cybersource
A Visa Solution

# 3 Steps for protecting your business from card testing attacks.

Card testing happens when an attacker "tests" a card number that was either made up or obtained through phishing or spyware software, or from the dark web. The objective of the test is not necessarily to purchase a product or service, but to see if the details of the card are valid by attempting small purchases online on the site of an unsuspecting vendor and then checking to see if the card was approved.[1]

## 1

Make sure your checkout pages include technologies for detection and prevention of sending transactions coming from automated scripts such as:

- **Firewalls.** Tools for detecting, preventing and eliminating botnets.
- **CAPTCHA.** A challenge-response visual test to distinguish a human from an automated script.
- **Device fingerprinting.** Identifies multiple contacts with the same device.
- **Velocity thresholds.** Limits the number of transactions permitted within a specified timeframe.
- **Anomaly Detection.** Detection of unusual peaks in the traffic of a webpage, unusual patterns during purchase or when filling out forms.

## 2

If your site accepts donations or free text payment amounts, it is especially important that you include measures to avoid automatic scripts for card testing. These sites are vulnerable. In addition to the previous steps, keep the following in mind:

- **Set thresholds for minimum amounts.** Fraudsters seek to know if the card is valid, avoiding the possibility of the cardholder noticing and reporting. The smaller the amount of the purchase, there is less the probability that it attracts attention.
- **Avoid transactions for small amounts.** It is often common to see transactions for very small amounts, even equal to zero. It is better to set a higher minimum amount.

## 3

Stay alert and identify any anomalies in advance.

- **Investigate** any changes in daily transactions.
- **Pay attention** to sudden increases in the number of card rejections.
- **Use velocity tools** to track totals and other data specs

### More tools that can help prevent fraud:

**Limits of established amounts**
Limit transactions to those that pertain to your business.

**Device Fingerprinting**
To better identify the users connecting to your service.

**Cybersource Account Takeover Protection (ATP)**
Block fake accounts creation or account takeover fraud on your site.

**Cybersource Fraud Management Essentials (FME)**
Provides pre-set rules with machine learning to identify and block higher risk transactions.

**Cybersource Decision Manager (DM)**
Comprehensive solution using machine learning and Artificial intelligence to identify and block higher risk transactions.

**Cybersource helps protect your business from card test attacks.**
If you want to know more about how Cybersource can help, contact your team Cybersource account management or visit **www.cybersource.com**

cybersource
A Visa Solution