

Compromised PIN-Entry Device Listing Updated; Reminder of Upcoming Mandatory Sunset Dates

Visa has recently identified PIN-entry devices (PEDs) that are susceptible to compromise. Specifically, two hardware versions of the VeriFone Everest Plus PED have been identified in recent compromises:

- VeriFone Everest Plus part numbers P003-400-01, P003-400-02 and P003-400-03 are untested and unapproved. These devices support only single Data Encryption Standard (DES) cryptography and were required to have been retired effective 1 July 2010.
- VeriFone Everest Plus part numbers P003-400-12 and P003-400-013 are pre-Payment Card Industry (PCI) approved. These devices have a **mandatory sunset date of 31 December 2014**.

Both VeriFone Everest Plus point-of-sale (POS) PED hardware versions have been used in tampering and skimming attacks to capture PIN and magnetic-stripe card data. These devices have been compromised in the U.S.; however, this compromise warning is applicable to all deployments. All Visa and Interlink clients must take action to mitigate the risks introduced by these recently compromised POS PEDs.

POS PED Thefts

Visa has also received new reports regarding POS PED thefts from merchant locations. This type of fraud typically occurs in merchant locations operating after hours with minimal customer traffic or employee supervision over cash registers; however, any store may be affected by this scheme.

Recent evidence indicates that these devices were physically removed during business hours and replaced with modified devices designed to skim account and PIN data, which was then transmitted wirelessly to the fraudsters via Bluetooth. In most cases, surveillance footage showed that the suspects were able to remove and install a modified POS PED in seconds.

Terminal Authentication Systems

Many of these vulnerabilities can be addressed by deploying a terminal authentication system, which allows the host system to continuously verify the PED's internal serial number and confirm that the terminal is online and operating correctly. If a terminal is ever replaced with an unauthorized device (or is unplugged, as would be necessary to execute an attack), the host system would immediately be alerted to tampering.

POS PED Vulnerabilities

Clients that sponsor merchants or agents that use known compromised PEDs or deploy PEDs past mandated Visa sunset dates that lead to a breach may be subject to increased liability under the Account Data Compromise Recovery (ADCR) program, in addition to potential fines.

For more information regarding Visa's PED usage and retirement requirements, refer to the *General PED Frequently Asked Questions* document, included in the "Related Documents" section below.

The table below lists known compromised POS PED makes and models.

Attended POS PED Category	Compromised PED Description	Mandatory PED Sunset Date
<p>Untested / Unapproved POS PEDs—Devices deployed before Visa and the PCI Security Standards Council (SSC) implemented a PED testing program.</p> <p>These devices have been targeted by criminals and are known to have been compromised. Visa previously identified and published these compromised POS PEDs in editions of the <i>Visa Business News</i> and the <i>Visa Business Review</i>, and in security alerts published at www.visa.com/cisp.</p> <p>Note: In 2003, Visa announced that all untested and unapproved attended POS PEDs must be removed from production by 1 July 2010. Clients may be liable under the ADCR program, and may be fined, if merchants are found using these PEDs.</p>	<ul style="list-style-type: none"> • VeriFone PINpad 101, 201 and 2000 • VeriFone Everest Model P003-3xx • VeriFone Everest Plus part numbers P003-400-01, P003-400-02 and P003-400-03 • Hypercom S7S and S8 • Ingenico eN-Crypt 2400 (also known as the C2000 Protégé) 	<p>1 July 2010¹</p>
<p>Pre-PCI Approved POS PEDs—Devices validated as compliant via lab testing and approved by Visa under pre-PCI requirements (listed at www.visa.com/cisp).</p> <p>Approval for the new deployment of POS PEDs listed in this category expired on 31 December 2007. These devices are actively targeted by criminals for compromise; clients are encouraged to retire these devices immediately.</p> <p>Note: In May 2010, Visa announced a mandatory sunset date of 31 December 2014 for all pre-PCI approved attended POS PEDs; however, the POS PEDs listed here should be replaced as soon as possible.</p>	<ul style="list-style-type: none"> • Ingenico eN-Crypt 2100 • VeriFone Everest Plus part numbers P003-400-12 and P003-400-013 	<p>31 December 2014¹</p>
<p>PCI-Approved POS PEDs—Devices validated as compliant via lab testing according to PCI requirements (i.e., Version 1.x or higher) and approved by the PCI SSC.</p> <p>In May 2010, Visa announced that the Ingenico i3070MP01 and i3070EP01 devices were compromised. As a precaution (and to prevent further deployments), the PCI SSC, in coordination with Ingenico, revoked the approval of these devices.</p> <p>The Ingenico i3070MP01 and i3070EP01 devices are no longer approved PED terminals; both have been removed from the <i>List of Approved PIN Transaction Security Devices</i>.</p>	<ul style="list-style-type: none"> • Ingenico i3070MP01 • Ingenico i3070EP01 	<p>TBD²</p>

¹ Mandatory sunset date for all PEDs in this category (includes both known compromised PEDs and non-compromised PEDs).

² Visa will evaluate appropriate sunset dates for expired PCI-approved POS PEDs.

