ergonomic solutions

How to secure devices, data & networks

PCI DSS 3.0 compliance and what this means to you

An Ergonomic Solutions white paper
Foreword by Chris Field of Fieldworks Connections

TECHNOLOGY MOUNTING SOLUTIONS

Why in-store payment security isn’t just about locks and keys

Despite the advent of both regulation and best practice across Europe to improve the way that payments are secured, there is still a great deal of uncertainty, from territory to territory, as to how merchants should best respond.

For some, uncertainty has been exploited by vendors who use fear to force merchants to adopt measures that are at times excessive, leading to unnecessary investment, poor ergonomics at the point of sale and difficulties for consumers using payment devices.

Sometimes, the measures taken are misdirected – for instance, while they may appear to meet the requirements of the PCI Council’s guidelines, they may not work in all circumstances in a live environment.

What remains is the simple fact that, while most aspects of the PCI standards have been taken care of by the terminal vendors, the last line of defence towards potential criminals remains with the retailer. And these criminals are becoming smarter and more determined by the day: On any given day, there are over 5,000 terminals available for auction online, and legitimate terminals in stores are permanently under threat.

As a result, retailers are inundated by companies in the payment device-security business, due in part to the requirements set on them by PCI, but also as the issue of data security continues to hit the headlines and raise consumers’ concerns.

These are real concerns, evidenced by the impact that lax data security processes can have on retailers of any size, however, pressure on retailers to respond comes exactly at a time when they are having to look harder than ever at every single investment. Already trading in a tough environment, retailers are having to focus harder on the customer experience, driving new investments into mobile devices that connect to the network wirelessly and yet which must still conform to PCI DSS 3.0 requirements for data protection.

We decided to work with the market leader, SpacePole, on the request of our retailer members to bring some sanity to the problem, by publishing a guide to payment data security that embraces not only the physical securing of terminals and other payment devices, but also the implications of PCI compliance on device security, management, registration and maintenance, as well as the payments environment.

It is our mission to take a cooler look at the problem and help merchants understand their options so that they can make decisions based on their own particular requirements.

By using this guide, merchants will find it easier to comply fully with PCI DSS 3.0 recommendations on:

» physical security of payment terminals
» the payments environment
» skimming prevention
» risk assessments

This approach is endorsed by the leading organisations in payments, from VeriFone to Visa, and follows the guidelines and requirements published by the PCI Council.

Chris Field
Fieldworks Connections

The threats

Some in the payments industry have used the fear factor to drive merchants down a narrow path of at times excessive, at times incorrect and at other times, unnecessary security of in-store fixed and mobile point of sale devices and other add ons.

Significant investments are made in the payment terminals, so the last conversation that many merchants want to have is about how they have to spend even more money on securing the devices. The honest approach is to help them understand the risks and build their own risk profile that can then be matched to any subsequent investments. This contrasts starkly with the fear-peddlers who are only interested in moving equipment.

There is therefore, a balance to be struck between inaction and overreaction.

*PCI DSS 3.0, 9.9 state that a merchant must protect the point-of-sale devices that capture payment card data via direct physical interaction with the card from tampering and substitution. **This will become a requirement for merchants after June 30 2015.***

For mobile devices the guidance say that where a merchant either owns or is otherwise responsible for a mobile device being used as part of a payment solution, it is the merchant‘s responsibility to take steps to establish and maintain the security of that device. The measures described in this section should also be applied to any additional hardware components that form part of the mobile payment-acceptance solution (e.g., card readers).

5.1. Prevent unauthorized physical device access
5.1.1. The merchant is responsible for ensuring the integrity and security of the mobile device and its secure storage when not in use (e.g., locked in a cabinet, tethered to a counter or under 24-hour surveillance).

The threats are real and the requirement to mitigate them under the Payment Council Industry Data Security Standards (PCI: DSS) are critical if retailers want to avoid fines and a loss of customer confidence if data is stolen.

Any security breach of payment card data has far-reaching consequences for affected organisations including;

- Regulatory notification requirements,
- Loss of reputation
- Loss of customers
- Potential financial liabilities
- Litigation

However, many vendors of physical security devices simply ignore PCI and focus only on the device.

