



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

November 17, 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 emerging vulnerabilities and take steps where appropriate to mitigate risk.

Security Vulnerabilities

Risks Affecting Petroleum Merchants

Petroleum merchants (gas stations) have been increasingly targeted by fraud rings seeking sensitive cardholder data. To help merchants reduce the threat of data compromise, this alert highlights four common vulnerabilities and provides recommendations to help secure merchant payment systems.

Storage of Full Magnetic Stripe Data—Merchants are reminded that storage of full magnetic stripe data post authorization is prohibited by Visa Operating Regulations. Further, retention of full magnetic stripe data can significantly increase a merchants' risk of compromise, as hackers are now aware that certain payment applications store track data by default, and merchants may not be aware of it. Merchants can reduce their risk of compromise by ensuring they are fully compliant with the Payment Card Industry Data Security Standard ("PCI DSS") and by ensuring any payment card data is securely stored in a PCI compliant manner.

Handling of Brass Keys—Certain Automated Fuel Dispenser ("AFD") models share common pump keys (aka "brass keys") that allow service station employees and technicians to gain access to the interior of the pump. This ease-of-entry feature supports legitimate maintenance activity. However, criminals have exploited the use of 'common' brass keys to access the AFD in order to attach devices that capture or 'skim' cardholder information.

Personal Identification Number ("PIN") and Card Skimming at AFDs—Merchants that fail to restrict AFD access to designated employees may be vulnerable to skimming attacks. These attacks occur when criminals and/or 'collusive' employees access the interior of the pump and attach devices that capture PIN and account information.

Point-of-Sale ("POS") PIN-Entry Devices ("PED")—

Merchants that accept PIN transactions at the register are cautioned that fraud rings may attempt to pose as service technicians in order to introduce 'tampered' POS PEDs into the merchant's POS environment. Merchants should ensure all POS PEDs are firmly affixed to the counter top and only approved technicians are permitted access to POS systems and devices.

Recommended Mitigation Strategy

To minimize the risk of data compromise, merchants and agents should take the following actions:

- Confirm your software version does not store full magnetic stripe data or PINs.
- Review proprietary POS applications for any evidence of prohibited data storage. Eliminate any functionality that enables storage of full magnetic stripe data or PINs.
- Search for and expunge all historical prohibited data elements that may be residing within your payment system infrastructure.
- Initiate an independent CISP validation audit and verify that your POS software version has been validated as compliant against the Visa Payment Application Best Practices ("PABP"). For more information please visit <http://www.visa.com/cisp>.
- Ensure AFD access keys are never shared among large populations of devices and all brass keys are securely managed.
- Verify AFD access is restricted to designated employees or service technicians as appropriate.
- Conduct regular inspections of AFD interiors to look for any sign of tampering. Train security cameras on AFDs where possible.
- Ensure merchants are only purchasing hardware with adequate physical and logical security features.
- Ensure all AFDs use Encrypting PIN Pads ("EPPs").
- Purchase only Triple Data Encryption Standard ("TDES") compliant PEDs that have passed laboratory testing and have been approved by Visa. Target current non-TDES capable PED inventories for early retirement. See www.visa.com/pin for a listing of all Visa approved PIN entry devices.

For more information on Visa's Cardholder Information Security Program,

please visit <http://www.visa.com/cisp>. Questions about this alert may be directed to CISP@Visa.com.

Alert 111506