VISA SECURITY ALERT

August 2014

CONTINUING FRAUDULENT CREDITS TREND: ATM REVERSALS

Distribution: Acquirers, Issuers
Who should read this: Risk Management, Fraud Prevention, Operations

Summary

In the 19 December 2013 edition of the Visa Business News, Visa warned payment system participants that criminals are continuing to use merchant account information to issue fraudulent credits. These transactions make it appear as though cardholder accounts have been credited for the return of goods or cancellation of services. In reality, no goods or services were purchased, and the funds go to the criminals' accounts. In some cases, these credits are reversed by the acquirer or merchant after the funds have been depleted, potentially leaving issuers with significant financial losses.

Visa has recently seen a variation to this scheme where criminals are able to successively withdraw the same funds preloaded on a card account: Once an initial withdrawal has been made using compromised merchant account information, criminals will issue a reversal (0400) to the previously authorized ATM withdrawal transaction, thus replenishing the funds on the account. The criminals will repeat these steps successively, enabling them to make multiple withdrawals. The reversals are likely issued through gateway portals or virtual POS software.

Recommendations and Best Practices

Visa strongly recommends that members, processors and agents actively identify and make use of all available tools to protect sensitive merchant account information and monitor suspicious reversals.

Recommendations for Acquirers

Acquirers are responsible for preventing fraudulent reversals from entering the payment system and should implement the following precautions:

- Implement strict controls to authenticate merchant transactions sent through gateway portals and virtual POS "integrator" software directly to processors.
- Monitor authorization messages for any or a combination of the following elements: excessive numbers of reversals, cross-border reversals, foreign currency indicators and unusual numbers of reversals going to a single card or issuer BIN.
- Alert merchants and third party agents to MID Probing, phishing and other social-engineering schemes that target merchant credentials.

- Monitor merchant accounts for unusual authorizations, reversals and merchant name changes.
- Confirm that incoming transaction data matches the existing merchant source of communication (e.g., dial-up versus Internet Protocol address).

Recommendations for Issuers

Issuers are responsible for monitoring their cardholders' credit, debit and prepaid card accounts for unusual reversals of ATM and Visa Direct authorizations.

- High-value, numerous or cross-border reversals should be monitored and measures taken to hold funds if the issuer suspects fraudulent activity.
- Any discrepancies and velocity alerts must be investigated promptly, before money is moved into the cardholder account and funds are released.
- Issuers must exercise tight controls while processing 0400 messages ensuring accurate matching of original and reversal messages and that the transaction identifier is used as a part of the matching criteria.

Report Suspected Activity

Members must immediately report suspected fraudulent reversals schemes to the appropriate law enforcement agency and to the Visa office in the region in which the fraud originated:

• AP and CEMEA: VIFraudControl@visa.com
• Canada, LAC and U.S.: USFraudControl@visa.com

Fraud originating in Europe should be reported to Visa Europe at FraudOperations@visa.com