

# Reminder: PIN Entry Device Testing Program Changes Effective December 31, 2007

## Suggested Audience:

Acquirers, Processors

DEBIT OPERATIONS,  
MERCHANT RELATIONS,  
RISK MANAGEMENT

Martin Elliott, Vice President, Enterprise Risk and Compliance

---

**In Brief:** As announced in the June 19, 2007, edition of the Visa Business Review, Visa's PIN Entry Device (PED) testing program, which was introduced in 2003, is transitioning to the PCI Security Standards Council. As part of this transition, PEDs tested under the original, Visa-only program will be removed from the Approved PIN Entry Devices list, effective December 31, 2007. Acquirers, processors, merchants and agents will need to plan now to purchase point-of-sale (POS) PEDs in compliance with these program changes.

---

## Expiration of Pre-PCI Approved PEDs Approaching

The Visa PIN Entry Device (PED) Security Evaluation Program was initiated in 2003 to ensure that PEDs were evaluated by independent testing laboratories to validate that all PEDs met the same minimum security requirements. In 2004, the Visa program became the foundation for what is today's Payment Card Industry (PCI) PED Security Program.

Under the original, Visa-only program, PEDs were approved for a three-year period, beginning from the day the successful lab evaluation was completed. At the end of this three-year period, devices were either removed from the Approved PIN Entry Devices list, located at [www.visa.com/pin](http://www.visa.com/pin), or reassessed for continued approval. Approximately 200 pre-PCI PEDs were lab-evaluated and Visa-approved under the Visa-only PED testing program.

To further align with the PCI PED Security Program and have all PEDs transitioned to one common method of expiration, pre-PCI PEDs will be removed from the Approved PIN Entry Devices list. These pre-PCI PEDs will expire between December 31, 2007, and September 30, 2008, with the majority being point-of-sale (POS) PEDs that will expire on December 31, 2007. Acquirers, processors, Encryption and Support Organizations and merchants should continue to actively review Visa's Approved PIN Entry Devices list, located at [www.visa.com/pin](http://www.visa.com/pin), to validate pre-PCI PED expiration dates for each pre-PCI PED currently in use.

## PCI-Approved PEDs Should Be Used Whenever Possible

Many of the more secure PCI-approved PEDs are backward compatible with the pre-PCI PEDs, and Visa recommends that PED purchasers make plans to transition and purchase only PCI-approved PEDs. Entities should work with their vendors to validate compatibility between pre-PCI and PCI-approved PEDs. In cases where the PCI PED is not backward compatible with an existing base of deployed pre-PCI PEDs, entities will need to ensure they plan now in order to purchase and take delivery of any pre-PCI POS PEDs prior to their being removed from the Approved PIN Entry Devices list. To ensure all entities understand and comply with these changes, Visa has developed a list of Frequently Asked Questions that addresses potential scenarios (see attached).

The current versions of the PCI PED and Encrypting PIN Pad (EPP) security requirements provide a higher level of PIN protection because they address emerging threats the pre-PCI PED security requirements did not cover. Pre-PCI PEDs will be removed from the Approved PIN Entry Devices list unless vendors resubmit their PEDs for laboratory testing under the more rigorous *PCI PED Security Requirements* or *PCI EPP Security Requirements*.

For acquirers to maintain compliance with the Visa PIN Security rules and retain liability protection when newly deploying these devices, they must purchase and take delivery of pre-PCI PEDs prior to their approval expiration, which for most pre-PCI POS PEDs is December 31, 2007. Acquirers and their sponsored entities may continue to deploy previously approved pre-PCI PEDs provided they purchase and take delivery of those devices prior to the approval expiration date. Pre-PCI POS PEDs purchased after the device's approval expiration date shall not retain liability protection when deployed.

Acquirers deploying devices that are not on the approved list at the time of purchase will be liable in the event of a PIN compromise attributable to the use of those devices, and they may also be fined in accordance with the *Visa U.S.A. Inc. Operating Regulations*, Section 1.8; *Interlink Network, Inc.*

---

Visa Business Review is published biweekly by Visa U.S.A. Inc., P.O. Box 8999, San Francisco, California 94128-8999, for the exclusive use of U.S. members in operating their Visa-sponsored programs. The information furnished herein is CONFIDENTIAL and shall not be duplicated, published or disclosed in whole or in part without the prior written permission of Visa.

