Dealing With Fraudulent Transactions

Non-profit organizations have recently become subject to high levels of fraudulent activity. This is a fairly new development, and has the industry scrambling to come up with solutions.

What is happening, and why:

Lists of credit card numbers are sold on the black market. The scammers purchasing those numbers need a way to test if the credit cards are valid by first running a small transaction. Non-profit organizations with online donation portals are the easy target. Once a donation portal is found, the scammers often run multiple credit cards for a small donations, anywhere from $1 - $20 each, to verify that the credit card will work.

This creates several problems for the organization. Your system is being flooded with fake donor data, and puts your organization at risk for disputes from the credit card holder, leaving you to foot the bill for each dispute fee from the credit card company. Unfortunately, once your organization has been targeted, there is not much you can do to stop the scammers from continuing to make these attempts. The truth is, currently there are no security measures built into any donation software out there.

Now that we've heard the bad news, it's time for the good news! Here is what we're doing at Flipcause to protect you, and additional measures you can take:

What we're doing:

We developed a proprietary algorithm (AFTA) that is scanning and monitoring system is catching 99+% of fraudulent attempts, so what you are seeing still getting through, is only a tiny fraction of total fraudulent attempts.

Companies pay $150,000+ to build systems like these in-house, and we have these additional measures available to all of our clients at no additional charge!

What you can do:

1. Monitor each donation for suspicious activity. You should be receiving an email
notification of every donation that comes through. Make a point to inspect every
donation you receive that is under $20. Things to look for: Fake names, fake email
addresses, and fake street addresses (they will often look like "weruowhe jdsoeu" or
"abc@123.com"). Log into Flipcause, go to Funds and Account Records to view the details.
Click "Details" next to the transaction to check if the name and contact information looks
real.

3. If anything is suspicious but you're unsure, contact the donor personally to confirm this
donation. (In the Details view, there is a button to "Contact" the donor.)

2. If anything is clearly fake, flag the transaction as fraud. Flagging a transaction as fraud
will initiate an investigation with our compliance team who will look to reimburse the card
holder (refund the transaction), and file a fraud report. Once the fraud investigation is
initiated, the related funds will be deducted from your merchant account.

If you have any questions, don't hesitate to reach out to your Success Team.