The result is:

- Misdirected investment
- Long-term ROI missing
- Non-compliance with PCI
- Chosen device becomes obsolete long before ROI
- Chosen device acts as deterrent to fraudsters but also puts off customers

Fear can tend to override retailers' natural instincts to ensure that all technology and equipment investments are backed by a solid ROI and TCO model. This is wrong; retailers not only want to understand the hard financial ROI, but also the so-called softer but nevertheless critical benefits in terms of customer experience, which equates to their willingness to buy.

The balance to strike is between security, accessibility and design. The solution needs to consider where you will be tomorrow not just fixing a problem and then having to write off the investment.

It's not just about the device

Because PCI is about the protection of data, it is important to secure not just the device but all the cabling that connects it to the network, the network on which it sits and the whole environment in which the network and devices sit. To treat the equipment independently of the network is to run the risk of multiple solutions that are incompatible, areas that may get overlooked, possible duplication of effort and a return on investment model that may be difficult to validate.

Focusing on the device alone can result in significant costs:

- If the device is not fixed it gets dropped as it is handed between staff and customers
- The cabling gets worn in the process which can result in the device switching to tamper, mode, rendering it unusable

- Securing the device alone does not necessarily deter fraud on other parts of the network, such as through the cables

We must therefore consider two main areas:

- Securing the device, both fixed and mobile
- Securing the environment

Requirements PCI DSS 3.0 June 30, 2015

Secure the terminal or mobile device

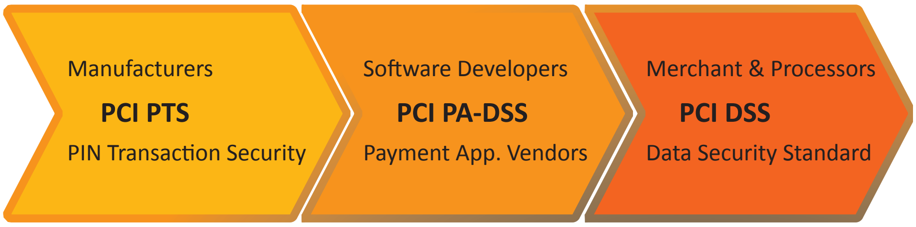
According to Visa, retailers should track and monitor details of all payment acceptance devices that accept its cards. As part of this, retailers should regularly examine devices to identify anything abnormal, such as missing or altered seals or screws, extraneous wiring, holes in the device or the addition of labels or other material that could be used to mask damage from device tampering. Retailers should at a minimum check the following:

- Is the terminal in its designated location?
- Is the manufacturer's name correct?
- Is the model number correct?
- Is the serial number printed on the label and displayed on the screen correct?
- Is the colour and general condition of the terminal as described, with no additional marks or scratches (especially around the seams)?
- Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
- Are the manufacturer's security markings and reference numbers as described?
- Are any expected ultra-violet markings present and as described?
- Are all connections to the terminal as described, using the same type and colour of cables and with no loose wires or broken connectors?
- Is the number of connections entering the terminal as expected?
- Is the total number of terminals in use the same as the number of terminals officially installed?

Securing the terminal is about:

- Preventing theft or replacement with an unauthorised terminal
- Preventing data capture from the payment infrastructure
- The addition of skimming equipment to the terminal or network

- Securing PIN data that is vulnerable to shoulder surfing
- Securing unattended terminals and preventing physical removal
- Securing not only the terminal but the cables as well



Manufacturers
PCI PTS
PIN Transaction Security

Software Developers
PCI PA-DSS
Payment App. Vendors

Merchant & Processors
PCI DSS
Data Security Standard

The above diagram describes the ecosystem of payment devices, applications, infrastructure and users structure and users structured by the PCI Security Standards

We believe that it is best practice to strike a balance between securing the asset and damaging usability and therefore, customer service. A device can be secured in such a way that it is almost impossible to snatch but this will not necessarily deter a bogus engineer or collusive member of staff. In PCI's document Skimming Prevention: Best practices for Merchants, it says that retailers are strongly recommended to use security tethers with key management services, as well as device registration and tracking to prevent both terminal and cables from being compromised as best practice.

