

Data Security Brief for U.S. Financial Institutions

POS and ATM Hardware

November 9, 2007

To support compliance with the *Payment Card Industry Data Security Standard (PCI DSS)* and *PCI Personal Identification Number Security Requirements*, Visa is committed to helping 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 regarding best practices.

Acquirers may share this brief with their merchants, agents and other parties to help ensure their awareness of these vulnerabilities, and take steps, where appropriate, to mitigate risk.

Eliminate Storage of Prohibited Cardholder Data on POS and ATM hardware

Due to recent reports received by Visa regarding Automated Teller Machine (ATM) hard drives and other point-of-sale (POS) devices being re-sold while containing prohibited stored data, Visa would like to remind members to ensure their merchants and ATM deployers are using proper procedures to prevent the storage of prohibited cardholder data.

Prohibited data includes unencrypted account numbers, magnetic stripe "track data," Card Verification Value 2 (CVV2) data and PIN blocks. Track data is the information encoded in Track 1 and 2 within the magnetic stripe on the back of a Visa card that is read by a POS or ATM device. CVV2 is the three-digit number typically found on the signature panel of the card, and PIN blocks are encrypted versions of a PIN used to conduct PIN-based transactions. Storage of this data is in violation of the PCI DSS and PCI PIN Security requirements.

PIN Entry Devices must be properly decommissioned

PCI PIN Security requirements state that all PIN Entry Devices (PEDs) and Hardware Security Modules (HSMs) being removed from service must have all cryptographic keys, and any other sensitive data, securely removed prior to being decommissioned.

Procedures must exist and be followed to ensure the secure destruction of all cryptographic keys and any PINs or PIN-related information within these devices. Refer to the PCI PIN Security requirements on www.visa.com/pin for details.

Recommended Mitigation Strategy

To safeguard systems and reduce risk associated with storing prohibited data, merchants and ATM deployers should:

- Ask your POS or ATM hardware / software vendors (or reseller / integrator) to confirm your software version does not store prohibited magnetic stripe data, CVV2 or encrypted PIN blocks. If this information is being stored, these data elements must be removed immediately.
- Ask your POS or ATM hardware / software vendors to share a list of files written by the application, as well as a summary of the content to verify prohibited data is not stored.
- Review custom POS or ATM applications for any evidence of prohibited data storage. Eliminate any functionality that enables storage of this data.
- Search for and remove all prohibited data elements that may be residing within your ATM or payment system infrastructure.
- Verify your POS / ATM software version has been validated as compliant against the Visa Payment Application Best Practices (PABP). A list of PABP-compliant applications is available at <http://www.visa.com/cisp>.
- Entities must ensure that no prohibited data is stored on any ATM or POS hardware that **is in service or has been removed from service**.

For additional information, please visit www.visa.com/cisp and www.visa.com/pin.