits can set limits and be more aware of fraudulent activity from the outset. While loyal donors may make repeat gifts over time, a large number of donations in a short period of time is suspicious. Multiple donations from the same IP address or large numbers from the same unknown donor should also be red flags.

- IP ADDRESS/BIN BLOCK: Every credit card has an associated Bank Identification Number, and nonprofits can block donations from risky areas. Similarly, IP ranges can be blocked from the payment gateway. For example, a fraud ring was uncovered in Romania in December 2012 after tampering with U.S. auction items, so nonprofits need to be aware of high-risk regions. Though nonprofits want to achieve maximum donations, they should recognize that reaching out to international audiences requires extensive security preparation.

- REQUIRE THREE-DIGIT CARD SECURITY CODES: This can cut down on card tumbling since fraudsters do not have security codes from the back of cards.

- ADDRESS VERIFICATION SYSTEM: This measure requires the address used in the transaction to match the bank's records. While this can impact international donations, it's recommended that nonprofits create a separate online donation form to collect contributions from overseas.

PCI COMPLIANCE AND ITS ROLE IN PREVENTING FRAUD

The Payment Card Industry Data Security Standard 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.

PARTNER WITH A TRUSTED PAYMENT PROCESSING COMPANY

Partnering with a reliable payment processing provider is one of the best ways for nonprofits to reduce fraud. Charities are particularly vulnerable to fraudulent credit card activity, and the financial and reputational damages can be significant. Nonprofits can trust iATS Payments for a range of fraud protection services, including address verification, IP blocking, BIN checking, card verification code requirement capabilities and minimum transaction limits. All of these preventive measures can help nonprofits mitigate the threats of credit card fraud so they can continue fundraising and spreading cause awareness.

SOURCES

1. http://www.deleonandstang.com/news-articles/nonprofit-edge-article/how-to-prevent-fraud-within-your-nonprofit-organization/

2. http://www.nonprofitquarterly.org/management/164-how-to-steal-from-a-nonprofit-who-does-it-and-how-to-prevent-it.html

3. http://abcnews.go.com/blogs/business/2013/04/apple-ceo-coffee-auction-hit-by-card-fraud/

4. http://finance.yahoo.com/news/didn-t-donation-charity-watch-120000865.html

5. http://www.networkworld.com/news/2012/121112-gang-responsible-for-multimillion-dollar-online-265002.html

6. http://www.bbb.org/blog/2013/07/online-auctions-safeguarding-yourself-from-being-scammed/

7. http://www.pcicomplianceguide.org/pcifaqs.php#1

8. http://www.eisneramper.com/non-profits-fraud-0410.aspx

9. http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

600-1188 W. Georgia St.,
Vancouver, BC, Canada,
V6E 4A2

1.866.300.4287
iats@iatspayments.com

iatspayments.com