# Reminder: PIN Entry Device Testing Program Changes

## Effective December 31, 2007 (Continued)

---

*Bylaws and Operating Regulations*, Section 1.5; and *Plus System, Inc. Bylaws and Operating Regulations*, Section 6.7. For PEDs purchased after the device's approval expiration date, where the security of the PED was not reassessed by the manufacturer and therefore not provided a new expiration/renewal date, there will not be any liability protection for the acquirer.

Currently, there is no mandatory removal or sunset date for any PEDs that were listed on the Approved PIN Entry Devices list at the time of purchase/deployment. All pre-PCI PEDs may continue to be used after their expiration date. The impact of the PED expiration is strictly associated with new equipment purchases and not existing PED deployments.

### Member Impact

There are approximately 130 PCI-approved PEDs available and listed on [www.visa.com/pin](http://www.visa.com/pin), and entities must purchase only these PCI-approved PEDs after December 31, 2007. Entities that transition now to purchase only PCI-approved PEDs can help ensure they will not be affected when pre-PCI PEDs are removed. Further, entities with PCI PEDs will be using the most secure PEDs available for the protection of PINs. Members are reminded that to be in compliance with the Visa PIN Security rules and retain liability protection when newly deploying PEDs, they must purchase and take delivery of pre-PCI PEDs prior to the device's approval expiration date.

For additional details and examples of PED approval lifecycle scenarios, acquirers and their sponsored entities should review the Payment Card Industry PIN Entry Device Testing and Approval Program Guide available at [www.visa.com/pin](http://www.visa.com/pin). Additionally, acquirers may view the Payment Card Industry PIN Entry Device Testing and Approval Member Implementation Guide available in the PIN Security section of Visa Online ([www.us.visaonline.com](http://www.us.visaonline.com)). To further help acquirers disseminate these important program changes to merchants, Visa published this information in the Fall 2007 edition of Visa Directions.

### Related Information

Additional information on the Triple Data Encryption Standard (TDES), *Payment Card Industry PIN Security Requirements* and PED security may be found in the following Visa publications and Visa Web sites.

- ▶ Recently Updated: *Visa PIN Security Tools and Best Practices for Merchants* brochure, available at [www.visa.com/pin](http://www.visa.com/pin)

[www.visa.com/pin](http://www.visa.com/pin) or from the Visa Fulfillment Center at (800) 235-3580 (reference document number VRM 08.05.07).

- ▶ *Payment Card Industry PIN Entry Device Testing and Approval Program Guide*, available at [www.visa.com/pin](http://www.visa.com/pin).
- ▶ *Payment Card Industry PIN Entry Device Testing and Approval Member Implementation Guide*, available at [www.us.visaonline.com](http://www.us.visaonline.com).
- ▶ *Payment Card Industry PIN Security Requirements* manual, *Payment Card Industry PIN Entry Device Security Requirements* manual and *Payment Card Industry Encrypting PIN PAD (EPP) Security Requirements* manual, available at [www.visa.com/pin](http://www.visa.com/pin) or the Risk Management section of Visa Online ([www.us.visaonline.com](http://www.us.visaonline.com)).
- ▶ "Visa Announces Changes to PIN Entry Device Testing Program," in the June 2007 *Visa Business Review*, Issue No. 070619
- ▶ "Visa Announces a New Category for Unattended PIN Entry Devices," in the June 2007 *Visa Business Review*, Issue No. 070619
- ▶ "PIN Pad Found Vulnerable to Skimming Attacks," in the March 2007 *Visa Business Review*, Issue No. 070327
- ▶ "Members Are Reminded That POS PIN Pads Susceptible to Skimming Attacks Must Be Replaced," in the February 2006 *Visa Business Review*, Issue No. 060214

### Attachment

Visa PIN Entry Device Frequently Asked Questions

### For More Information

Contact Stoddard Lambertson, Enterprise Risk and Compliance:

Phone: (650) 432-1470  
Fax: (650) 432-2946  
E-mail: [stoddard@visa.com](mailto:stoddard@visa.com)

Or contact your Visa Account Executive or call (888) 847-2242 for a Visa subject matter expert.

