VISA SECURITY ALERT

September 2016

PROTECT AGAINST ATM CASH-OUT FRAUD

Distribution: Acquirers, Issuers, Processors

Summary

Visa has seen an increase in global ATM cash-out fraud, which can extract millions of dollars from financial institutions in a short time. The key to limiting losses is quick detection and decisive action, carefully coordinated with Visa.

ATM cash-out fraud can happen at any time, anywhere in the world. It often affects issuers in one country and acquirers in another. To help clients combat this global and sophisticated type of fraud, Visa is providing guidance and best practices.

How Cash-Out Attacks Work

ATM cash-out fraud often results from a breach to the issuer back-end systems and system parameters, which attackers manipulate to increase card balances, reset PINs and transaction limits for selected cardholder accounts, and/or remotely control the ATMs themselves. Attackers then use the breached cardholder data to produce counterfeit magnetic-stripe cards. An orchestrated, coordinated attack follows, with attackers withdrawing significant amounts of cash from ATMs across the globe within a few hours. Cash-out fraud attacks also capitalize on issuer and acquirer time zone differences, country holidays and other times when normal support and monitoring staff may not be available.

Another popular ATM attack involves loading malware onto ATMs, often referred to as ATM jackpotting. Organizations should familiarize themselves with this and other current ATM fraud trends and take steps to protect themselves from such attacks.

Stopping Attacks Before They Start

Knowledge and vigilance help ensure that network intrusions do not occur. To further reduce risk, clients should:

- Comply consistently with security standards such as Payment Card Industry Data Security Standard (PCI DSS), PCI PIN and/or Visa's PIN Entry Device (PED) requirements.
- Limit remote access to a network.
- Monitor suspicious activity.
- Prevent phishing emails from entering a network.

Monitoring and Detection

The following tips help prevent ATM cash-out fraud:

- Understand normal ATM withdrawal behavior, especially for magnetic-stripe debit card portfolios.
- Identify out-of-range withdrawal conditions at both the cardholder account and the Bank Identification Number (BIN) level. ATM cash-out schemes often involve multiple compromised account numbers within the same BIN.
- Invest in and implement real-time internal fraud controls and systems to detect ATM fraud schemes.
- Report unusual balance inquiry activity or suspicious withdrawal patterns.
- Detect and send alerts when cards are used multiple times at various ATMs during a short time.
- Monitor PIN resets and subsequent activity.

Taking Action and Limiting Losses

- Verify that expected transaction validation is consistently performed.
- Ensure ATM security by keeping software patched and up-to-date.
- Only allow authorized entities and processes to remotely access ATMs and perform ATM software updates.
- Log software updates to ensure they are authorized and appropriate.
- Establish processes and/or implement automation to block ATM transactions after out-of-range thresholds are met.
- Work with your Visa representative to walk through ATM cash-out scenarios (e.g., tabletop exercises) to ensure sound processes and preparedness are in place in the event of an actual incident.
- Use robust multifactor authentication (MFA) for access into a cardholder data environment.
- Establish and internally communicate ATM fraud incident response and escalation procedures.
- Clients should validate their contact information with Visa.
- Follow *What to Do If Compromised* instructions (for AP, Canada, CEMEA, LAC, U.S. | for Europe) for suspected or confirmed fraud or data breaches.

Additional Resources:

"ATM Cashout Malware Compromise in Southeast Asia," Visa Security Alert, August 2016
"ATM Jackpotting Malware Alert," Visa Payment Fraud Disruption Technical Analysis, August 2016
Payment Card Industry ATM Security Guidelines
Visa Inc. PIN Entry Device (PED) Requirements
PCI Data Security Standard
What to Do If Compromised (AP, Canada, CEMEA, LAC, U.S. | Europe)

Online Resources

Visit the *PCI SSC Documents Library* for additional PCI standards, guidance and best practices.