However, the physical location of the device and security of components should also be considered. Can it be removed easily; are components hard wired together or physically protected to prevent easy tampering or theft? Devices should always be placed in a location that allows the customer to use them in a manner that obscures their PIN entry from other customers and where practical should include PIN shielding.

Usability is not just about convenience but about compliance with European disability and accessibility regulation. Where the needs of regulation can be met with the device in a mounting bracket, consideration should be given to modifying the bracket from a 'support only' mechanism to one that physically restrains the device reducing the potential for a 'smash and grab' type theft. Where locking the device into the mounting bracket would contravene disability and accessibility regulation, consideration should be given to connecting a security tether to the device and the mounting bracket so giving a degree of movement but maintaining security against a snatch theft.

The increasing use of customer facing technology in the retail environment through devices such as Chip & PIN terminals, iPads, and a host of other portable devices may have brought about a new shopping experience for many, but this has been at the cost of increased theft and fraud. The store in general and the point of sale in particular are at risk from increasingly sophisticated forms of criminality. Card data and PIN information are most at risk. Records show that it only takes about 30 seconds to remove an entire card device and replace it with an identical one fitted with electronic skimmers.

Criminals have developed a comprehensive understanding of the functionality and vulnerabilities of many of the terminals. Having successfully defeated security features of a particular terminal, it becomes easier to use this information to attack similar terminals, making POS security all the more relevant.

The iPad and other tablet devices have transformed the manner in which we use mobile technology and have led to a reassessment of the traditional approach to commercial technology integration, and especially within the retail sector. But these devices are of high value and highly sought after.

To protect digital information, prevent data loss and further secure hardware, Ergonomic Solutions has a range of security lock for payment terminals, mobile devices and POS hardware.

Secure the environment

This is about securing the device as an IP connected device. With data being encrypted point to point, along the entire network, all points of vulnerability must be investigated, secured and processes and procedures put in place for their monitoring.

- Device registration and tracking
- Compliance though processes and procedures
- Best practice documentation
- Risk assessment
- Impact analysis and response procedures

Device registration and tracking

Securing devices is one thing, but it is perfectly possible that the secure device has been compromised and there are no procedures in place to spot this. With skimming on the rise, which sees fraudsters tampering with devices in an attempt to steal card data through both the device and the network, it is critical to register all devices, which in turn meets the PCI Council's recommendations.

Registration should record the following key characteristics:

- Device serial and model number
- Manufacturer
- Existing distinguishing marks (based on wear and tear)
- Image of device
- Connection type
- Colour of lead
- Number of connections
- Display stands, charity boxes or other merchandising material in the vicinity of the terminal
- Location of security seals (manufacture seals or additional seals)
- Location at site e.g. checkout number 1

Terminals that have been tampered can then be identified because their original unique characteristics have been recorded. If the terminal present differs in any way, it may be fraudulent.

This is also safer for the user as they are provided with their own unique account and smarter for an organisation that wants to ensure its assets are recorded and available following personnel change.

Registration also enables administrators to manage their lock programmes through a single web portal, and manage access and keys to suit the individual environment. Assigning keys to a person, a checkout, a region as appropriate.

Administrators can

- Register locks individually or en-mass to individuals or groups (stores/areas etc.)
- Manage master keyed, like keyed or shared keyed programmes
- Create user accounts for their end users where replacement keys can be ordered or combination codes saved
- Prompt users to access tutorial videos and validate account details
- Record lock ownership and download reports
- Find the owners of lost keys
- Reassign locks to new users

Individuals can:

- Order replacement keys
- Retrieve stored combination codes (for the future maybe?)
- Validate account and keycode details
- Update their personal details

We are also recommending a unique device marking system for additional tamper-proofing, such as a UV Hologram seal that is only visible in UV light and if tampered with is impossible to replace or fix again. A seal is not only tamperproof but also signals to staff that the payment terminal is a POS device that need to be treated with special care and processes in order to meet the security standards.

