Fraud Doesn't Take a Holiday: Beware of Card Testing

If your business or non-profit organization accepts payments from a payment gateway or e-commerce site, you may be exposed to a new form of merchant account fraud called **card testing**. Unfortunately, there is no fail-safe system to protect against it, but your close attention to daily batch and authorization details before settling will go a long way in alerting you of a possible problem.

Fraudsters obtain credit card information from a variety of sources. To know which cards have not yet been reported stolen and can be successfully highjacked, the data has to be tested. The process involves creating an account to test the credit card numbers until a valid one is found. The program then finds the corresponding expiration date that would allow for a valid the transaction.

With card testing, the fraudster doesn't care about a merchant's product or service; they are simply focused on testing the card number. Charities are frequent targets because most are donation based, and fraudsters know the amount and frequency of donors can vary, making their testing attempts less obvious. This type of fraud can be difficult to catch at businesses as well for a similar reason: the goal isn't to secure a huge order which would be a red flag but to identify a working credit card by having an order created. Sadly, prime time for fraudsters to slide these transaction tests through is during the hectic holiday season.

Fraudsters test hundreds, even thousands of combinations to get a match that will allow them to use a given card. Because a merchant's gateway charges for *every attempted* authorization—whether it has been approved or not—this testing process could end up costing a merchant a bundle in fees.

Is there any way to tell if this is happening at your site? Here are a few things to look for:

- Many authorization attempts in a short time frame
- A strand of tests where card brands rapidly switch from Visa to MasterCard back to Visa, etc.
- Notices that authorizations have FAILED—not "partial matches" or "review"—but FAILED

Preventative measures include the following:

- Collect AVS (address verification system) and CVV (3-digit code on back of the card) data on your authorization file/gateway settings.
- Enhancements to your gateway/internet shopping card can block IP addresses, block/limit authorization attempts and set other velocity checks to reduce the likelihood of being targeted by authorization testing. Many of these enhancements are at no cost or minimal cost, depending on the gateway.
- Ask your processor about additional security protocol you may need when accepting transactions in a card-not-present environment.
- Alert your processor to any suspect activity for immediate review. Once a transaction is settled, you would be liable for chargebacks associated with unauthorized charges.

Remember to routinely review your daily transactions. If you have questions or concerns, please call your Veracity support team. We want to help protect you against fraudulent activity.