Visa Business News

Best Practices

13 September 2021

This article originally ran in the 12 August 2021 edition of the Visa Business News*. It is being republished to correct the first CVV2 indicator name in the Best Practices for Issuers section below and to provide an additional reference guide for the use of CVV2 parameters. Please use this version of the article going forward.*

Visa Guidance to Guard Against Enumeration Attacks and Account Testing Schemes

Global | *Acquirers, Issuers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: Visa is reminding clients to maintain adequate controls to swiftly detect and block enumeration attacks and account testing schemes.

Visa is committed to upholding and protecting the integrity of the payment system. Through monitoring of fraud activity, Visa has observed a sustained increase in enumeration attacks and account testing. Visa employs real-time detection and machine-learning analytical capabilities to help protect the payment system against such attacks. However, Visa reminds clients that it is critical to maintain appropriate controls to block such fraud attacks as part of their obligation to safeguard payment account information and payment system participants.

Related Training From Visa University:

- Introduction to the Payments Landscape
- Introduction to the Payments Landscape: Understanding Acquiring
- Intermediate Fraud Prevention

Enumeration and Account Testing Attacks Background

Enumeration and account testing attacks occur when fraudsters use automated scripts or software to obtain or validate payment account information. These attacks most often occur on e-commerce-enabled merchant websites, where fraudsters submit the automated transaction attempts. While these attack methods are similar, there are some important differences:

- **Enumeration attack:** An enumeration attack is a scheme where fraudsters systematically submit card-not-present (CNP) authorization attempts, while concentrating on a single Bank Identification Number (BIN) or multiple BINs and iterating through various combinations of payment values. These payment values generally include the primary account number (PAN), expiration date, Card Verification Value 2 (CVV2), and postal code. Issuers decline the authorization attempts until the right combination of payment values returns an approval response. An approved authorization response (and often a subsequent sale) is an indicator to the fraudster that they have obtained a combination of valid payment values. This scheme is also known as a brute force attack.

- **Account testing:** Account testing is a scheme where fraudsters submit one to two low-amount transactions to test or validate if an illicitly obtained payment account is active, in order to take it over to commit fraud. In many cases successfully tested payment credentials are sold to others to commit fraud. This scheme is

sometimes referred to as BIN testing, card stuffing, card tumbling or Credit Master attacks. Generally, account testing attacks occur on multiple payment accounts within the same issuing BIN.

Ecosystem Impacts

Enumeration attacks and account testing schemes generally lead to compromised accounts and account takeovers. However, the residual aspects of these schemes, while not always conspicuous, have additional negative effects on various ecosystem parties. Impacts include:

- **Fees:** These include fees for authorization (for approvals and declines), clearing and settlement, interchange, dispute processing, system integrity and gateway transactions charged by Visa, VisaNet processors, service providers and other parties involved. Such fees could be substantial if the scale of an enumeration attack is significant.

- **Operational impacts:** These include operational expenses for customer service, submitting and responding to disputes, the reissuing of payment credentials, possible loss of business and the potential for non-compliance assessments.

- **Fraud impacts:** These impacts result from the use of compromised accounts for the purchase of goods or services at merchants not involved in the initial attack or scheme. Cardholders whose accounts were taken over at this stage notice fraudulent use of their payment account and resort to initiating disputes with their issuers. This often leads to merchants sustaining losses due to fraud disputes for goods or services they delivered.

- **Risk exposure:** Other than financial risk, there may be exposure to compliance risk (such as identification in Visa's risk monitoring programs), regulatory risk and the potential for reputation or brand risk for the various parties involved.

While this list is not all inclusive, Visa has further referenced these and a variety of other impacts in the materials linked in the "Additional Resources" section below.

Recent Trends and Observations

Over time the objective and general aspects of enumeration attacks and account testing have remained consistent. However, Visa has observed some evolving tactics, which include:

- **Enumeration through authentication:** Fraud actors have recently targeted various e-commerce merchants with a high volume of authentication attempts to identify valid payment account details for specific issuing BINs. This is a notable development in enumeration tactics, as most enumeration attacks prior to these campaigns were conducted solely through authorization attempts.

- **Targeting specific merchant categories:** Visa identifies trends in targeting victimology, where fraudsters conduct enumeration and account testing attacks on specific merchant category codes (MCCs) over a period of time before shifting to other MCCs.

