Help Protect Your Merchant Account from Card Testing

What is Card Testing?

Card Testing, also known as "carding", "enumeration", or "account testing", is a practice used by fraudsters to submit unauthorized transactions to identify valid card information so that it may be used to perform fraud elsewhere. The most common method of Card Testing is to target a Merchant's website or mobile app by using an automated process to submit multiple transactions. These transactions may take the form of purchases, pre-authorizations or card verifications performed when adding a card.

How does Card Testing impact Merchants?

Card Testing has many negative impacts on Merchants, which include:

- **Cardholder Disputes:** Approved transactions are likely to result in cardholder disputes, especially if they are not refunded. These disputes are costly and reputationally damaging.
- **Additional Fees:** Card Testing can result in excessive transaction attempts (ETAs) and additional non-compliance fees from Payment Card Networks (PCNs). ETAs are defined by PCNs as continued authorization attempts (using the same card number), the consequence of which is typically declined transactions. Examples of ETAs are 10 or more decline responses within a 24-hour period, or 15 or more decline responses within a 30-day period. For more information, please refer to *"Payment Card Network – Changes to Decline Codes, Rules and Fees"* at www.tdmerchantsolutions.com/notices.
- **Increased Declines:** Card Testing creates a negative association with your business from the perspective of the PCNs and card issuers, which may cause more of your transactions to be declined even when the Card Testing activity has stopped.

How does TD Merchant Solutions help protect Merchants from Card Testing?

TD Merchant Solutions has controls in place that are designed to help mitigate Card Testing, including monitoring, reporting and alerts. Unfortunately, these controls alone cannot prevent Card Testing. Merchants must take steps to prevent unauthorized transactions on their websites or mobile apps.

What should I do if my Merchant Account is being used for Card Testing?

The first thing you should do is determine if the Card Testing is going through your website, or if it is going directly to your payment gateway. If the Card Testing is going through your website, please review the recommendations below.

If the Card Testing is going directly to your payment gateway, your API keys may be comprised and should be rotated. If this happens you should review how you are managing your API keys to ensure they are secure. You should also be mindful of phishing scams aimed at obtaining your API keys.

Regardless of the form of Card Testing, it is important that you refund any approved Card Testing transactions to avoid further reputational impact and disputes.

How can I protect my website from Card Testing?

Typically, preventing Card Testing involves code-level changes that require Merchants to work with their developers. If you are using a platform, please work with your vendor. You can also work with your payment gateway provider to ensure you are leveraging the fraud prevention tools they have available. These tools may include 3-D Secure, Card Verification Value 2 (CVV2) and Address Verification Service (AVS) or fraud scoring tools. While these tools will not directly prevent Card Testing, but they will discourage the fraudster from targeting your website as they will cause more of the Card Testing attempts to result in a decline.

How to help protect your website from card testing

CAPTCHA

- Implement CAPTCHA controls to prevent automated transaction initiation by bots and scripts.
- Ensure your CAPTCHA solution is configured to prevent Card Testing by adjusting available thresholds and ensuring that it is placed in the payment or card add flow.

Monitor and Limit

- Monitor the velocity of small and large transactions. Account testing transactions are typically for a small amount. Create limits based on identified transaction amounts or ranges and number of transactions within a specified timeframe.
- Monitor the velocity on various data elements such as devices, IP addresses, emails, etc.
- Analyze time zone differences and browser language inconsistency from the cardholder's IP address and device. Classify these transactions as high risks and perform more stringent review.
- Monitor IP addresses associated with large numbers of declines. Limit or temporarily block these IPs.
- Look for excessive usage and bandwidth consumption from a single user. Limit or block these users.
- Look for multiple tracking elements in a purchase linked to the same device. For example, multiple transactions from different accounts using the same email address or same device ID.
- Look for logins for a single payment account coming from many IP addresses.
- Limit the number of accounts that can be created per IP within a set time limit. Monitor the frequency of payment method changes on accounts.

User Sessions

- Limit the number of cards that can be added per ‘account’ and session.
- Terminate sessions that are pending for guest users for a certain time-period.
- Inject random pauses (i.e., throttling) when checking an account, to slow attacks that are dependent on time.
- Include HTTP session velocities, which limit the number of operations per user session and set the session to expire after seconds of inactivity.
- Lock out an account if the user inputs a username/password in any account authentication data incorrectly on "x" numbers of logins attempts.

Network Tools

- Implement a web application firewall (WAF).
- Utilize basic tools for botnet detection, prevention, and removal. Tools like Network Intrusion Detection Systems (NIDS), rootkit detection packages, network sniffers, and specialized antibot programs may be used to provide more sophisticated botnet protection.

Cross Site Request Forgery (CSRF) Detection

- Implement CSRF tokens to prevent simplistic automated attacks.
- Ensure all the *site* pages are loaded with “https” protocol and protected with CSRF token.