Visa U.S.A. Inc. Data Security Alert

August 30, 2006

To support compliance with the Visa U.S.A. Cardholder Information Security Program, Visa is committed to helping all payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues security alerts when vulnerabilities are detected in the marketplace, or as a reminder about best practices.

Members may share this alert with their merchants, agents, and other parties to help ensure they are aware of security vulnerabilities and take appropriate steps to mitigate risk.

Security Vulnerability

Storage of Magnetic Stripe Data and other Sensitive Information by Merchant Point-of-Sale Systems

Visa is aware of compromises of credit and debit card account information resulting from the improper storage of magnetic stripe data ("track data") after transaction authorization is completed. Track data refers to the information encoded in Track 1 and 2 contained within the magnetic stripe on the back of a payment card.

This information is received by a merchant's point-of-sale ("POS") system when a payment card is swiped through a terminal. Some merchant POS systems improperly store this data post authorization in violation of longstanding Visa USA Operating Regulations. Hackers are aware of this vulnerability and are targeting vulnerable POS systems to steal this information.

Visa has also observed compromises involving other data elements that are prohibited to store, namely Card Verification Value 2 ("CVV2"), Personal Identification Numbers ("PINs") and PIN blocks. CVV2 is the 3-digit number typically found on the signature panel on the back of the payment card. A PIN is the secret code consumers use to conduct debit transactions, and PIN blocks are encrypted versions of a PIN.

Merchants may only store specific data elements from the magnetic stripe to support card acceptance. These data elements include: cardholder's name, primary account number, expiration date, and service code. However, this data should only be stored if needed, and must be protected in accordance with the Payment Card Industry Data Standard ("PCI DSS").

Merchants can limit the damage from a compromise by not storing track data, CVV2, PINs, and PIN blocks. Merchants can also decrease their risk by only storing cardholder data if it is needed to perform their business functions. *If you don't need it, don't store it!*

Merchants may mistakenly believe they need to store prohibited elements to process merchandise returns and transaction reversals. Acquirers should ensure their merchants have proper processes for each type of transaction.

Recommended Mitigation Strategy

To safeguard their systems and reduce risk from a compromise, merchants should verify they are not storing prohibited data. Visa offers the following suggestions to verify prohibited data is not stored:

- Ask your POS or payment software vendor (or reseller / integrator) to confirm your software version does not store magnetic stripe data, CVV2, PINs, or encrypted PIN blocks. If it does, these data elements must be removed immediately.
- Ask your payment software vendor to share a list of files written by the application, and a summary of the content to verify prohibited data is not stored.
- Review custom POS applications for any evidence of prohibited data storage. Eliminate any functionality that enables storage of this data.
- Search for and expunge all historical prohibited data elements that may be residing within your payment system infrastructure.
- Confirm that all cardholder data storage is necessary and appropriate for the transaction type.
- Verify that your POS software version has been validated as compliant against the Visa Payment Application Best Practices ("PABP"). A list of PABP compliant applications is available *on <u>http://www.visa.com/cisp.</u>*

For more information on Visa's Cardholder Information Security Program, please visit <u>http://www.visa.com/cisp</u>. Questions about this alert may be directed to CISP@Visa.com.

Alert 083006