Increase in Account Testing, BIN and Enumeration Attacks

The payments industry continues to see an increase in the number of card testing attacks globally. Worldpay advises you and your merchants to be diligent, increase awareness and review current detection controls to help prevent these types of fraudulent attacks.

Account Testing: Account testing attacks occur when fraudsters submit one to two low-amount transactions to test / validate if a payment account is active; if the account is active the fraudsters will later take it over to commit fraud. In most cases, the attack happens on multiple payment accounts within the same issuing BIN. In some instances, payment accounts that have been successfully tested are sold to others to commit fraud. This attack is also known as BIN testing, card stuffing, card tumbling or a Credit Master attack.

Enumeration attack: An enumeration attack is a scheme where fraudsters systematically submit card-not-present (CNP) authorization attempts. The attacks are concentrated on a single Bank Identification Number (BIN) or multiple BINs and iterate through various combinations or payment values such as primary account number (PAN), expiration date, Card Verification Value 2 (CVV2) or postal code. The attack is successful when the right combination of payment values returns an approval response.

We would like to remind you to continuously monitor and take immediate action to mitigate these attacks ensuring the safety and security of the payment ecosystem.

What can you do?

Worldpay will continue to notify you of any suspicious authorization activity that may be potential card testing. In partnership with the card brands, we recommend the below list of best practices to assist with any mitigation efforts.

- The card brands or issuers may block transactions to mitigate exposure.
- Standard authorization fees will apply and may include additional excessive authorization fees. The card brands do not reimburse these fees.
- The card brands can also levy non-compliance assessments if card testing activity is not mitigated in a reasonable timeframe.

Effective Mitigation Measures:

- Recommend engaging with your gateway, webhosting provider, or independent software vendor (ISV) as soon as possible to discuss the recommendations highlighted below.
- Leverage authentication and CAPTCHA controls to prevent automated transaction initiation by bots or scripts (e.g. 5 authorizations from one IP address or Account)
- 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
- Include IP address with multiple failed card payment data in a fraud detection blacklist database for review and analysis

Effective Mitigation Measures (cont.)

- Alert on transactions with a large volume of approvals or declines from a similar BIN range
- Utilize fraud detection systems that support device fingerprinting and botnet detection
- Inject random pauses (i.e. throttling) when checking an account to slow brute force attacks that are dependent on time, especially for Bank Identification Numbers (BINs) that have been determined to have a high fraud incidence
- Look for logins on a single account coming from many IP addresses
- Review logins with suspicious passwords that hackers commonly use
- Lock out an account if a user guesses the username/password and any account authentication data incorrectly on “x” number of login attempts

More Information

Click here to view Visa’s Anti-Enumeration and Account Testing Best Practices for Merchants white paper.

If you have any questions or would like further information, please reach out to your Worldpay from FIS contact.