



Visa USA Data Security Alert

POS PIN Entry Device Vulnerabilities

November 19, 2007

To support compliance with the *Payment Card Industry PIN Security Requirements*, Visa is committed to helping members and payment system participants better understand their responsibilities related to securing PIN data. As part of this commitment, Visa issues alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Acquirers 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.

POS Vulnerabilities

Visa has received an increasing number of reports regarding point-of-sale (POS) PIN Entry Device (PED) thefts from merchant store locations, typically occurring late at night. Evidence indicates POS PEDs are being physically removed from their locations and are being replaced with modified devices designed to skim account and PIN data. Surveillance has also shown that suspects in most of these cases were able to remove and install a POS PED in under one minute.

This type of fraud is typically occurring in merchant locations with “after-hours” operations, and where there is minimal customer traffic and employee supervision over cash registers. The types of merchant locations that have been targeted include supermarkets (MCC 5411), drug stores (MCC 5912) and convenience stores (MCC 5499). However, any store may be affected by this scheme if they have deployed older POS PEDs that are not tamper-evident or tamper-resistant, as required by Visa security requirements. PEDs that are known to be targeted by criminals include VeriFone PINpad 101, 201 and 2000, VeriFone Everest model P003-3xx, Hypercom S7S and S8, and the Ingenico eN-Crypt 2400 (also known as the C2000 Protégé).

Recommended Mitigation Strategies and Best Practices

Visa strongly recommends merchants use heightened vigilance and maintain a secure store environment at all times, especially around cash registers and POS PEDs. Additionally, Visa recommends the following best practices:

- Merchants should have the ability to monitor PED internal serial numbers and detect when PEDs are disconnected or removed.

- Merchants must ensure that only authorized personnel service deployed terminals and PEDs in accordance with *Payment Card Industry PIN Security Requirements* (see www.visa.com/pin). Merchants must properly manage PED inventories and physically secure PEDs at all locations so they cannot be easily modified or replaced.
- Merchants are advised to purchase only PCI-approved PEDs that have been lab-evaluated. *The Visa U.S.A. Inc. Operating Regulations* and *Visa U.S.A. Inc. Interlink Networks Operating Rules* require that PEDs deployed by members and their agents comply with *Payment Card Industry PED Security Requirements*. Visa requires that newly purchased attended POS PEDs from Original Equipment Manufacturers must be Visa-approved and lab-evaluated as of January 1, 2004. Visa/Interlink merchants must deploy PEDs listed on the *Visa PIN-Entry Device Approval List* found at www.visa.com/pin.
- Merchants are encouraged to work with their merchant bank and/or Encryption and Support Organization (ESO) to create a plan that ensures **all** deployed POS PEDs are Visa-approved, lab-evaluated and comply with the *Triple Data Encryption Standards (TDES)* by July 2010.
- Merchants should train their employees about the potential of PIN compromise when POS PEDs are stolen or missing, or when there are any noticeable signs of device-tampering. Merchants should also be advised to inspect POS PED inventories regularly.
- Merchants are advised to immediately contact their merchant bank, Visa and law enforcement if they suspect tampering of any POS PEDs.

To aid member and merchant compliance efforts, Visa provides ongoing educational workshops to help entities gain further knowledge in all aspects of secure key management. For workshop information, please e-mail pinusa@visa.com.

Additionally, Visa has recently updated the *Visa PIN Security Tools and Best Practices for Merchants* brochure, now available online at www.visa.com/pin. Hard copies can be requested from the Visa Fulfillment Center at 800-235-3580. This brochure reviews all of Visa’s upcoming PED testing and TDES mandates and their impacts to merchants.

For more information on Visa’s PIN Security Program, please visit www.visa.com/pin.