Visa Updates Compromised PIN Entry Device Listing and Reminds Members of Upcoming Mandatory Sunset Dates

Compromised point of sale (POS) PIN entry devices (PEDs) have been used in tampering and skimming attacks to capture PIN and magnetic stripe card data. Visa members must take action to mitigate the risks introduced by these compromised POS PEDs. Although some of the recently identified devices are newer devices, many are over 10 years old and were never evaluated by an independent lab or approved by Visa or the Payment Card Industry (PCI).

Visa continues to receive 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.

Evidence indicates that these devices were physically removed from their locations and replaced with modified devices designed to skim account and PIN data. Surveillance footage shows that the suspects in most cases were able to remove and install a POS PED in less than one minute.

POS PED Vulnerabilities

The following table lists the known compromised POS PED makes and models.

Attended POS PED Category	Compromised PED Description	Mandatory PED Sunset Date
Untested and Unapproved PED	• VeriFone: PINpad 101, 201 and 2000 • VeriFone: Everest model P003-3xx • Hypercom: S7S and S8 • Ingenico: eN-Crypt 2400 (also known as the C2000 Protégé)	1 July 2010[1]
Pre-PCI (Visa-only Program)	• Ingenico: eN-Crypt 2100	31 December 2014[1]
PCI-approved	• Ingenico: i3070MP01 • Ingenico: i3070EP01	TBD[2]

[1] *Mandatory sunset date for **all** PEDs in this category, including both known compromised PEDs and non-compromised PEDs.*

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

- **Untested and unapproved PEDs** are devices deployed before Visa and the PCI Security Standards Council (SSC) implemented a PED testing program. Compromised POS PEDs listed in this category have been targeted by criminals and are known to be compromised. Visa previously identified and published these

compromised POS PEDs in editions of the *Visa Business News,* the *Visa Business Review,* and in security alerts published at www.visa.com/cisp.

Note: In 2003, Visa announced that **all untested and unapproved attended devices must be removed from production by 1 July 2010**. To meet this mandate, Visa clients, processors, agents and merchants must complete their upgrade processes.

- **Pre-PCI POS PEDs** are devices validated as compliant via lab testing and approved by Visa under pre-PCI requirements (listed at www.visa.com/pin). Approval for new deployments of POS PED listed in this category expired on 31 December 2007. This device has been targeted by criminals for compromise; members are encouraged to retire this device as quickly as possible.

  Note: In the 5 May 2010 *Visa Bulletin* article entitled, "Retirement of Pre-PCI Attended POS PIN Entry Devices," Visa announced a mandatory sunset date of 31 December 2014 for **all pre-PCI attended POS PEDs**; however, the POS PED listed in the table above should be replaced as soon as possible

- **PCI-approved PEDs** are devices validated as compliant via lab testing according to PCI requirements (Version 1.x or higher), and approved by the PCI. In the 26 May 2010 *Visa Business News* article entitled, "Payment Card Industry Security Standards Council Delists Two Compromised PIN Entry Devices," Visa announced that the Ingenico i3070MP01 and i3070EP01 devices have been compromised. As a precaution (and to prevent further deployments), the PCI SSC, in coordination with Ingenico, revoked the approval of these devices. Effective immediately, Ingenico i3070MP01 and i3070EP01 are no longer approved PED terminals and have been removed from the *PCI SSC PIN Transaction Security Devices List*. In the future, Visa will evaluate and announce appropriate sunset dates for all expired PCI-approved POS PEDs.

For more information on delisted PCI PEDs and mandatory retirement requirements, please review the *May 2010 Visa PED Frequently Asked Questions* document available at www.visa.com/cisp under the "PIN Security" section.

Recommended Mitigation Strategies

Visa strongly recommends that merchants use heightened vigilance and maintain a secure store environment at all times, especially around cash registers and POS PEDs. The PCI SSC has published skimming prevention best practices that include:

- Regularly inspecting terminals visually 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 covering material that could be used to mask damage from device tampering.
- Physically securing terminals and PIN pads to counters to prevent removal, and physically securing cable connections.
- Physically securing (under lock and key) stored terminals awaiting deployment, and periodically validating the inventory on hand against asset records.
- Using terminal asset tracking procedures for devices deployed, devices awaiting deployment, devices under repair, and devices in transit to location.
- 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 to vendors' specification weight to identify the insertion of bugging devices.

