VISA PIN SECURITY BULLETIN 1 May 2018

Original publication 16 November 2012

Help Protect Cardholder Data From Attacks on PIN Entry Devices

To promote the security and integrity of the payment system, Visa is reminding clients, merchants and payment system participants of their responsibility to protect cardholder account and PIN data.

Criminals trying to obtain cardholder account and PIN data at the point of sale (POS) frequently target PIN Entry Devices (PEDs) that are known to be vulnerable. Evidence obtained from a previous case indicates the devices were removed from the point of sale and replaced with modified devices designed to capture magnetic stripe card and PIN data, which was then transmitted to criminals wirelessly. Surveillance footage shows that the suspects were able to remove a PED and install a modified device in less than one minute.

Recommended Mitigation Strategies

Merchants must be vigilant and maintain a secure store environment at all times, especially around cash registers and PEDs. Inventory-control and monitoring procedures will help protect against PED substitution, loss and modification.

- **Mount or tether PEDs to counters to prevent removal.** Payment Card Industry (PCI) PIN Security Requirements and PCI Data Security Standard require that precautions are taken to minimize the threat of compromise once PEDs are deployed.
- **Implement a PED-authentication system.** Merchant host systems can continuously verify that terminals are online and operating correctly.
- **Use terminal asset tracking procedures.** Secure stored terminals awaiting deployment under lock and key, and periodically validate PED inventories on hand against asset records.
- **Regularly inspect PEDs visually to identify abnormalities.** Look for altered seals or screws, extraneous wiring, holes or labels or other materials that could be added to mask damage from device tampering.
- **Retire PEDs known to be vulnerable.** To avoid potential compromises, merchants should plan to replace vulnerable PEDs now and consider implementing dual-interface chip capable devices whenever possible.

Visa strongly urges acquirers to share this information with merchants, Encryption and Support Organizations, POS vendors, resellers and integrators to ensure that PEDs are maintained securely in accordance with the PCI PIN Security Requirements.

A merchant that detects a security breach should notify its acquiring bank immediately. Merchants can also follow the steps outlined in *Visa's What to Do If Compromised Document* on visa.com.