



This Article Originally Appeared in Issue 07:04:01 • April 9, 2007

## PIN pad security: Get a grip

By Bulent Ozayaz

VeriFone

**D**o you have Dec. 31, 2007, clearly marked on your calendar? How about July 1, 2010? If not, take out a red pen. The first date is the last day on which acquirers can purchase Visa-approved PIN entry devices (PEDs).

Second is the date by which PEDs deployed before Jan. 1, 2004 – when Visa U.S.A. established its PED standard – must be removed from service.

PED security is a major issue for merchants, even if they're not yet fully aware of it. The experience of Stop & Shop Supermarket Cos. should be a call to action for you and your customers.

In February 2007, the company reported it had discovered tampering at several of its stores. Spyware had been inserted into PEDs to capture card data and PINs.

The compromised systems appear to involve devices that pre-date the Visa PED security standard.

Tampering in this context generally means insertion of spyware into PEDs to capture credit or debit card account numbers, magnetic stripe data, and consumer PINs. You may have heard about criminals inserting such software into ATMs or gas pumps.

A commonly used tactic has been for criminals to purchase on the resale market PED models that are similar to those used by targeted merchants.

The deviants insert spyware into these PEDs and then replace merchants' devices with the tampered ones.

Thus, the altered PEDs can gather consumer information for malicious purposes. There are several ways criminals can collect this data, including the following:

- Retrieve tampered devices after they have collected enough sensitive information.
- Transmit information in real time over wireless connections to other computers.
- Transmit data through merchants' computer networks to remote computers.

Media reports in the wake of arrests made in the Stop & Shop breach indicate the culprits brought tampered replacement units into the stores, diverted the attention of store personnel as they swapped the units and came back later to collect cardholder information.

### Security requirements evolving

Prior to 2004, minimal standards governed the manufacture of PEDs. Protection of master keys, key encryption schemes and proper software operation of devices were usually the only requirements.

Validation of software standards and tamper prevention and detection were left to individual manufacturers. As of Jan. 1, 2004, Visa required PED testing by an independent laboratory to ensure that PEDs maintain a consistent level of physical and logical security.

Older devices are typically referred to as nonapproved. Due to the risk of compromise, retailers should replace them sooner rather than later.

For protection from liability from PIN compromise at the POS, Visa required acquiring members to deploy only POS PED models that had passed an evaluation by a Visa-recognized laboratory to determine the device's compliance to Visa's PED security requirements.

### Standards converging

In August 2004, Visa and MasterCard Worldwide (later joined by JCB International Credit Card Co. Ltd.) announced they would align their separate specifications under the Payment Card Industry PED Security Requirements banner: PCI PED.

For the time being, there is no sunset date for Visa-approved PEDs, meaning there is currently no requirement that retailers remove them from service. But as of the end of 2007, acquirers may no longer purchase them.

PCI PED is currently administered independently from the PCI Data Security Standard (PCI DSS). The two standards evolved separately and are targeted at different aspects of the identity theft and data compromise arenas.

PCI PED is specifically intended to enforce security of hardware devices that accept consumer PINs and house acquirers' secret encryption keys.

PCI DSS covers any system that houses or handles cardholder information. Card Associations supporting both standards have stated publicly the standards should be linked. But they have not provided formal guidance as to how or when this should occur.

What does this mean to you as ISOs and merchant level salespeople? Ensuring the security of your customers' payment systems is as challenging as it is critical to your business.

In addition to the PCI PED and PCI DSS, you must master a growing alphabet soup of standards, including PABP (Payment Application Best Practices), Visa's CISP (Cardholder Information Security Program), MasterCard's SDP (Site Data Protection), DISC (Discover Information Security and Compliance) and American Express Co.'s DSOP (Data Security Operating Policy).

These differing standards make it hard to determine not only what requirements apply in any given situation, but also how to comply with them.

### **Security tips**

---

It's likely your customers will expect you to guide them as they become more cognizant of PED security issues. Here are seven things merchants can do to help secure their systems:


1. Immediately perform a visual inspection on every terminal. If anything appears out of the ordinary, have the unit checked by an authorized repair facility.
2. Have the inspector verify that the serial number printed on the bottom of the terminal matches the internally stored serial number. Immediately remove from service any devices for which these numbers do not match.

3. Require all repair technicians to log in and verify their identity before they examine any equipment. Never allow them to work on PEDs unaccompanied.

4. Check PED installation. Devices should be mounted on the counter. Unplugging cables should require more than turning the unit over. Consider using locking stands.

5. Review the POS-to-PED interface to determine if it tracks or identifies the serial number of the attached PED. If not, consider implementing such a software security scheme.

6. Only purchase PEDs from manufacturers or manufacturers' authorized partners. Unauthorized resellers, such as may be found at online auction sites, could be selling compromised devices, whether intentionally or unwittingly.

7. Have PEDs repaired at their respective manufacturers or at manufacturer-authorized repair centers that have completed TG3 Key Injection audits. 

---

*In an effort to educate and inform, VeriFone has established a Web site focused on payment security information: [www.verifone.com/security](http://www.verifone.com/security). It provides a range of tools, from best practices documents, white papers and updated information about security standards to webinars and listings of upcoming payments industry conferences.*

*Bulent Ozayaz is VeriFone Vice President of Marketing for North America. He can be reached at [bulent\\_ozayaz@verifone.com](mailto:bulent_ozayaz@verifone.com).*