Acquirers should encourage merchants and agents who have deployed compromised POS PEDs to consider following these best practices to help defend against skimming attacks.

Many of these vulnerabilities can be addressed if terminals are deployed with a terminal authentication system. In this case, the host system continuously verifies the PED's internal serial number and confirms that terminals are online and operating correctly. If a terminal is ever replaced with an unauthorized device (or is unplugged, as would be necessary to execute this attack), the host system would immediately be alerted to tampering.

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 device-tampering. Merchants are also advised to inspect POS PED inventories regularly. If POS PED tampering is suspected, merchants should immediately contact their merchant bank, Visa, and law enforcement. Members should also refer to the *What to Do If Compromised* document available at www.visa.com/cisp under the "If Compromised" section.

PED Procurement, Replacement and Retirement Planning

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

When selecting PED replacements strong consideration should be given to replacing any pre-PCI device with the most recently approved device available, including using PCI PED Version 2.0 devices (or later), which will be available in the future (possibly when the older devices are being replaced).

Visa and Interlink merchants must only deploy PEDs included on the *PCI SSC PIN Transaction Security Devices List*. Members must ensure that all PEDs purchased use the exact PED identifier, make, model and firmware version listed on the *PCI SSC PIN Transaction Security Devices List*.

For more information on best practices for PED retirement planning, see the 5 May 2010 *Visa Bulletin* entitled, "Retirement of Pre-PCI Attended POS PIN Entry Devices."

Compliance Requirements

The *Visa International Operating Regulations* and the *Interlink Network, Inc. Bylaws and Operating Regulations* require that PEDs deployed by members and their agents comply with the *PCI PED Security Requirements*. As of 1 January 2004, newly deployed attended POS PEDs must be PCI approved.

To review Visa global PED testing requirements, refer to the *PCI PIN Security Requirements*, Appendix A, available at www.visa.com/cisp under the "PIN Security" section

Visa is aware that some unapproved PED acquisitions still occur. Entities that deploy non-compliant devices are in violation of Visa PED deployment mandates and may be found liable in the event of a PIN compromise.

Merchants are encouraged to work with their merchant banks and/or Encryption Support Organizations (ESOs) to ensure that all deployed POS PEDs are PCI-approved and comply with Visa Triple Data Encryption Standard (TDES) requirements.

Attend Upcoming PIN Security Training

To support compliance with the *PCI PIN Security Requirements*, Visa is committed to helping members, merchants, and payment system participants better understand their responsibilities related to securing PIN data. Visa provides ongoing educational PIN Security training to help members gain further knowledge in all aspects of secure key management and aid client and merchant compliance efforts.

The next Visa Key Management training sessions will be held in Foster City, California, in September and October 2010. For training and registration information, please visit www.visa.com/cisp or e-mail VisaBusinessSchool@visa.com for more information.

Related Documents

To access the content below, please visit www.visa.com/cisp.

- *November 2009 - Update on Visa's Compliance Validation Program*
- *November 2009 - Visa NA PIN Security Training Schedule*
- *September 2009 – Interlink Merchant TDES Compliance (webinar)*
- *August 2009 - US POS TDES Frequently Asked Questions*
- *May 2010– General PED Frequently Asked Questions*
- *April 2009 - Update on Visa's TDES Policy*
- *May 2010- Retirement of Pre-PCI Attended POS PIN Entry Devices*
- *March 2010 - Reminder: Registration and Compliance Requirements for Encryption Support Organizations*
- *Visa PIN Security Tools and Best Practices for Merchants*
- *PCI PIN Security Requirements* v2 Jan. 2008
- Visa specific requirements - Annex A
- *Visa PIN Security Program: Auditor's Guide*
- Other PIN security related Bulletins documents

To access the content below, please visit www.pcisecuritystandards.org/pin.

- PCI PIN-Entry Device Approval List

For More Information

Contact pinusa@visa.com.