Anti-Enumeration and Account Testing Best Practices for Merchants

V1.2

April 2023

Visa Public

Contents

Executive Summary

Account Enumeration is a prolific problem that affects issuers, merchants, and acquirers globally. Cybercriminals are taking advantage of big data and artificial intelligence to find and exploit new vulnerabilities. To conduct fraudulent eCommerce transactions, cybercriminals use scalable and programmatic automated testing of common payment fields, a method also known as account enumeration. This practice results in hundreds of millions of dollars in fraud losses across the payments ecosystem. Once valid payment information is obtained, it is then sold on the dark web and on cybercrime underground carding sites. Further, enumeration increases processing fees for acquirers and issuers, disrupts risk management models, and frustrates merchants as they may lose inventory, and waste resources fulfilling orders unrelated to legitimate customers. This guide will provide an overview for acquirers on implementing mitigation techniques to ensure their merchants are not susceptible to these attacks.

Enumeration and Account Testing Overview

Enumeration is the criminal practice of submitting fraudulent card not present transactions into the payments ecosystem in order to obtain valid payment information. The most common types are:

1. Enumeration Attack: This is a fraud attack in which a criminal systematically submits transactions with enumerated values such as Primary Account Number (PAN), card verification value (CVV2), expiration date, and postal code to derive legitimate payment account details. This type of attack is commonly referred to as a Brute Force attack.

2. Account Testing: The process of initiating 1-2 low dollar transactions to verify if an account is active in order to take it over for illicit means or to sell. Typically, these attacks focus on a single BIN range.

Enumeration and Account Testing Causes

There are several ways that fraudsters can perpetrate these types of attacks.

- The most common method is for fraudsters to target legitimate eCommerce merchants or third party service providers that have weak fraud controls in place. Due to the lack of fraud controls it makes it hard for the merchant to detect and block fraudulent use of their website for enumeration purposes.
- Fraudsters can gain access to the payment system by applying for merchant accounts with synthetic merchant identities and use those accounts to conduct enumeration attacks. Criminals target acquirers or agents with weaknesses in their underwriting and onboarding practices that allow fraudsters to open merchant accounts for enumeration attack purposes.
- Fraudsters perform merchant account take-overs and gain access to the payment system by obtaining a merchant's login credentials and subsequently taking over their payment gateway to conduct enumeration attacks. These credentials can be obtained when a merchant falls victim to phishing schemes, or gateway service providers lack proper merchant authentication when fraudsters call in pretending to be merchants resetting credentials. This form of attack can also impact virtual point-of-sale (VPOS) and mobile point-of-sale (MPOS).
- Fraudsters set up cloned point-of-sale (POS) devices or gateways using existing merchant credentials and access processor hosts to submit transactions as part of an enumeration attack. This is due to processors who have front-end platform hosts that fail to validate that POS devices or payment gateways belong to their legitimate merchants.

Visa Account Attack Intelligence

Account Testing Detection

Account testing affects merchants worldwide and stakeholders can feel its impact immediately. Therefore, it is imperative to detect the activity quickly so defense measures can be implemented to mitigate the fraudulent activity. Visa Account Attack Intelligence uses cutting-edge machine learning to identify account testing, analyze the details of the attack, and enable Visa to take appropriate action in near real-time.

3. Identify patterns and take defensive actions and proactively help prevent future attacks.
4. Collaborate with acquirers to remediate merchants vulnerable to account enumeration and testing attacks due to weak validation practices.
5. Reduce losses and brand damage for issuers, merchants, acquirers, and Visa.
6. Identify tactics, techniques and procedures of threat actors perpetrating account enumeration and testing to better defend against and disrupt payment account enumeration, including working with law enforcement.

All VisaNet clients are monitored for account testing. If a fraud case is identified, Visa will engage the proper stakeholders to address the case.

Protecting the Ecosystem

The following defensive measures are recommended to deter account testing that leverage merchant websites:

Anomaly detection

- Identify anomalies early, sudden spikes in the daily average and declined transactions should be investigated. These spikes could indicate that the business has become a target.
    - Alert on transactions with a large volume of approvals or declines from a similar BIN range.
    - Alert on an increase in reversals being sent. Occasionally, fraudsters will immediately send a reversal after an authorization receives an approval.
- Analyze time zone differences and browser language inconsistency from the cardholder's IP address and device. Classify these transactions as higher risk and perform more stringent review.
- Include IP addresses with multiple failed card payment data in a fraud detection blacklist database for manual review.
- Look for excessive usage and bandwidth consumption from a single user.
- Look for multiple tracking elements in a purchase linked to the same device. For example, multiple transactions with different payment accounts using the same email address and same device ID, may be a trigger for fraud classification or review.
- Look for logins for a single payment account coming from many IP addresses.
- Review logins with suspicious passwords (or unique encrypted hashes of passwords) that hackers commonly use. Some merchants are able to detect fraud based on a gray list with set or combinations of passwords commonly used in fraudulent transactions.

Velocity thresholds

- Monitor the velocity of small and large transactions and use velocity checks for low amounts or authorization-only transactions. Account testing transactions are often less than $10 USD.
- Thresholds should also be set on the number of transactions within a specified timeframe.
- Monitor the velocity on various data elements such as IP address, device, email.