Alignment

The approach recommended in this report is validated against the PCI DSS 3.0 Council document: Point-to-Point Encryption. Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices,
PCI Mobile Payment Acceptance, Security Guidelines, Version 1.1.1.

3A-1.1 Maintain inventory-control and monitoring procedures to identify and locate all POI devices, including where devices are:

- Deployed
- Awaiting deployment
- Undergoing repair or otherwise not in use
- In transit

Solution: Register & Retrieve database and checklists

3A-1.2 Perform POI device inventories at least annually to detect removal or substitution of devices.

Solution: Register & Retrieve checklist

3A-1.3 Maintain a documented inventory of all POI devices to include at least the following:

- Make, model of device
- Location (site/facility, and/or identity of merchant)
- Serial number
- General description
- Photograph of device that clearly shows device type and model (to assist with identification of different devices)
- Security seals, labels, hidden markings, etc.
- Number and type of physical connections to device
- Date of last inventory performed
- Firmware version
- Hardware version
- Applications (including versions)

Solution: Register & Retrieve database

3A-1.4 Implement procedures for detecting and responding to variances in the annual inventory, including missing or substituted POI devices. Response procedures must include inclusion of any procedures defined by all applicable PCI payment brands, including timeframes for incident reporting, and providing a point of contact for merchants to report missing/substituted devices.

Solution: Register & Retrieve database

3A-4.1 Provide instructions via the P2PE Instruction Manual for the merchant to select appropriate locations for deployed devices, for example:

- Control public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader).
- Locate devices so they can be observed and/or monitored by authorized personnel (for example, during daily device checks performed by store/security staff).
- Locate devices in an environment that deters compromise attempts (for example, through use of appropriate lighting, access paths, visible security measures, etc.)

Solution: Register & Retrieve checklist

3A-4.2 Provide instructions via the P2PE Instruction Manual for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured.

Solution: Register & Retrieve
Security tethers

3B-8 Solution provider implements tamper-detection mechanisms for devices in their possession, and provides related instructions to merchants.

Solution: StealthSafe

3B-8.1.1 Provide instructions via the P2PE Instruction Manual for the merchant to perform periodic physical inspections of devices to detect tampering or modification of devices. Detailed procedures for performing periodic physical inspections to include:

- Description of tamper-detection mechanisms
- Guidance for physical inspections, including photographs or drawings of the device illustrating what the merchant is to inspect, for example:
    - 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 tamperings.

    - Instructions for weighing POI devices on receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices
- Recommendations for frequency of inspections

Solution: Register & Retrieve database and checklists
Security tethers

3B-8.2 Implement tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations—for example, use cameras or other physical mechanisms to alert personnel to physical breach.

Solution: Security tethers

About Ergonomic Solutions

Founded in 1996, Ergonomic Solutions has grown rapidly to become a global leader in the design, manufacture and supply of the most ergonomically advanced mounting and security solutions for a wide range of in-store, and mobile technology for markets including retail, banking, mass transit, and hospitality. Ergonomic Solutions has long been at the forefront of workspace planning and optimisation and our influential Ergonomics Consultancy has advised many of the major European retailers how to create a workspace which optimises accessibility, usability, safety and comfort for their staff and customers.

Our suite of technology mounting solutions is designed to provide an ergonomic solution across a huge range of applications. From the shop floor to the management suite, we can deliver a solution that ensures that your IT investment makes the best use of the available workspace whilst simultaneously being protected from damage and theft.

About Fieldworks Connections

Fieldworks Connections brings together retailers, brands and influencers to shape the future of multi channel trading.

Today, we are part of a community that embraces both traditional and new channels, in Europe, Asia and the US. Our influence enables us to support companies looking for growth in their chosen markets and to reduce risk by applying best practice.

Fieldworks Connections is headed by a team of experienced journalists, marketers, analysts and consultants, supported by a board of senior retailers, consultants and academics.

www.fieldworksconnections.co.uk