Visa Business News

Fraud

8 June 2017

Preventing Brute-Force Authorization Attacks

AP, Canada, CEMEA, Europe, LAC, U.S. | *Acquirers, Issuers, Processors, Merchants, Agents*

Overview: Visa is providing an overview of brute-force attacks and best practices on how merchants and clients can identify and mitigate them. Issuers, acquirers and merchants are ultimately responsible for preventing this type of attack.

A brute-force attack is a trial-and-error method used by fraudsters to obtain, within seconds, payment card information such as an account number, card expiration date, PIN or Card Verification Value 2 (CVV2), as well as a user password for online account access. In a brute-force attack, automated software commonly known as a "botnet" is used as a downloader or a credential-collection tool that generates a large volume of consecutive guesses of account data.

Related Training From Visa Business School:

- Fraud and Risk

Current Threat in LAC and How It Affects the Rest of the World

While automated attacks executed by botnets on networked zombie computers are not a new problem, the methods used by fraudsters are becoming more sophisticated. The brute-force attack is now a common threat that card-absent fraud managers face, where fraudsters perform a password / payment card guessing attack. A hacker can continue to run credit card numbers through merchant websites until the authorization response comes back approved (according to VisaNet data from January to December 2016, 90 percent of primary account number [PAN], expiry and CVV2 guessing attempts come back declined).

Since 2012, Visa has seen an increase of merchant botnet attacks in the LAC region. According to a joint study by the Center of Strategic Studies and McAfee, cyber attacks cost the global economy an estimated USD 90 billion per year.

According to authorization data analysis by Visa, a large number of merchants in LAC have seen a spike in the number of authorization requests, and the first warning sign is the excessive number of rejects with different response codes, such as "Invalid Account Number," "Invalid CVV2" or "Invalid Expiration Date."

All issuers should consider two types of fraud / authorization management methods to deal with brute-force attacks:

- Analyze merchant names that generate a high concentration of payment volume. The issuer should consider a more sophisticated analysis and strategy to avoid increasing the number of authorization rejects on good transactions, which results in higher false-positives.

- Analyze velocity by card account number. The issuer may consider adjusting the risk parameters on authorization requests if the same card reaches a suspicious number of tries in 24 hours.

Best Practices for Merchants

Merchants use different criteria in their fraud-prevention strategies than issuers or acquirers. Merchants' risk priorities are based on product type, history of chargebacks, delivery time for goods in the retail environment, time to departure in the airline industry, etc. Therefore, Visa recommends all merchants consider the following best practices:

Process	Recommendation
Real-time fraud detection	• Where available, use a layered validation approach that employs CVV2 and Address Verification Service (AVS). • All online merchants should manage fraud-detection systems that support device fingerprint, email validation and botnet detection. • Analyze time zone differences and browser language consistency from the cardholder's IP address and device. The transaction may be classified as a higher risk and be sent for manual review instead of bypassing the automatic approval process. • Look for multiple tracking elements in a purchase linked to the same device. For example, multiple transactions with different cards, using same the email address and same device ID, may be a trigger for fraud classification or review. • Look for logins for a single card account coming from many IP addresses. • Look for excessive usage and bandwidth consumption from a single user. • Review logins with suspicious passwords that hackers commonly use. For example, today some merchants are detecting fraud based on a gray list with set or combinations of passwords commonly used in fraudulent transactions.
Payment gateway	• Payment gateways should implement tracking rules to alert simultaneous transactions testing with low amounts at the merchant ID level.
Front-end controls	• Consider using Three-Domain Secure (3DS) authentication and captcha controls to prevent automated transaction initiation by robots or scripts (for example, five authorizations from one IP address or card). • Lock out an account if a user guesses the user name / password and any account authentication data incorrectly on "x" number login attempts. • Inject random pauses when checking a card to slow a brute-force attack that is normally dependent on time. This can be done on certain Bank Identification Numbers (BINs) that have been determined to have a high fraud incidence. • Include IP address with multiple failed card payment data in a fraud detection's black-list database for manual review. • In addition to velocity checks for small and large transactions, use velocity checks for low amounts or authorization-only transactions.
Analytics	• Create a Management Information System (MIS) or report based on "Invalid Account Number" fraud detection attempts at the issuer BIN level, the account number or terminal ID level, or the IP address or device ID level.