**Article Number: 07102306**

---

*Visa Business Review* is published biweekly by Visa U.S.A. Inc., P.O. Box 8999, San Francisco, California 94128-8999, for the exclusive use of U.S. members in operating their Visa-sponsored programs. The information furnished herein is CONFIDENTIAL and shall not be duplicated, published or disclosed in whole or in part without the prior written permission of Visa.

# Visa PIN Entry Device Frequently Asked Questions

---

## **1. What is the impact to an acquirer if it or its agent deploys point-of-sale (POS) PIN Entry Devices (PEDs) or Encrypting PIN Pads (EPPs) that have not been evaluated by a Visa-recognized laboratory and are not on the current Visa-approved list?**

Acquirers deploying POS PEDs or EPPs that have not passed evaluation by a Visa-recognized laboratory and that are not approved by Visa will continue to be liable in the event of a PIN compromise that is attributable to the deployment of those devices and, additionally, may be liable for penalties in accordance with the *Visa U.S.A. Inc. Operating Regulations*, Section 1.8; *Interlink Network, Inc. Bylaws and Operating Regulations*, Section 1.5; and *Plus System, Inc. Bylaws and Operating Regulations*, Section 6.7.

## **2. For liability protection, how can acquirers and their agents ensure that the POS PEDs and EPPs they purchase are compliant with the applicable PED security requirements?**

Acquirers and their agents should always look to [www.visa.com/pin](http://www.visa.com/pin) to validate that the device matches **ALL** of the following: Model Name, Hardware #, Firmware # and, if applicable, Application #. Acquirers and their agents should be aware when making purchasing decisions that some vendors may sell the same model in both approved and unapproved versions.

## **3. What is the impact to the acquirer of the “renewal” or “expiration” date for a device’s approval (e.g., the expiration date of December 31, 2007, for all pre-PCI approved POS devices)?**

The renewal/expiration date for Payment Card Industry (PCI)-approved devices is the date by which a vendor must have the device re-evaluated against the current security requirements in order to maintain the approval.

The renewal/expiration date for pre-PCI approved POS devices is fixed at December 31, 2007, and cannot be extended. Pre-PCI approved devices may be submitted for approval against the current PCI requirements to receive a new renewal/expiration date.

Acquirers purchasing devices that are on the approved list retain protection against liability from a PIN compromise associated with the deployment of those devices.

Acquirers deploying devices that are not on the approved list at the time of purchase will continue to be liable in the event a PIN compromise is attributable to use of those devices, and they may also be liable for penalties in accordance with the *Visa U.S.A. Inc. Operating Regulations*, Section 1.8; *Interlink Network, Inc. Bylaws and Operating Regulations*, Section 1.5; and *Plus System, Inc. Bylaws and Operating Regulations*, Section 6.7.

Security requirements are reassessed every three years based on identified threats. If necessary, the requirements are updated. Devices evaluated against earlier versions of security requirements will have their approvals expire on a specific date. This expiration date is also known as the “renewal date.” In order to continue to maintain approval for a new approval cycle, the device must be evaluated against the current version of security requirements.

For example, for devices expiring December 31, 2007, acquirers retain protection against liability from a PIN compromise associated with the deployment of those devices purchased on or before December 31, 2007. For devices purchased after that date, where the security of that device was not reassessed and thus was not given a new expiration/renewal date, there will not be any liability protection.

It is important to note that there is currently not a sunset date for devices that were on the approved list at the time of deployment. Deployed devices that have their approval expire on December 31, 2007, may continue to be used after that date. The impact of the expiration is strictly associated with new purchases/deployments, not existing deployments.

---

*Visa Business Review* is published biweekly by Visa U.S.A. Inc., P.O. Box 8999, San Francisco, California 94128-8999, for the exclusive use of U.S. members in operating their Visa-sponsored programs. The information furnished herein is CONFIDENTIAL and shall not be duplicated, published or disclosed in whole or in part without the prior written permission of Visa.

