CyberSource® | A Visa Solution

Payment Card Testing

Fraudsters use advanced techniques to test the validity of stolen cards, commonly referred to as card testing. One method includes the use of botnets, or a network of machines that can automate card testing attacks at an exponential scale compared to manual testing.[1] Merchants should stay ahead of the curve to help avoid these types of large-scale attacks. Below is an overview of some best practices and tools merchants can use to help combat this increasing threat.

What is card testing and why is it becoming so prevalent?

Card testing occurs when a fraudster "tests" a credit card number that they may have purchased on the dark web, randomly generated, or acquired via phishing or spyware software. The central purpose of testing is not the purchase of a product or service but verifying if card details are valid by attempting either loading a card to an online account, or small purchases online on an unsuspecting merchant's site, then checking the response to see if the card was approved.[2]

For fraudsters, card testing can be an effective method to verify cards are still valid. Cardholders and banks may have taken preemptive action to cancel the cards that may have been stolen weeks or months previously, making them of no value. If these small purchases are successful, that indicates the cards could be approved if used for additional purchases. The fraudsters often move on to make larger purchases, or to resell the validated card numbers on the dark web.

[1] *The Ever-Changing Landscape of Bots and Credit Card Testing,* by John Canfield, April 26, 2018, business.com
https://www.business.com/articles/bots-credit-card-testing
[2] ibid

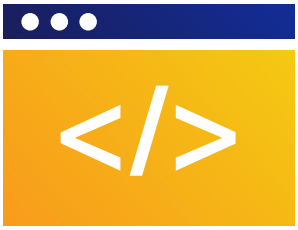
Small and medium businesses are often the target of card testing attacks as they may lack the tools and technologies to detect, deter and prevent these attacks.[3] While businesses under attack may not see a notable increase in chargeback rates, they might see a significant spike in declined authorizations. Although authorization fees are typically low, when a site is bombarded with thousands of transactions, these fees add up quickly and can easily reach exceedingly costly amounts.

What is a botnet attack and how is it associated with card testing?

Done manually, the process of card testing can be especially time consuming and laborious for fraudsters. To address this, they commonly turn to a more sophisticated system of using large networks of compromised computers (botnets) to perform this task.

A botnet attack is a type of malicious attack that utilizes a network of compromised computers to attack a website, network service or an IT environment.[4]

In these card testing attacks, bots can be programmed to run thousands of transactions at a time, each making a small purchase on a website to determine whether the card numbers are valid.[5]



What should businesses do to protect themselves from card-testing attacks?

1. One best practice is to ensure your checkout and card addition pages (or any other pages where cards are validated) include technologies to detect and prevent automated scripts from submitting transactions. Some of these include:
   - **Firewalls** typically include basic tools for botnet detection, prevention, and removal. Tools like Network Intrusion Detection Systems (NIDS), rootkit detection packages, network sniffers, and specialized anti-bot programs may be used to provide more sophisticated botnet protection
   - **CAPTCHA** visual challenges designed to distinguish humans from automated scripts

[3] *SMB Merchants Are Too Complacent When it Comes to Payment Fraud,* by Rei Carvalho, May 16, 2019, TotalRetail, https://www.mytotalretail.com/article/smb-merchants-are-too-complacent-when-it-comes-to-payment-fraud/

[4] https://www.techopedia.com/definition/29948/botnet-attack

[5] *Card Testing Fraud: What You Need to Know,* December 14, 2017, TransNational, https://blog.gotnpayments.com/card-testing-what-you-need-to-know

- **Device fingerprinting with proxy piercing capabilities** code designed to identify multiple contacts with the same device, along with technology to detect the originating device in the case of a botnet
- **Velocity thresholds** limits on the number of transactions permitted within a specified timeframe, Including HTTP session velocities, which limit the number of operations per user session
- **Anomaly detection** detects sudden or unusual spikes in traffic to your webpage or unusual patterns in shopping or form entry behaviors
- **Time out of user session** sets HTTP sessions to expire after periods of inactivity
- **Cross Site Request Forgery (CSRF) detection** allows user progression to sensitive pages that originate from your expected user flow, and invalidate used tokens
- **Guest checkouts** if you allow guest checkouts, make sure to add data validation

2. Another common area for attackers to test cards is at the point where cardholders are adding payment methods to their online accounts on merchant sites. Therefore, it's important to perform risk reviews for this step, including Account Verifications of the payment being added, and basic velocity checks over specified timeframes.

If your site accepts donations or custom payment amounts (free-text), it is particularly important to include measures that will prevent automated scripts and card testing. Fraudsters have discovered that these types of sites are generally easy prey and specifically target them to use in card testing.[6] In addition to the above, consider the following:

- **Set minimum amount thresholds.** In a card testing attack, fraudsters aim to validate if a credit card is good while avoiding the likelihood of the cardholder noticing and reporting it. The smaller the charge, the less likely it is to attract attention or result in a chargeback.
- It is common to see transactions for very low amounts, often less than $5. **If possible, it is best to set a minimum value that is as high as possible** while still being appropriate for most donors.

[6] *5 Ways to Minimize Card Testing Fraud On Your Nonprofit's Donation Page,* by Robert Wright, September 11, 2019, The A Group, https://www.agroup.com/blog/5-ways-to-minimize-card-testing-fraud-on-your-nonprofits-donation-page/

3. **Be vigilant**, identify anomalies early on.
    - If you see an unsuspected or sudden spike in your average daily transactions – research it.
    - A sudden increase in the number of credit card declines can be a serious signal that your business is being targeted.
    - Have a variety of velocity tools to track not only transaction totals, but also other specific data elements (including email, IP address, device fingerprint, etc...)

Can CyberSource help protect a business from card-testing attacks?

Yes. In addition to ensuring that your website includes technologies to help prevent automated scripts from submitting transactions (i.e. for bot attacks), CyberSource fraud tools can also help to identify and mitigate card testing.

Options to assist with defense:

- For merchants offering an option for customers to create online accounts, **CyberSource's Account Takeover Protection (ATP)** helps authenticate account creations and logins by detecting mismatches in locations, behaviors, devices and accounts. It also includes device fingerprinting with proxy-piercing technology and a bot-detection identifier. Implementing fraud checks during account creation and login can help to identify and block bots or fraudsters prior to logging in and prior to attempting to load and test cards.
- For merchants selling through an ecommerce platform, velocity rules implemented through **Decision Manager (DM)** or **Fraud Management Essentials (FME)**, can track, count, and reject repeated transaction attempts that share common data elements or that exceed total transaction volume limits. Amount thresholds set in DM or FME can help limit transactions to those appropriate for your business.

These fraud tools may be used upstream during processing, putting detection methods before the authorization (commonly referred to as pre-auth). Ultimately, you can reject a transaction prior to authorizing it, stopping a card testing attempt before it happens—and before authorization fees are incurred. Not sure which tools might be right for your business? Please reach out to your CyberSource representative, who can help put together a management plan that works for you.

Important guidance from CyberSource fraud management experts:

No single component can prevent card testing fraud. **It is imperative to implement multiple layers of protection.** Businesses should implement a combination of best practices and risk tools at every stage of the transaction flow, from account events to card loading to transaction requests. This multi-faceted strategy can help identify and block fraudsters who may be trying to attack your business through card testing.

For more information on how CyberSource can help, please contact your CyberSource Account Management team or www.Cybersource.com.

CyberSource® | A Visa Solution