

# Taking a stand on payment security

**Payment acceptance systems need to meet continually evolving standards and achieve rigorous certifications in order to help ensure a secure card transaction environment. But ever-stricter standards also create an opportunity to provide greater value, increased reliability and better performance.**

Creating payment systems for use in consumer environments requires building a protected world in which cardholders, merchants and banks can perform transactions reliably, securely, and with peace of mind. This mutual network of trust requires everyone in the payment chain to follow good practices: cardholders must take care of their cards and PINs, retailers must monitor staff and effectively manage their systems, and finally, anyone storing sensitive customer data electronically must properly safeguard that data.

Electronic payment acceptance systems must comply with a raft of national and international standards and safety requirements (for example, the CE mark), which can relate to various aspects of the hardware – including modems, wireless facilities and power supplies. Unique to the payments world, however, is the need for security. From a hardware perspective, it is these physical and logical security requirements that are now being mandated more stringently than ever.

Payment processing requires higher standards of security than many other business transactions. The consequences of security failure can be costly and may include a forensic incident investigation of any breach, a card association fine, government sanctions and, most damaging, the loss of consumer confidence and an injured business reputation.

## Evaluating the security

End-to-end security across the payments chain is only as strong as its weakest link. In this context PIN pad security is no longer an abstract concern, as recent headlines about payment security breaches and PIN pad tampering demonstrate.

The Payment Card Industry PIN Entry Device (PCI PED) security requirements are the latest set of security standards for online and offline PIN entry devices, including magnetic stripe and smart card PIN pads as well as terminals with built-in PIN pads.

The tampering incidents have involved older, less secure devices, known as pre-PED. Criminals have either substituted a device containing an electronic 'bug', or have directly inserted these bugs on systems in place to capture customer card data and PINs. PCI PED is an updated requirement for

PED suppliers that is designed to prevent or detect this type of tampering and to provide tighter security for sensitive consumer and card information. The newer PCI PED requirements includes a standardised testing process that combines one set of standards for each of the organisations that developed PED requirements – Visa, MasterCard and Discover Financial Services, American Express, and JCB. In conjunction with PCI security requirements, which are now under the auspices of the PCI Security Standards Council, PED manufacturers also need to adhere to regional and country-specific security requirements.

## Path to a global standard

Prior to 2004, minimal standards governed the manufacture of PIN entry devices. Protection of master keys, key encryption schemes and the proper software operation of devices were usually the chief requirements, while individual suppliers were free to validate software standards and tamper prevention and detection.

The introduction of EMV and increasing numbers of PIN-based cards led to a growing recognition that PIN pads in retail outlets could potentially become the 'weakest link' in the payments chain. In January 2004, Visa required PED testing by an independent laboratory to ensure PEDs maintain a consistent level of physical and logical security. Visa required its acquiring members to deploy only POS PED models that had passed a Visa-sanctioned evaluation that determined a device's compliance with Visa's PED security requirements. These devices are generally categorized as Visa PED-approved.

In 2004, Visa and MasterCard Worldwide and JCB aligned their separate specifications under the Payment Card Industry PED Security Requirements banner – PCI PED. The PCI PED security requirements cover all aspects of PED development, including its physical and logical characteristics, as well as how the PED is produced, controlled, transported, stored and used throughout its life cycle. It requires better protection of sensitive data storage and use, improved defences against keypad tapping, and stricter defences against display tampering, alongside stricter key management.

The requirements cover a variety of areas, including tamper protection, cryptographic control of prompting, PIN monitoring prevention, deterrents to prevent the visual observation of PIN entry, authentication of software applications, smart card reader security, as well as encryption and key management requirements. Under the latest PCI PED 2.0 certification standards, privacy shield requirements have been defined to ensure cashiers, customers or people standing nearby cannot easily observe the PIN during entry by the cardholder, deterring attempts to discover PINs by 'shoulder-surfing'.

Each device, including those used in unattended environments, must be equipped with proper shielding protection. In addition, a tamper resistant security module (TRSM) automatically deletes encryption keys and instantly puts the device out of service when a tampering effort is detected.

The new security standards are designed to secure PIN-based transactions globally, and apply to all devices that accept PIN entry. For PED manufacturers, security testing will now depend on a single set of requirements, helping to ensure cardholder security and providing opportunities for faster development and deployment.

Under the PCI PED certification process, manufacturers must deliver a fully functional device with test software to the relevant security auditors, including detailed design documents. Testing in the laboratory can take several months, depending on the complexity of the system. In addition to the PCI PED certification process, manufacturers can simultaneously undertake country or region specific standards testing for their devices.

After the testing, during which every attempt will be made to compromise and breach the payment device, the laboratory report goes to the relevant PCI Card Associations for approval and confirmation of the certification award.

## Achieving compliance

The PCI Security Standards Council has issued a mandate relating to the phased PCI PED implementation programme. Under this guidance, all devices previously approved and designated as compliant with existing PCI PED requirements will automatically be accepted into the new programme until their current approvals expire. From 1 January 2008, manufacturers have been required to ensure that any newly introduced device is PCI PED certified.

As of 1 January 2008, Visa PED-approved PIN entry devices can no longer be sold, although retailers may still deploy any device purchased before this date. At the present time, no 'sunset' date for the withdrawal of these devices from service has been defined.

Acquirers are mandated to ensure that currently installed, non-approved PEDs (those that don't

meet either Visa PED or PCI PED requirements) must be removed from service by June 2010. Failure to comply with this mandate means liability protection will be removed. As a consequence, in the event of a PIN compromise, card reissue costs are likely to be passed to the retailer and penalties will be imposed by the card association, which may also revoke a merchant's service agreement.