## Visa PIN Entry Device Frequently Asked Questions (Continued)

---

### **4. Pre-PCI approved POS devices have their approvals for new deployments expire December 31, 2007. Is there a sunset date when these devices must be removed from deployment?**

A sunset date for deployed devices that were approved at the time of deployment, but have had their approvals expire, does not currently exist. Due to the changing threat environment, PCI PED Security participants are evaluating the need to establish a sunset date for pre-PCI devices. However, that date, if established, will take into account the expected normal life cycle of devices subsequent to deployment, balanced against the emergence of threats.

### **5. EPPs and POS PEDs are approved for new deployments if they are on the approved list at the time of purchase. If a deployed device that was approved at the time of purchase requires replacement or repair, can that device be replaced with a newly purchased device of the same make/model and hardware/firmware versions when the device's approval has expired?**

One-to-one replacements of like-kind devices for repair and replacement are permitted, if the replacement is performed by the device's original purchaser or their agent, even though the approval has lapsed. This does not apply to devices that have had their approval revoked for reasons other than normal approval expiration (e.g., in the event of a widespread compromise of the device).

### **6. Pre-PCI POS PED approvals expire December 31, 2007. What is the latest date that an acquirer or its merchant agents can purchase a pre-PCI POS PED and still retain liability protection for the use of those devices?**

The expectation is that acquirers or their merchant agents must purchase and take delivery of pre-PCI POS PEDs prior to 2008. These devices can then be deployed as needed. Under certain conditions, delivery may be taken after December 31, 2007. This is allowed when all of the following conditions are met:

- 1) Full payment or invoicing has occurred prior to 2008
- 2) The devices purchased are manufactured inventory on hand prior to 2008
- 3) The devices are specifically identified and designated for that specific customer

The aforementioned applies when the acquirer or its merchant agent makes the purchase, whether it is from the original equipment manufacturer or a third-party reseller.

### **7. What is the relationship of the PCI PIN Security Requirements to PED testing?**

PCI-approved PEDs must be able to support the implementation of the PIN security requirements in a manner that is compliant with those requirements.

### **8. How do the PCI PIN Security Requirements relate to the PCI PED Security Requirements?**

Both the PCI PIN and PED Security Requirements have the common overall objective of protecting the cardholder's PIN during a financial transaction using a payment card.

The *PCI PIN Security Requirements* consist of 32 security requirements divided into seven logically related groups, which are referred to as Control Objectives. The PIN requirements are about process management – primarily dealing with the secure management of cryptographic keys throughout their life cycle (key creation, conveyance, loading, usage and administration) and with the use of secure PIN processing methodologies and the management and use of secure equipment for that processing. This results in a complete set of requirements for the secure management, processing and transmission of PIN data during online and offline payment card transaction processing at ATMs and attended and unattended POS terminals.

---

Visa Business Review is published biweekly by Visa U.S.A. Inc., P.O. Box 8999, San Francisco, California 94128-8999, for the exclusive use of U.S. members in operating their Visa-sponsored programs. The information furnished herein is CONFIDENTIAL and shall not be duplicated, published or disclosed in whole or in part without the prior written permission of Visa.

## Visa PIN Entry Device Frequently Asked Questions (Continued)

---

The *PCI PED Security Requirements* (both POS and EPP) are primarily concerned with device characteristics impacting the security of the PED used by the cardholder during a financial transaction. It also includes device management, but the testing process currently only addresses the device characteristics.

These requirements are divided into the following categories:

Device Characteristics:

- ▶ Physical Security Characteristics
- ▶ Logical Security Characteristics

Device Management:

- ▶ Device Management During Manufacturing
- ▶ Device Management Between Manufacturing and Initial Key Loading

Device characteristics are those attributes of the PED that define its physical and logical (functional) characteristics. The physical security characteristics of the device are those attributes that deter a physical attack on the device, for example, the penetration of the device to determine its key(s) or to plant a PIN-disclosing “bug” within it. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a cleartext PIN encryption key.

Device management considers how the PED is produced, controlled, transported, stored and used throughout its life cycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.

The *PCI PED Security Requirements* are only concerned with the device management for PEDs up to the point of initial key loading. Subsequent to receipt of the device at the initial key loading facility, the responsibility for the device falls to the acquirer and is covered by the operating rules of the card associations and the *PCI PIN Security Requirements*.