



This Article Originally Appeared in Issue 09:07:01 • July 13, 2009

## Pulling the PIN on older systems

By Scott Henry

VeriFone

The compliance clock is ticking. It is estimated that more than 500,000 PIN entry devices (PEDs) that predate security certifications are in use in the U.S. market. These devices predate the Visa Inc. PED standard – now the Payment Card Industry (PCI) PED Standard – and were "never approved" by the card brands, which have mandated they must be removed from service by July 2010. Are you ready for that challenge and opportunity?

### Liability landing

Criminals are increasingly targeting older, unsecure PIN pads and terminals as a relatively easy means to gain access to cardholder data. The liability for these attacks is being placed with greater frequency squarely at the feet of merchants and acquirers.

The 2009 Verizon Business Data Breach Investigations Report examined 98 confirmed data breaches that compromised almost 300 million consumer records. Of the organizations victimized, 81 percent were not PCI Data Security Standard compliant, according to Verizon Business.

### PINs beguiling

While many of these breaches had nothing to do with PIN pad compromises, obtaining PINs by exploiting vulnerable elements of computer networks is now the primary game in town for a number of criminal organizations.

Offending breaches range from highly sophisticated computer networking assaults to crude efforts that might be equated to "smash and grab" attacks in which criminals simply replace an existing terminal with a device that appears identical but has been bugged.

For example, according to *The News Journal* of Delaware, two men pled guilty in February 2009 to using a skimmer at the counter of a Rite Aid Corp. store to scoop up account numbers and PINs and use them to make counterfeit cards, with which they stole more than \$500,000 from bank accounts.

### Standards strengthening

The payments industry has long recognized the need to stay ahead of scofflaws by requiring ever more secure procedures

and devices to protect PINs, making it difficult to tamper with devices and ensuring merchants and acquirers are quickly alerted to tampering when it occurs.

In 2004, Visa mandated that new installations connecting to its payment network be certified as meeting a series of requirements it had set forth for PEDs – which became known as the Visa PED standard.

Later in 2004, Visa and MasterCard Worldwide agreed to align their separate PED requirements into an industrywide standard, which subsequently became known as the PCI PED standard.

In 2006, the PCI Security Standards Council (SSC) was formed by the major card brands to oversee security standards; in April 2007, Visa, MasterCard and JCB International Co. Ltd. formally transferred responsibility for PCI PED to the council, providing a more formal structure for future development of PED requirements.

### Confusion clearing

The evolution of PED standards has been a source of confusion to merchants, and to enhance understanding of these standards and their impact, it is helpful to categorize PEDs into three classes:

1. Devices that were never certified as conforming to the Visa PED. These are commonly referred to as "never approved" or "pre-Visa PED" and must be removed from service by July 1, 2010.
2. Devices that were certified to the Visa PED but not to the PCI PED. Among other things, this means they are capable of using Triple DES (often referred to as TDES or 3DES) encryption. As of Dec. 31, 2007, they could no longer be newly deployed.
3. Devices that meet the newer PCI PED requirements. These are the only systems approved for deployment as of Jan. 1, 2008.

Prior to 2004, PEDs were governed by minimal standards. Generally, the only things required were protection of the master keys and key encryption schemes, as well as proper software operation of the devices. Validation of software requirements and tamper prevention and detection were left to individual manufacturers.

As stated in the preceding numbered points, the card brands

mandated that, as of Dec. 31, 2007, acquirers and merchants deploy PCI PED-approved devices only.

And they set July 1, 2010, as the date by which unapproved devices must be removed from service. No such sunset date has been set for pre-PCI devices, although they can no longer be installed except as replacements for PIN pads that are already in place.

### **Sanctions coming**

---

Although Visa has indicated it won't strictly enforce penalties against noncompliant organizations until 2012, acquirers have the ability to penalize merchants once the July 1, 2010, cutoff arrives.

There are several reasons to take this seriously and not postpone helping merchants replace devices that are now or soon will be obsolete:

- In 2007, Visa mandated that acquirers submit plans to identify security risks for smaller merchants (whom it classifies as Level 4) and to apply "targeted compliance measures to merchant subgroups."
- While Visa may not proactively level fines before 2012,

acquirers will still be liable for any breaches where non-compliant devices are used after July 1, 2010. They in turn may fine ISOs that are supporting noncompliant merchants. Those ISOs may levy some or all of that cost on merchants.

- Acquirers may implement more aggressive compliance schedules than those mandated by Visa and the PCI SSC.
- Acquirers bringing new merchants on board must ensure they are compliant now.

### **Opportunities rising**

---

Many merchants are unaware of or confused about target dates for implementation of PCI PED-approved devices. Many may be tempted to put off PIN pad upgrades to some future time.

Educating them on the facts behind the compliance effort and the perils of delay presents a great opportunity to up-sell with new technologies such as Internet protocol and wireless, as well as value-added applications to which newer systems are better suited. ☞

---

*Scott Henry is Director, North America Product Marketing, for VeriFone. He can be contacted at [scott\\_henry@verifone.com](mailto:scott_henry@verifone.com).*