Best Practices for Acquirers

Process	Recommendation
Merchant activity	- Monitor all merchant accounts to detect suspicious activities, such as spikes in sales draft transactions from a card acceptor or terminal ID. - Monitor transactions with a large volume of approvals or declines from a similar BIN range. - Monitor all BINs for suspicious events, such as spikes in transactions, approvals or declines (for more information, refer to the Additional Resources section at the end of this article). - Monitor potential suspicious purchases based on ordered products / services (e.g., purchase of numerous high-value, same-model televisions in one transaction). - Use captcha or alternative anti-robot controls during the check-out stage.
Analytics	- Create an MIS or report based on “Invalid Account Number” fraud detection attempts at the issuer BIN level, or the issuer Processor Control Record (PCR), account number or merchant doing business as (DBA) name level.

Best Practices for Issuers

Process	Recommendation
How to report these attacks to Visa or acquirers	- The issuer can contact the acquirer of record directly by using the Client Directory at Visa Online. - The issuer can ask Visa to reach out to the acquirer if the acquirer is unreachable or uncooperative. Please contact your Visa representative / customer support.
Personalization controls	- Avoid issuing card numbers sequentially. - Use random expiration dates (once an issuer approach is known, the actual expiry date can be found easily).
BIN management	- Block unused account ranges. - Monitor all BINs for suspicious events, such as spikes in transactions, approvals or declines (for more information, refer to the Additional Resources at the end of this article).
Case creation rules for Visa Risk Manager (VRM) users	- Combine the CVV2 “Presence” indicator and the CVV2 “Result” code to establish rules to identify an increase of transactions with invalid CVV2 transactions. In some regions, the issuer is required to decline an invalid CVV2.
Fraud control and authorization strategies	- Create a rule on the authorization host that cues fraud detection staff to validate consequent transactions on cards that present more than ”x” number of “Invalid Account Number” attempts on the same day.
Stand-in processing (STIP)	- If an issuer is using STIP on a permanent or regular basis, ensure velocity counts are in place to decline excessive authorization requests. - Make cryptogram keys available to Visa to validate CVV2 on the issuer’s behalf. - Leverage Visa Advanced Authorization (VAA) risk scores in STIP parameters. - Implement an advice retrieval process to recover all transactions with “Invalid Account Number” response codes processed in STIP.

Additional Resources

Documents & Publications

"How to Protect the Visa Payments System From Fraudulent Authorizations," *Visa Business News*, 23 June 2016

BIN Utilization

BIN Utilization Policies Frequently Asked Questions

What to Do If Compromised

Online Resources

Visit the Merchant Resource Library.

Note: For Visa Online resources, you will be prompted to log in.

For More Information

AP, Canada, CEMEA, LAC, U.S.: Contact your Visa representative. Merchants and third party agents should contact their issuer or acquirer.

Europe: Contact Visa customer support on your country-specific number, or email CustomerSupport@visa.com.

Notice: This Visa communication is furnished to you solely in your capacity as a customer of Visa Inc. (through its operating companies of Visa U.S.A Inc., Visa International Service Association, Visa Worldwide Pte. Ltd, Visa Europe Ltd., Visa International Servicios de Pago España, S.R.L.U. and Visa Canada Corporation) or its authorized agent, or as a participant in the Visa payments system. By accepting this Visa communication, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Rules, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a participant in the Visa payments system. You may disseminate this Information to a merchant participating in the Visa payments system if: (i) you serve the role of "acquirer" within the Visa payments system; (ii) you have a direct relationship with such merchant which includes an obligation to keep Information confidential; and (iii) the Information is designated as "affects merchants" demonstrated by display of the storefront icon (🏪) on the communication. A merchant receiving such Information must maintain the confidentiality of such Information and disseminate and use it on a "need to know" basis and only in their capacity as a participant in the Visa payments system. Except as otherwise provided, the Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Visa is not responsible for errors in or omissions from this publication.