

Visa Data Security Bulletin

Eliminating Storage of Prohibited Data

April 2, 2009

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

Payment system participants may share this bulletin with their merchants, agents and other parties to help ensure that they are aware of emerging vulnerabilities and take steps, where appropriate, to mitigate risk.

Security Vulnerability

Eliminating Storage of Prohibited Cardholder Data

Improper storage of magnetic stripe (track data), Card Verification Value 2 (CVV2) and PIN blocks post authorization have resulted in the compromise of credit and debit account information. Visa reminds clients to ensure that their merchants use proper processing procedures that do not lead to the storage of this prohibited data.

Track data is the information encoded in Track 1 and 2 within the magnetic stripe on the back of a Visa card. This information is read by a merchant's point-of-sale (POS) system. Some merchant POS systems improperly store this data post authorization. This is a violation of Visa 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 for storage, namely CVV2 and PIN blocks. **CVV2** is the 3-digit number typically found on the signature panel of the card. **PIN blocks** are encrypted versions of a Personal Identification Number (PIN) used to conduct PIN-based debit transactions.

Merchants may store specific track data elements to support card acceptance. These data elements include cardholder 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 PCI DSS. Other data elements such as CVV **must not** be stored after authorization.

Merchants may mistakenly believe that they need to store prohibited cardholder data post authorization to process certain transactions or to represent chargebacks.

For clarification of processing procedures and data storage requirements please see *Attachment A*.

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

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 track data, CVV2 or PIN data. If the vendor does store these data elements, that data must be removed immediately.
 - Ensuring that their POS software version has been validated as compliant with the PCI Payment Application Data Security Standard (PA-DSS). The PA-DSS was adopted from the Visa Payment Application Best Practices (PABP) in April 2008. A list of compliant applications is available at www.visa-asia.com/secured.
- Confirm that cardholder data storage is necessary and appropriate for each transaction type.
- Only store allowable cardholder data elements if necessary for business functions and in accordance with PCI DSS.
- Eliminate the need to store account numbers by consulting with your merchant bank to determine whether truncated account numbers are acceptable to facilitate business functions.
- 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.

Data Security Bulletin – Attachment A

Processing Procedures

Misconceptions Regarding Cardholder Data Storage

Some merchants mistakenly believe that to process certain transactions they need to store prohibited cardholder data post authorization. The transaction examples below are provided to correct common misconceptions and to help ensure that merchants store only the necessary and permissible cardholder data elements.

Recurring Transactions

- *Card-Not-Present Merchants:* In the initial authorization request, CVV2 may be used to set up a recurring transaction for an Internet or telephone order. However, CVV2 is not required for subsequent transactions.
- *Card-Present Merchants:* For an initial authorization request, track data may be required to set up a recurring transaction in a card-present environment (e.g., gym or 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 set up.

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 transaction pays the balance due. Track and CVV2 data **must not** be stored post authorization.

Orders placed and paid in full must ship within 7 days after 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 representation, the merchant can provide documentation demonstrating the following:

- The merchant submitted a CVV2 verification request during authorization and received a “U” response from the card issuer denoting non-support of CVV2.
- The cardholder acknowledges the validity of the transaction either by letter or by some 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 that their merchant bank 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 to fulfill copy requests for sales receipts.