Stolen Credit Card Testing Explained

Occasionally, nonprofit organizations will experience stolen credit card testing on their accounts. This page outlines the basics about credit card testing and the fraud protection process GiveSmart Fundraise uses to ensure your organization and your donors are never compromised.

Why are nonprofits targets for stolen credit card testing?

Fraud occurs when a scammer uses your donation form to test a stolen credit card number to see if it works. Nonprofit organizations are often used this way for a few reasons:

- Nonprofit forms are short and simple -- they're usually one page and don't require lots of information like billing address, etc.
- Scammers can enter any donation amount they like, making it very easy to test transaction limits.
- Donation forms are relatively simple, making it easier for criminals to use an automated script.

What does credit card testing look like?

Typically, stolen credit card testing appears in the form of multiple donations in a very short period of time, often increasing in amount and connected to suspicious-sounding names. We monitor for this kind of activity continuously, identifying and investigating suspicious activity every day. If something unusual happens on your account, we will know and start working to resolve it immediately.

What does this mean for my donors?

In short, nothing. Stolen card testing of this kind has nothing to do with your donors, your organization, or any credit cards associated with your organization.

What does it mean that GiveSmart Fundraise is PCI Level 1 Certified?

The safety and security of your payment information is our highest priority at GiveSmart Fundraise. Every piece of user data held by GiveSmart Fundraise is guarded by 100% PCI compliant systems. With all our online donation forms, your data is protected by the highest standard for credit-debit card security on the web.

For more answers about merchant services, review the **Frequently Asked Questions**.