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

August 27, 2007

To support compliance with the Payment Card Industry Data Security Standard (PCI DSS), Visa USA is committed to helping members and payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues Data Security Briefs when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

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

Security Vulnerability

Eliminating Storage of Prohibited Cardholder Data

Due to recent compromises of credit and debit account information resulting from improper storage of magnetic stripe "track data," Card Verification Value 2 (CVV2) and PIN data post authorization, Visa would like to remind members to ensure their merchants are using proper processing procedures in order to ensure that prohibited cardholder data is not being stored in merchant environments.

Track data is the information encoded in Track 1 and 2 within the magnetic stripe on the back of a Visa card which is read by a merchant's point-of-sale (POS) system. CVV2 is the 3-digit number typically found on the signature panel of the card, and PIN blocks are encrypted versions of a Personal Identification Number (PIN) used to conduct PIN-based debit transactions.

Some merchant POS systems improperly store this data post authorization in violation of *Visa U.S.A. Inc. Operating Regulations*. Hackers are aware of this vulnerability within merchant environments, and are targeting vulnerable POS systems in an attempt to steal this information.

Merchants may believe they need to store prohibited elements of track data for certain types of transactions or to re-present chargebacks. However, members should ensure that their merchants have proper processes in place for each type of transaction so prohibited data is not retained.

Storage of some data elements from the magnetic stripe is permitted, including the cardholder's name, primary account number, expiration date and service code. However, these values should be stored only if needed to perform business functions, and must be protected in accordance with the PCI DSS. Other data elements such as CVV, must not be stored following authorization.

For clarification of processing procedures and data storage requirements, please see Attachment A of this security brief.

Recommended Mitigation Strategy

To safeguard systems and eliminate risks associated with cardholder data storage, merchants should:

- Verify that prohibited data is not stored by:
  - Confirming with their POS or payment software vendor (or reseller / integrator) that their software version does not store magnetic-stripe data, CVV2 or PIN data. If this information is being stored, these data elements must be removed immediately.
  - Ensuring their POS software version has been validated as compliant against the Visa Payment Application Best Practices (PABP). A list of PABP-compliant applications is available at www.visa.com/cisp.
- Confirm that cardholder data storage is necessary and appropriate for each transaction type.
- Store allowable cardholder data elements only if necessary for business functions and in accordance with the PCI DSS.
- Consult with their merchant bank to determine whether truncated account numbers are acceptable to facilitate business functions in order to eliminate the need to store this information.
- Consider outsourcing some or all cardholder data storage and handling to a PCI DSS compliant service provider.

By minimizing cardholder data storage within merchant environments, merchants may mitigate the risks associated with cardholder data compromises. A common best practice to follow is, "If you don't need it, don't store it!"

For more information on Visa's CISP, please visit www.visa.com/cisp.

Questions about this alert may be directed to CISP@Visa.com.

Processing Procedures

Misconceptions regarding cardholder data storage

It has come to Visa's attention that merchants may mistakenly believe they need to store prohibited cardholder data post authorization to process certain transactions. The transaction examples below are provided to correct common misconceptions, and to help ensure merchants store only the necessary and permissible cardholder data elements.

Recurring Transactions

- *Card-Not-Present Merchants.* CVV2 may be used in the initial authorization request to set-up a recurring transaction for an Internet or telephone order. However, CVV2 is not required for subsequent transactions.
- *Card Present Merchants.* Track data may be required for the initial authorization request to set-up a recurring transaction in a card present environment (i.e., gym, insurance office). Full track data is not needed for subsequent transactions.

Merchants must ensure that all recurring transactions are clearly identified and confirm with their merchant bank that their system is properly configured.

Delayed Shipments

To facilitate delayed delivery of merchandise after the initial transaction date, merchants can:

- Require the customer to pay the full amount for the merchandise in a single transaction upon receipt of the order. Track and CVV2 data must not be stored post authorization.
- Facilitate two separate transactions. The first transaction functions as a deposit or down payment; the second is to pay the balance due. Track and CVV2 data must not be stored post authorization.

Orders placed and paid in full must ship within seven days following transaction authorization. Other requirements for delayed delivery apply.

Chargebacks

- *Card-Not-Present Merchants.* CVV2 data is not required for handling a chargeback request. For chargeback representment, the merchant can provide documentation demonstrating the following:
  - The merchant submitted a CVV2 verification request during authorization and received a "U" response from the U.S. card issuer denoting non-support of CVV2.
  - The cardholder acknowledged the validity of the transaction either by letter or other form of communication.
- *Card Present Merchants.* Full magnetic-stripe data is not required for handling a chargeback request.
  - If track data was successfully obtained for authorization, the merchant can request their merchant bank to send a copy of the authorization record to the card issuer as proof that the card's full magnetic stripe was read. The merchant must also provide a copy of the sales receipt containing the cardholder's signature.
  - If a card present transaction required a manual key-entry, the merchant can provide a legible copy of the sales receipt containing a manual imprint of the embossed account number and expiration date along with the cardholder's signature.

A signed POS terminal receipt with a truncated account number and the accompanying authorization log showing "POS 90" is valid fulfillment and will remedy a fraud chargeback. As such, a merchant may mitigate their risk by storing only truncated account numbers. Merchants should consult with their merchant bank before taking this action.

Copy Requests

Full track and CVV2 data are not required for fulfilling copy requests for sales receipts.

Additional Resources

For additional information or clarification, merchants should contact their merchant bank to receive a copy of the *Rules for Visa Merchants: Card Acceptance and Chargeback Management Guidelines* or download this document online at www.visa.com/merchants.