Recommended Mitigation Strategies

Visa strongly recommends that merchants be vigilant and maintain a secure store environment at all times, especially around cash registers and POS PEDs. To encourage such vigilance, the PCI SSC has published skimming prevention best practices that include:

- Visually inspecting terminals on a regular basis to identify anything abnormal, such as missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other materials that could be used to mask damage from device tampering.
- Physically securing terminals and PIN pads to counters to prevent removal; physically securing all cable connections.
- Physically securing (under lock and key) stored terminals awaiting deployment; periodically validating the inventory on hand against asset records.
- Using terminal asset tracking procedures for devices that are deployed, devices that are awaiting deployment, devices that are being repaired and devices that are in transit.
- Validating the identity of repair technicians. Unauthorized or unexpected service personnel should be denied access; authorized and validated repair technicians should be escorted and monitored.
- Periodically weighing the equipment and comparing it with vendors' specification weights to identify the possible insertion of bugging devices.
- Periodically scanning for any unidentified Bluetooth signals and pairings at store locations.

Visa and Interlink acquirers should encourage merchants and agents that have deployed compromised POS PEDs to consider following these best practices to help defend against skimming attacks. For more information, refer to the *POS Terminal Tampering Is a Crime...and You Can Stop It* document, included in the "Related Documents" section below.

Merchants should educate their employees on the potential for PIN compromise and ensure that staff members know what actions to take if a POS PED is stolen, missing or has noticeable signs of tampering.

Merchants are also advised to inspect POS PED inventories regularly. If POS PED tampering is suspected, merchants should immediately contact their bank, Visa and law enforcement. Clients should also refer to the *What to Do If Compromised* document, included in the "Related Documents" section below.

PED Procurement, Replacement and Retirement Planning

As entities make plans for POS system upgrades, migration to EMV contact and contactless chip technology is encouraged. Visa recently announced plans to accelerate the migration to contact chip and contactless EMV chip technology in the U.S. The adoption of dual-interface chip technology will help prepare the U.S. payment infrastructure for the arrival of Near Field Communication (NFC)-based mobile payments by building the necessary infrastructure to accept and process chip transactions. For more information, refer to the article "Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments," listed in the "Related Documents" section below.

Visa requires Visa and Interlink acquirers, processors and their merchants to purchase only devices that are currently included on the *List of Approved PIN Transaction Security Devices*, included in the "Related Documents" section below. To help ensure that sensitive cardholder PIN data is adequately protected, Visa encourages acquirers, processors and merchants to work with device manufacturers and to consider deploying only the most secure (or most recent) versions of terminals.

When selecting PED replacements, strong consideration should be given to replacing any pre-PCI approved device with the most recently approved device available, including using PCI PED Version 3.0 devices. To remain in full compliance with Payment Card Industry PIN Security Requirements and Visa PED usage mandates, clients must ensure that all PEDs purchased use the exact PED identifier, make, model and firmware version listed on the *List of Approved PIN Transaction Security Devices*.

For more information on best practices for PED retirement planning, refer to article "Retirement of Pre-PCI Attended POS PIN Entry Devices," listed in the "Related Documents" section below.

Compliance Requirements

The *Visa International Operating Regulations* and the *Interlink Network, Inc. Bylaws and Operating Regulations* require that PEDs deployed by clients and their agents comply with the *PCI PIN Security Requirements*, included in the “Related Documents” section below. As of 1 January 2004, newly deployed attended POS PEDs must be PCI approved. To review Visa global PED testing requirements, refer to Appendix A of the *PCI PIN Security Requirements*.

Visa is aware that some unapproved PED acquisitions still occur. Entities that deploy noncompliant devices or deploy PEDs past Visa-mandated sunset dates are in violation of Visa PED deployment mandates and may be fined and found liable in the event of a PIN compromise.

Merchants are encouraged to work with their banks and Encryption Support Organizations to ensure that all deployed attended POS PEDs are PCI-approved or pre-PCI approved and using triple DES (TDES) cryptography.

Visa clients, processors, agents and merchants must plan now to complete their upgrades from older, pre-PCI approved attended POS PEDs. To ensure that the 31 December 2014 deadline is met, entities should stop deploying pre-PCI PEDs in 2013.

Attend Upcoming PIN Security Training

Visa provides ongoing PIN security training to help clients learn all aspects of secure key management and aid in compliance efforts. Upcoming Visa Key Management training sessions will be held in Miami, Florida, in September 2011, and in Foster City, California, in October 2011. For training and registration information, visit the www.visa.com/cisp website.

Related Documents

[General PED Frequently Asked Questions](#)

[List of Approved PIN Transaction Security Devices](#)

[List of Visa Approved PIN Entry Devices](#)

[PCI PIN Security Requirements](#)

[PCI SSC Information Supplement: Skimming Prevention—Best Practices for Merchants](#)

[POS Terminal Tampering Is a Crime ... and You Can Stop It](#)

[What to Do If Compromised](#)

[Visa Announces Plans to Accelerate Chip Migration and Adoption of Mobile Payments](#)

[Retirement of Pre-PCI Attended POS PIN Entry Devices](#)

[Update on Visa’s Compliance Policy to Facilitate Triple Data Encryption Standard Usage](#)