  For example, in early 2021, Visa identified fraudsters targeting merchants categorized under the following MCCs:

  - MCC 5912—Drug Stores and Pharmacies
  - MCC 8220—Colleges, Universities, Professional Schools, and Junior Colleges
  - MCC 5399— Miscellaneous General Merchandise and MCC 5999—Miscellaneous and Specialty Retail Stores (specifically merchants selling cannabidiol (CBD)-related products)

- MCC 7992—Public Golf Courses and MCC 5941—Sporting Goods Stores (specifically golf-related merchants)

Visa releases tactical-level alerts on these shifting trends, which can be accessed by referencing the links below.

These merchants are likely targeted due to a higher probability of inadequate fraud controls on their respective checkout pages. After fraud actors identify merchants with vulnerabilities, they tend to pivot to other merchants within the same industry segment.

- **Third parties with vulnerabilities:** Fraud actors tend to target merchants that use third parties for their e-commerce business that are known to lack adequate fraud controls. Specific third parties targeted include payment gateways and shopping cart providers—a.k.a. merchant servicers or technology integrators. Many third parties develop payment platforms for specific industry segments, thus there is often a correlation between third parties and specific MCCs being targeted.

Visa payment system participants are urged to periodically visit Visa Online for updates and alerts on changes in tactics and trends—see links below.

Safeguarding the Payment System

A prudent approach to mitigate enumeration and account testing schemes is to adopt a layered method. This includes:

- **Protect the payment system from unauthorized access:** Fraudsters must identify potential vulnerable entry points in the payment system to initiate enumeration and account testing schemes. It is the first hurdle fraudsters will attempt to overcome, and they do so by exploiting such entry point vulnerabilities. Common vectors to gain unauthorized access include:
    - **Exploiting vulnerable merchant websites or service providers:** Sometimes referred to as card stuffing, fraudsters employ bots for the automated injection for payment account information into a legitimate merchant's checkout pages. This is the most common method for fraudsters to gain access to payment processing, primarily due to weak fraud controls used by merchants and/or their service providers.
    - **Merchant application fraud:** Acquirers or agents exhibiting weaknesses in their underwriting and onboarding practices may allow criminals to slip through and open fraudulent merchant accounts for enumeration and account testing purposes.
    - **Merchant account takeovers:** Fraudsters gain access to the payment system by obtaining a merchant's credentials through phishing schemes or targeting payment gateways with weak customer validation and identification (CV&ID) practices. Fraudsters subsequently use the merchant account for fraudulent activity.
    - **Merchant cloning:** Fraudsters clone POS devices or payment gateways by programming them with illicitly obtained merchant credentials. Cloned devices or gateways are subsequently connected to processor hosts with weak authentication controls and fraud transactions are submitted.
- **Monitor for, detect, and block attacks:** Acquirers—and by extension any designated VisaNet processors, applicable third party agents (TPAs), and merchants—have an obligation to maintain adequate controls to detect and block fraudulent transactions, enumeration and account testing attacks from entering the payment system.

- **Mitigate suspect activity:** While issuers are the recipient of enumeration and account testing transactions submitted by acquirers, it is imperative for issuers to employ sound controls and authorization logic to mitigate the impact of such activity.

Best Practices for Acquirers, TPAs, Processors, and Merchants

The following best practices are recommended for acquirers, designated VisaNet processors, applicable TPAs (e.g., payment facilitators, marketplaces, and merchant servicers), and merchants:

