Credit Card Testing Explained

Last Modified on 12/20/2024 10:29 am PST

Occasionally, Non Profit organizations will experience Card Testing on a giving form. This article outlines the basics of what Card Testing is, and the protections that GiveSmart employs to help combat this behavior.

What is Card Testing?

Card Testing (also referred to as "stolen credit card testing") occurs when fraudsters use bots or click farms to make bulk donation attempts through a giving form, with the goal of determining the validity of various credit card numbers or CVVs.

If a GiveSmart form is impacted by Card Testing, please be assured that there have been no intrusions into the system and no data has been compromised.

Why are Non Profits impacted by Card Testing?

These bad actors often target Non Profits as they can easily locate a giving form via the organization's website, Google search, or other means.

Non Profit giving forms are often short and simple, which is another reason why they are often targeted by bad actors. They're usually one page, and tend to have minimal required fields other than basic contact information. This ultimately makes it easier for bad actors to use automated scripts or bots.

What does Card Testing look like?

Typically, stolen credit card testing can be identified by the following traits:

- Multiple bulk-declined donation attempts in a very short period of time, often within minutes or seconds of each other.
- The donation attempts are often in small $ amounts, typically less than $5 but can be more than $25.
- The donation attempts will often have suspicious/fake names, emails, and contact information.

What does GiveSmart do to combat Card Testing?

Multi-factor authentication (MFA) has been deployed on all payment forms in GiveSmart Fundraise to mitigate bot testing. Read more here.

Additionally, the GiveSmart systems team identifies, monitors, and shuts down Card Testing activity on a daily basis, and employs security measures such as reCAPTCHA, Firewalls, Velocity/Rate Limits, and IP activity monitoring with automatic banning.

As Card Testing continues to evolve with new tactics, the GiveSmart team also continues to research and implement new tools (such as AI bot detection) to combat card testing activity originating from bots, scripts, click farms, or other means.

Although rare, if there are one or more successful transactions which were determined to have originated from card testing activity, the team will Void/Refund those transactions and remove them from your account to prevent any potential chargebacks.

Does this impact my donors?

Card Testing has no impact to your donors or their data. Although the notion of a fraudulent credit card testing attack may sound concerning, please be assured that Card Testing activity is not indicative of any intrusions into the system or compromised data.

That being said, the safety and security of your payment information is our highest priority at GiveSmart. All donor data collected via GiveSmart is guarded by Level 1 PCI compliant systems, meaning that with any GiveSmart donation form, all card data is protected by the highest security standards in the payment card industry.