Account Creation:

- Limit the number of cards that can be added per 'account' and session.
- 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.
- Utilize Re-Captcha for user registrations.
- Terminate sessions that are pending for guest users for a certain time period.

Technical Tools

- Implement CAPTCHA controls in web portal to
    - Use visual challenges to prevent automated transaction initiation by bots or scripts, example five authorizations from one IP address or PAN within a set timeframe.
    - Aid in determining where the IP address in the transactions are coming from and block malicious IP addresses.
    - Make sure the CAPTCHA requires validation on all request that enable card validation or payments.
    - Google offers 3 different CAPTCHA versions: reCAPTCHA Enterprise, reCAPTCHA v3, and reCAPTCHA v2. When implementing CAPTCHA onto your website, ensure to use Google specialist when placing reCAPTCHA within websites as improper placement can lead to vulnerabilities.
- Implement a web application firewall (WAF).
    - Firewalls usually include 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.
    - Adjust Firewall to limit page submission and repeat actions on websites.
    - Adjust Firewall to automatically ban visitors and users from known malicious origins.
- Implement fraud detection system that have device fingerprinting with proxy piercing capabilities to identify multiple contacts with the same device and to detect the originating device in the event of a botnet.
- Utilize 3-D Secure authentication.

Account Verification Implementation

- Integrate Account Verification (AV) checks to prevent incorrect or unauthorized account into the ecosystem. AV request are not authorizations and do not authorize purchases, nor do the messages need to be accompanied by payment authorization.
    - After the request is made, your acquirer will pass the request to the issuing bank and will confirm if the account is an open valid account.
    - AV request must also include Card Verification Value (CVV2), expiration, and address verification to authenticate the account.
    - Allows card-on-file merchants to run CVV2 checks on their stored payment accounts prior to introduction to the ecosystem.
    - AV aids in preventing incorrect or unauthorized use of payment information in a merchant's card-on-file, wallet, or recurring payment ecosystem.
- AV Request are sent as 0100 Authorization Requests that must contain Field 4, Field 25, and Field 123. Improper formatted AV request may result in unexpected declines
    - Field 4: Amount, transaction = zero (0)
    - Field 25: POS Condition Code = 51 (Account Verification)
    - Field 123: Address Verification Data

- Follow the corresponding issuer response that appear in the 0110 Authentication Response message in Field 39 (AV Response), Field 44.10 (CVV2 Response), and Field 44.2 (AVS Response).
  - Field 39, Codes 85 (No Reason to Decline) or 00 (Approved) can be authenticated as the account is valid and has no adverse status. Do not authenticate other codes.
  - Field 44.10, CVV2 Code M (Match) and U (Issuer is not certified) can be authenticated. If response is Code U (not supported), do not authenticate.
  - Field 44.2, Code A, B, C, N, and R should not be authenticated. AVS response that indicate postal code checks have failed or technically disrupted should not be authenticated. Code I, G, S, and U should not affect authentication.
- Monitor for and block excessive failed AV attempts. AV attempts can be tracked by account IP and device to prevent clandestine exploitation of their authentication mechanism.

User Sessions

- Inject random pauses (i.e., throttling) when checking an account, to slow brute-force attacks that are dependent on time, especially for BINs that have been determined to have a high fraud rate.
- Include HTTP session velocities, which limit the number of operations per user session and set the session to expire after periods of inactivity.
- Lock out an account if a user inputs the username / password and any account authentication data incorrectly on "x" number of login attempts.

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.

Additional Recommendations

- Account information and terminal applications should be securely deleted from all memory slots when decommissioning a POS device
- Be cognizant of phishing scams aimed to obtain payment gateway credentials.
- Use a layered validation approach that employs CVV2 and Address Verification Service (AVS).
- Combined Application Program Interfaces (API) keys if the card testing attacks are going directly to your API rather than the website form.
- It is important to implement measures that prevent automated scripting and card testing on websites that accepts donations or free-text payment amount. Fraudsters have specifically targeted these sites to be used in card testing.
  - Set a minimum amount threshold. It is best to set a minimum value that is as high as possible but is still appropriate for most donors. The smaller the charge, the less likely it is to attract attention or result in a charge back.

Collaborate Together

Account testing is a global issue that requires collaboration between merchants, acquirers, issuers, and Visa to find a solution. Threat actor attribution is a significant step towards identifying fraudsters and putting an end to their malicious activity. To assist in identifying threat actors and deterring future attacks, please provide the following details for account testing transactions to PaymentIntelligence@visa.com :

1. Source IP Addresses: IP addresses potentially provide the threat actors' location, infrastructure, and method of attack.
2. Customer Name and Billing Address: These elements help correlate transaction attempts. Threat actors generally use the same name and/or billing address for multiple transactions. Visa uses this information to group suspicious activity on a single client's system or on multiple clients' systems.
3. Source Email Address: Threat actors may use the same or similar email addresses.
4. User-Agent Header: String that provides user browser / operating system information specific to the user when connecting to another website. This field helps identify connecting websites or browsers.

Contacts

Payment Systems Intelligence Contact Information:

- Team e-mail: PaymentIntelligence@visa.com

Risk Operations Center Contact Information:

- roc@visa.com
- Phone: 1-844-847-2106

Resources

Payment Systems Intelligence Visa Online Page

Account Testing Visa Online Page