- Ensure merchants use CAPTCHA controls on their check-out pages to prevent automated transaction initiation by bots or scripts.
- Use velocity checks that monitor for:
    - Deviations or spikes in merchant authorization attempts, including velocity to the same issuer or issuing BIN, sequential PANs, CNP activity, cross-border activity, identical or similar amounts, and activity originating from new or inactive / dormant merchants.
    - Authorization declines with response codes indicative of potential fraud, including: Response Code 14—Invalid Account Number, Response Code 54—Expired Card, Response Code 55—Incorrect PIN, Response Code 59—Suspected Fraud, Response Code 82—Negative Online CAM (card authentication method), dCVV (dynamic card verification value), iCVV (Visa Integrated Circuit Card [ICC] verification value) or CVV results and Response Code N7—Decline for CVV2 failure. **Note:** Some issuer and stand-in processing (STIP) response codes may be converted to Response Code 05—Do Not Honor, depending on if an acquirer is activated to receive the original codes.
    - Merchants with approved authorizations for which the corresponding sales drafts have not been submitted for clearing and settlement within 24 hours or longer.
    - Suspect activity pertaining to merchants with MCCs listed in this *Visa Business News* article.
- Use sound merchant underwriting and onboarding practices to detect fraud merchant applications, including compliance with the *Visa Global Acquirer Risk Standards* (GARS), linked in the Additional Resources section below, use of the GARS Auto-Boarding best practices, merchant application fraud scrubbing and velocity checks on new merchant applications.
- Employ controls to detect BIN spikes and other suspect activity on 3D-Secure (3DS) transactions.
- Monitor for merchant descriptors with random characters (key smashing).
- Monitor host and network traffic for unauthorized or suspect connections and probing activity. Use Point-to-Point Encryption (P2PE) or PCI-validated cryptographic keys (e.g., Triple Data Encryption Standard [TDES] or Triple Data Encryption Algorithm [TDEA]) for all host and transaction session activity.
- Implement HTTP session and velocity limits or pauses (i.e., throttling), which restrict the number of operations per user session and set the session to expire after periods of inactivity.
- Ensure merchants and technology integrators (e.g., gateway service providers) employ measures to prevent account takeovers, such as periodic password changes, avoid use of default login credentials, and education on the risks of phishing scams and social engineering.

Best Practices for Issuers

The following best practices are recommended for issuers, designated VisaNet processors, and applicable TPAs:

- Refrain from issuing sequential or incremental PANs, or batch issuance of expiration dates.
- Use velocity checks that monitor for:
    - Deviations or spikes in authorization attempts, including velocity from the same merchant (descriptor, CAID, Terminal ID), the same issuer BIN, sequential / unissued / inactive /dormant PANs, CNP activity and cross-border activity.
    - Authorization declines with response codes indicative of potential fraud, including: Response Code 14—Invalid account number, Response Code 54—Expired card, Response Code 55—Incorrect PIN, Response Code 59—Suspected Fraud, Response Code 82—Negative Online CAM, dCVV, iCVV, or CVV results and Response Code N7—Decline for CVV2 failure.
    - Suspect activity pertaining to merchants with MCCs listed in this VBN article.
- Block unused account ranges.
- Consider leveraging Visa Risk Manager (VRM) rules by combining the CVV2 Fraud Indicator and the CVV2 Result code to establish rules to identify an increase of transactions with invalid CVV2 transactions. Check the *VRM Rule Criteria Reference User's Guide,* available via the help menu in the VRM tool*,* for more information regarding the use of these parameters. Please ensure rules are tested prior to publishing.
- Make cryptogram keys available to Visa for STIP to validate the CVV2 on the issuer's behalf and utilize Visa Advanced Authorization risk scores in STIP parameters.
- Develop and use a predefined incident response plan with steps to mitigate and/or escalate active attacks, including blocking of attack-related authorization attempts and an option to contact an acquirer directly in case of a large-scale event.
- Monitor the Access Control Server for spikes in activity. Numerous one-time password or step-up authentication requests in a short period should be treated as suspicious and indicative of authentication enumeration, especially if the authentication is not completed (e.g., the alleged cardholder does not follow through on entering the one-time password).
- In the event of a confirmed or suspected breach, refer to *What To Do If Compromised* (AP, Canada, CEMEA, LAC and U.S. only) and *What To Do If Compromised—Visa Europe Data Compromise Procedures* (Europe only) on the Global Risk Investigations page at Visa Online.

Visa strongly recommends organizations access and subscribe to the Payment Systems Intelligence section at Visa Online. This ensures that appropriate teams are receiving timely alerts and best practices. The provided information can be utilized to help identify, mitigate and prevent fraud and cyberattacks targeting the payments ecosystem. The 17 October 2019 *Visa Business News* article, "Accessing and Subscribing to Visa Security Alerts," provides a guide on how to subscribe to these alerts. Please contact Payment Systems Intelligence with any questions.

For More Information

Merchants and third party agents should contact their acquirer.