## The PCI PIN Security

In addition to security requirements relating to the payment terminal itself, the PIN Security Program, which is designed to protect cardholder PINs during message processing, requires compliant equipment for PIN entry, specified cryptography to protect PIN during transmission, and documentation and methods that ensure key secrecy.

The program also specifies acceptable cryptography and mandates for Triple DES (Data Encryption Standard) usage. To underpin device security, from 1 January 2004 all newly deployed POS PIN entry devices were required to support Triple DES (single DES has been fully retired by ISO and ANSI). As of 31 December 2007, all VisaNET/Interlink endpoint Issuer Working Keys (IWKs) and Acquirer Working Keys (AWKs) must use Triple DES, and by 1 July 2010, all transactions must be encrypted in Triple DES from point-of-origin to the issuer. Note: PINs can never be stored.

## PCI DSS

There are several ways that criminals can collect customer data for later fraudulent use. Fraudsters may retrieve a tampered device once it has collected enough data, or interfere with the transmission of information in real-time over a wireless connection. Finally data can be transmitted through the merchant's own computer networks to remote computers. Because of this, new PCI standards have evolved in response to the threat posed to both the terminal and the retailer's entire system.

The PCI Data Security Standard (PCI DSS) was introduced in 2005 and supersedes the various standards used by card schemes for the secure storage of accounts and transaction data. It applies to all processors and merchants, and effectively codifies best practice while instituting a mechanism for evaluating, testing and monitoring compliance. Administered by the PCI Security Standards Council, PCI DSS establishes a single standard of due care for data security across the payment card industry.

## Payment apps: PABP

Ensuring confidence in the payment application software that runs on and interacts with

the payment system is equally critical to maintaining a secure acceptance environment.

Payment Application Best Practices (PABP) are a set of requirements devised by Visa that apply to software vendors who develop point-of-sale payment applications that store, process, or transmit cardholder data as a part of payment card authorisation or settlement. The requirements for PABP are based upon PCI DSS and the PCI DSS Security Audit Procedures.

Within the PABP framework, all payment applications must be certified by an independent, Visa-approved auditor in order to achieve PABP validation, which ensures that payment applications do not retain full magnetic stripe or CVV2 data (both prohibited under PCI DSS). Ensuring that all payment software is PABP-certified is a key step to achieving full PCI DSS compliance for retailers.

Since the software infrastructure within a retailer organisation handles all of the retailers' business – not just payment – there needs to be a clear understanding and appreciation of related procedures by all parties involved, including how any security solutions need to work within whole networks. By working closely with technology experts, retailers should be able to define a seamless PCI DSS compliance strategy that delivers the required security without compromising the business functions of its non-payment software and systems architecture.

## Navigating standards

Alongside PCI PED, PCI DSS and PABP, there's a growing alphabet soup of standards to negotiate, including Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection (SDP), Discover Information Security and Compliance (DISC) and American Express' Data Security Operating Policy (DSOP).

In the future, security requirements can only become more multi-layered and rigorous. The introduction of additional layers of security and authentication at the point-of-payment – such as biometric methods – will not eradicate the need to implement robust standards and adopt comprehensive security best practices at the point of sale.

For merchants, keeping up with the very latest developments in security mandates and ensuring the ongoing compliance of their payment systems can seem a complex and daunting task. Retailers will increasingly look to experts to help simplify compliance, and advise how best to meet those requirements while incurring minimal cost and effort. In this way, payment solution providers have a key role to play in delivering transparent security to merchants and customers, so that retailers can stay focused on their core competence.

With certifications now starting to stabilise, now is the time for banks and retailers to develop a compliance upgrade plan with trusted suppliers

## PIN pad best practices

Seven actions can help merchants improve the security of their systems:

1. Immediately perform a visual inspection on every terminal. If anything appears out of the ordinary, have the unit checked by an authorised repair facility.
2. Have an inspector verify that the serial number printed on the bottom of the terminal matches the internally stored serial number.
3. Ensure all repair technicians log in and verify their identity before they examine any equipment.
4. Check PED installation. Devices should be mounted on the counter. Unplugging cables should require more than turning the unit over. Consider locking stands.
5. Review the POS-to-PED interface to determine if it tracks or identifies the serial number of the attached PED.
6. Only purchase PEDs from manufacturers or manufacturers' authorised partners. Unauthorised resellers, such as may be found on online auction sites, could be selling compromised devices.
7. Have PEDs repaired at their respective manufacturer-authorised repair centres that have completed a TG3 Key Injection audit.

Ideally, retailers need to identify the steps they need to take in the event of an incident. These include ensuring they understand how to isolate their payments system to prevent future sensitive information loss. Designating one individual to lead this effort is also advised.

to avoid the fines, losses and damage to reputation that could result from any security breach. Payment solution providers who have a proactive security strategy – well in advance of compliance deadlines – can deliver PCI PED-approved systems that offer greater value and lower cost of ownership, increased reliability and better performance. Ensuring a secure, compliant card transaction environment doesn't need to stand in the way of innovation and new ideas, but can actually be a powerful platform for delivering an enhanced payment experience for cardholders and promoting greater overall consumer confidence.

This feature was provided by Dave Faoro, chief security officer, VeriFone. He can be contacted at Tel: +1 916 630 0550, email: [dave\\_faoro@verifone.com](mailto:dave_faoro@verifone.com), Web: [www.verifone.com](http://www.verifone.com)