iATS payments

Case Study

iATS puts customized fraud protection to work for Pachamama Alliance

INTRODUCTION

Online fraud seems to grow more commonplace by the day. Companies such as Target and Home Depot recently detailed accounts of breaches that punched holes in their systems, leaving financial information out in the open for criminals to use to defraud unsuspecting customers.

However, when it comes to fraud and system hacks, one doesn't expect criminals to take aim at nonprofits. Unfortunately, for-profit businesses aren't the only organizations susceptible to hacks and data breaches. While the incidents might not make the news every day, they are a pressing matter for nonprofits. The Urban Institute announced earlier this year that the National Center for Charitable Statistics was hacked. The center collects tax filings from nonprofits across the country.

Meanwhile, online security is increasingly becoming a top concern for nonprofits, as 84 percent of not-for-profit presidents said hacking and data breaches are among the top 10 problems facing nonprofits, according to the 2015 CohnReznick Not-for-Profit Survey.

What's more, fraudsters often use stolen credit cards on nonprofits' websites as a means to test the cards. Criminals will use transactions of small amounts — typically under $5 — to ensure the card is valid and can be used for further fraudulent purchases.

A NONPROFIT IN NEED

Nonprofits can not only lose money, but also their donors' trust if they are subject to a fraud attack. The funds lost in fraud not only come from businesses or grants but also from individual donors' pocketbooks. That's why Tatiana Tilley was concerned.

The director of operations for Pachamama Alliance, a nonprofit that works with the indigenous people of the Amazon rainforest to preserve their land and culture, found irregularities within her organization. According to Tilley, a fraudster located in Brazil attacked the Pachamama Alliance's website using the online donation page to hack donor financial data. "We were able to return all the money to the people," Tilley said. "But we were stuck with the fees."

While the organization had fraud protection features in place on its online donation page, they didn't provide the highest security possible and weren't customized to fully fit Pachamama Alliance's needs.

However, just as Tilley was about to contact iATS Payments, the donation payment processor reached out to her first to inform the nonprofit of the unusual activity it found on the not-for-profits' donor page.

The company went to work by both pinpointing the source of the breach and customizing the iATS online anti-fraud tools for Tilley's organization. An iATS representative walked the nonprofit through the whole process, showing Tilley how they could rectify the situation and keep defrauders from comprising Pachamama Alliance's system ever again.

"They were great," Tilley said. "We called them, they helped us, they showed us what we hadn't implemented. [The fraudsters] tried again but since we had the blocks in place it shut it down."

SECURITY SOLUTIONS

Through the use of tools provided by iATS, including card and name tumbling, Internet protocol blocking and bank identification number checking, the nonprofit was able to track where the fraudulent transactions were coming from and block the fraudsters from accessing the website.

iATS works with nonprofits all over the world to deliver safe and reliable payment processing to the not-for-profit sector. In fact, the company offers fraud protection features and tools for free to its customers. Patrons that sign up for iATS' services can customize the protection solutions they need and want by simply turning them on and off. The iATS team works closely with nonprofits to educate and assist them with developing a level of online security to fit their individual needs.

The sophisticated features include Internet protocol (IP) and bank identification number (BIN) protections, which enable nonprofits to reject fraudulent transactions based on the country of the card and where the transaction originates from. Another free service institutes a gift minimum, blocking scammers from using a nonprofit's website from donating small amounts. Criminals often charge small amounts to a stolen credit card to see if it's still active before moving on to bill larger fraudulent charges with it.

Along with other free features, including name and card number tumbling, card verification code requirement capability and more, iATS is able to put security front and center for nonprofits without breaking the bank or stopping valid donations.

ABOUT iATS PAYMENTS

iATS Payments works exclusively with the not-for-profit sector and anticipates the security and payment processing needs of over 10,000 nonprofit organizations across the globe. In operation for nearly 20 years, the company makes the security of its clients a No. 1 priority.

iATS Payments is able to offer top-of-the-line cybersecurity for donation pages thanks to a certified Level 1 PCI Compliance grade. Level 1 means the company meets the highest ranking of data security, keeping cardholders' financial information secure from hackers and other criminals.

Meeting Level 1 for PCI Compliance also means iATS Payments frequently monitors its systems to find fraud and stop it as soon as possible, much like the case with Pachamama Alliance.

The company is dedicated to streamlining the donation process for nonprofits while keeping sensitive data secure. iATS Payments lets nonprofits stay focused on what they do best — helping others.

iATS payments

iATS Payments
1188 West Georgia St, Suite 600 • Vancouver, BC V6E 4A2
Toll Free: 88.955.5455 opt.1 • Fax: 604.682.1715 • Email: iats@iatspayments.com • www.iatspayments.com