PCI DSS v3.0 compliance: A closer look at Requirement 9.9 - Payment Terminal Protection

PCI DSS v3.0: A closer look at Requirement 9.9 - Payment Terminal Protection

Jason McWhirr CISSP,
Information Security Consultant, Sysnet Global Solutions

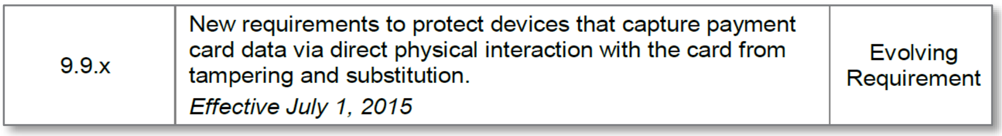
The reason for PCI DSS v3.0 Requirement 9.9

While EMV chip technology (chip & pin) and other technical measures have been effective at reducing card fraud in many countries across the world, criminals are increasingly resorting to physical attacks in order to steal cardholder data at the point of sale, or to devise new methods for data compromise.

To address this risk, in 2009 the Payment Card Industry Security Standards Council (PCI SSC) issued their skimming prevention information supplements to help merchants protect themselves against cardholder data exposure caused by the use of skimming (tampering) and substitution techniques. However this was always best practice advice and was not enforced in the Payment Card Industry Data Security Standard (PCI DSS).

However, the most recent PCI DSS, version 3.0, requirement 9.9 will now turn these best practices into enforceable requirements starting July 1st 2015. This is to ensure that merchants have controls and countermeasures in place to minimise their vulnerability to future attacks of this type.

Does the new requirement affect you?



9.9.x	New requirements to protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *Effective July 1, 2015*	Evolving Requirement

Any merchant accepting face-to-face payments via a physical point of interaction (POI) device or terminal will need to adhere to the new PCI DSS regulations.

These requirements state that all merchants must have controls in place to protect against direct physical tampering and substitution of their card-reading devices used in card-present transactions at the point of sale. That is any card swipe (or dip) POI device or terminal used in face-to-face transactions (including any unattended payment terminals accepting transactions where the customer's card is present).

In summary, the protection requirements are:

- Maintain an up-to-date inventory of your terminals/devices
- Periodically inspect terminals/devices to look for tampering or substitution
- Train personnel to be aware of suspicious behaviour and to report tampering or substitution of devices/terminals

What do you need to do to comply?

Inventory - Know what you have, and who is responsible

You can only protect what you know you have, so maintaining an inventory is critical.

This should, at the least, include;

- a list of all payment terminals
- terminal make and model
- any unique identifiers (e.g. serial number, barcode, security tape)
- terminal location

There is no wrong way to store this inventory; a spreadsheet or internal database recording the required information is adequate.

Location information should cover the terminals throughout their life whether in use or not. For example, recording which store/till each terminal is used at, whether a terminal is in a storage as a backup terminal, when a terminal has been removed from use due to a fault, when a terminal has been sent out of the business, where it was sent to and why.

The inventory must be kept up to date, so it is necessary to conduct regular checks to validate the accuracy of the details on record. Maintenance of the inventory can become un-wieldy for larger organisations and other solutions may need investigation.

The inventory must be supported by documented policies and procedures allocating responsibility for;

- compliance
- management of the inventory
- management of changes; such as replacements and new devices
- reporting in the event of an incident relating to the devices
- setting out the consequences for any non-compliance

Risk - Know how exposed your payment devices are

Understanding the risk factors associated with your POI terminals is integral in setting the right inspection frequency. While periodic inspections verify the integrity of your terminal estate, they are costly. Periodic could mean daily, weekly, monthly, or longer depending on what you perceive the risk exposure to be. Some companies integrate periodic inspections with their pre-established business processes, for example; at each shift change, or as part of store pre-opening checks. The frequency will depend on your company and the risks involved.

Factors such as the type of device, location, attended or unattended, etc., will affect risk exposure. For example, the risk exposure is far greater for un-attended car park or cinema kiosks than for terminals in a secured area with supervised public access.

All terminal locations should be risk assessed at least on an annual basis and when there is a major change to the point of sale environment/terminal to identify potential vulnerabilities, risk exposure of the terminals, appropriate protection measures, and the frequency for inspections.

Countermeasures can be used to lower your risk exposure. These may include positioning at the point of sale for the terminal and its cables, tethers, and physical locks, use of CCTV at the point of sale (not viewing the terminal PIN pad).

For more information refer to the PCI-SSC - Skimming Prevention: Best Practices for Merchants document listed in the 'More Information' section.

Total global payment card fraud losses were $11.3 billion in 2012, up nearly 15% from the prior year. The United States, the only country in which counterfeit card fraud is consistently growing accounted for 47% of that amount. Card issuers lost $3.4 billion and merchants another $1.9 billion. **Nilson Report**

Fraud losses on UK cards totalled £450.4M in 2013, a 16% increase from £388.3M in 2012. This is the second year of increase; however levels are still down 26% since fraud was at its peak in 2008. **FFA UK**

Train - Know what to look for and who to report to

Ensure that terminal inspection checks are performed correctly by creating procedures to define;

- when checks are to be performed
- what must be checked
- whose responsibility it is to inspect
- what inspection records and inspection history must be maintained
- how to report actual or suspected incidents

Then, once these procedures are defined, train the staff responsible for performing these checks. Establish procedures for terminal installation, fault reporting, return, and replacement so that deviations will be noted and reported as incidents. Personnel must be aware of attempts to tamper or replace terminals, and required to report suspicious behaviour and indications of attempted or actual compromise.

