Visa Fraud Alert
US-VFA-2007-005
(As of April 13, 2007)

Synopsis

Visa has been receiving 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 has indicated that POS PEDs are being physically removed from their location 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 within 12 seconds.

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-responsive. PEDs that are known to be targeted by these criminals include VeriFone PINpad 101 and 201, VeriFone PINpad 2000, Hypercom S7S and S8, and the Ingenico eN-Crypt 2400 (also known as the C2000 Protégé).

Recommended 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 must ensure that only authorized personnel service deployed terminals and PEDs in accordance with *Payment Card Industry PIN Security Requirements* (www.visa.com/pin). Merchants must properly manage PED inventories and physically secure PEDs at all locations so they cannot be easily removed, modified or replaced.

- Merchants must have the ability to monitor PED internal serial numbers.

- Merchants are advised to purchase only Visa-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 PIN Security Requirements*, which state that newly purchased POS PEDs from Original Equipment Manufacturers (OEM) 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* 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.

- Visa offers educational workshops for personnel involved in any aspect of PIN security compliance. Merchants should be advised to contact their merchant bank for a Visa workshop schedule and registration details, or contact pinusa@visa.com for registration information.

- Merchants are advised to immediately contact their merchant bank, Visa and law enforcement if they suspect tampering of any POS PEDs.

For more information, please contact Visa Fraud Investigations and Incident Management:

(650) 432-2978
usfraudcontrol@visa.com