Incident responders also need to be trained and have documented procedures to follow so they know what to do in the event tampering or substitution is identified and they need to investigate.

Security awareness training should encompass all aspects of terminal protection.

Ensure that personnel at point of sale locations are aware of the procedures to verify the identity and authorisation of personnel seeking access to point of sale locations and terminals.

Evidence of this training, with employee sign-off, must be maintained to prove that training has been provided. Updated training information should also be performed at regular intervals, defined in your policy documentation.

Inspect - Checking the terminals

Procedure checks could include;

- Checking serial numbers & terminal identifiers against the inventory
- Checking the small screws on the base of a terminal are tight and secure
- Checking tamperproof serialised security tape is in-place and undamaged
- Checking the edges of a terminal have not been prised apart to insert a device inside.
- Checking that there are no unusually large gaps, scuffs or scratch marks that might suggest the terminal has been opened by force
- Checking that no cables have been changed or extra cables added to the terminal
- Taking photographs of the terminal and referencing current photos against known good images
- Weighing the terminals; if someone has attached an additional device or card skimmer onto the device it will change the weight of the terminal

This isn’t an exhaustive list of checks that could be performed, nor will it be appropriate to perform all listed checks for all terminals in all possible locations. It is an example of the types of activities that should be considered when developing a terminal inspection procedure.

Evidence - Maintain a record of inspections, findings, and incidents

Due to the assessment requirements for PCI DSS v3.0, all activities performed to fulfil requirement 9.9 need to generate evidence that controls are in place to protect your terminals against tampering and substitution and provide an auditable history.

Policies and procedures must combine to maintain a system that provides a record of all terminals, inspections carried out, findings from the inspections, and actions after an incident was reported.

Potential tools to help merchants comply with requirement 9.9

Termtegrity SpotSkim

Used by merchants to inspect, inventory, and document all their terminals via a software-as-a-service online portal and mobile app. Smartphones and tablets use the app to take photos of devices, create a visual inventory, and reference them against a known good state. All devices can be recorded and the state that they are in, such as in active use/in storage/awaiting replacement, etc.

SpotSkim then drives the inspection process and periodically requests new photos to be compared to the 'known good' reference images. Device attached bar codes can be used with the app to immediately identify the device and speed up checks.

Merchants can create reports for all devices and inspections to provide proof that terminal care has been performed according to the PCI DSS requirements.

SpotSkim enforces access controls to ensure only authorised personnel can update the inventory whilst checks can be carried out by other staff.

http://www.termtegrity.com

Libro Credit Union - Skimming Prevention Kit

Gives workable examples of an inspection form, terminal inventory form, and information regarding staff training & reporting.

https://www.libro.ca/Learn/Tools/SkimmingPreventionKit.pdf

Unique Secure

Manufacturer of stands and harnesses to prevent unauthorised access to the underside of the PIN pad, reducing the opportunity for tampering. A lock and tether prevent the PIN pad from being removed from the intended location – be that in-store or off-site.

http://www.unique-secure.com/page/chip-and-pin

Tesa Sribos coded security labels/tape

An example of tamperproof seal/tape that could be used to show tampering with point-of-sale devices. The unique codes can be cross referenced as part of periodic checks. A bar code brand ID can also be incorporated.

http://www.tesa-scribos.com/eng/security_technologies/tesa_codeseal

Versapak Tamper Proof Bags

For the storage of offline/in storage devices to provide assurance that they haven't been tampered with when not in use. Can also be used when sending devices for repair/replacement.

http://www.versapak.co.uk/

More information

PCI-SSC - Skimming Prevention: Overview of Best Practices for Merchants
https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

PCI-SSC - Skimming Prevention: Best Practices for Merchants
https://www.pcisecuritystandards.org/documents/Skimming%20Prevention%20BP%20for%20Merchants%20Sept2014.pdf

PCI-SCC - Increasing Security and Reducing Fraud with EMV Chip and PCI Standards
https://www.pcisecuritystandards.org/pdfs/PCI-EMV-Final1.pdf

VISA – Protect your terminals from illegal tampering
http://usa.visa.com/download/merchants/data-security-protect-terminals-from-illegal-tampering-020513.pdf

VISA – Point-of-Sale: Terminal Tampering Is a Crime… and You Can Stop It
http://usa.visa.com/download/merchants/alert-pos-terminal-tampering-020311.pdf

MasterCard – Terminal Manipulation
http://www.mastercard.com/us/company/en/docs/Terminal_Manipulation_At_POS.pdf

Verifone - PIN Pad Security Best Practices
http://www.verifone.co.uk/media/2616286/PIN%20Pad%20Security%20Best%20Practices.pdf

Reference Documentation

- PCI DSS v3
- PCI DSS v3 ROC Reporting Template v1.1
- PCI DSS v3 Summary of Changes
- PCI Skimming Prevention: Best Practices for Merchants Version 2
- PCI Guru 2014/12/09
- http://www.pymnts.com/january/2012/addressing-card-skimming-at-the-point-of-sale-pci-and-emv-chip-technology
- Financial Fraud Action UK - www.financialfraudaction.org.uk

About Sysnet Global Solutions

Established in 1989, Sysnet Global Solutions provides payment card industry compliance services, specialising in PCI DSS compliance validation and merchant retention solutions for acquiring organisations. Sysnet offers a range of services, including its award-winning, proprietary, compliance management and merchant intelligence solution Sysnet.air®, to a wide variety of businesses including acquirers, ISOs, international banks, payment service providers and merchants. Headquartered in Dublin, Ireland, Sysnet has clients in more than 40 countries worldwide.