

Requirement 9.9: Security for Point of Sale Devices



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

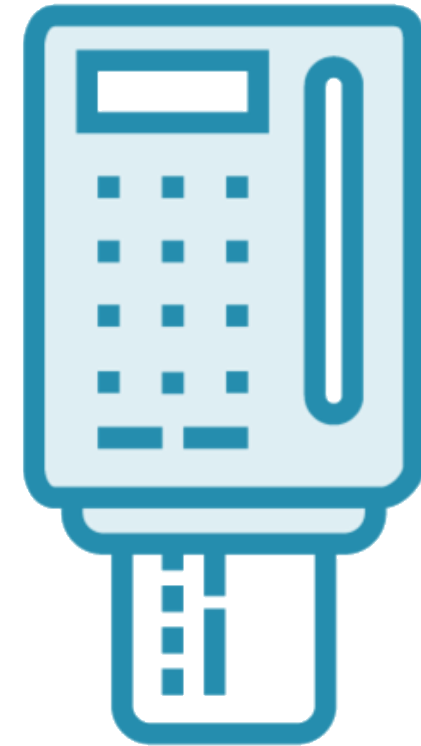
@withoutfire www.withoutfire.com





Requirement 9.9

Secure physical payment devices to prevent skimming attacks, tampering and substitution





Requirement 9.9

Protect devices that capture payment card data via **direct physical interaction** with the card from **tampering** and **substitution**.

**Not
contactless
only
readers**



Requirement Guidance

- Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. Criminals will also try to add “skimming” components to the outside of devices. In this way, transactions may still be completed without interruption while the criminal is “skimming” the payment card information during the process.
- This requirement is recommended, but not required, for manual key-entry components such as computer keyboards and POS keypads.
- Additional best practices on skimming prevention are available on the PCI SSC website.



9.9 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Policies and procedures
Examine records	-	
Interview people	-	





Requirement 9.9.1

Maintain an up-to-date list of payment entry devices.





Requirement 9.9.1

Maintain an up-to-date **list of devices**. The list should include the following:

- Make, model of device.
- Location of device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.



Requirement Guidance

- Keeping an up-to-date list of devices helps an organization keep track of where devices are supposed to be, and quickly identify if a device is missing or lost.
- **The method for maintaining a list of devices may be automated** (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned.

9.9.1 Testing Procedures

Observe/examine systems and settings	Y	Physical devices and device locations
Examine documentation	-	
Examine records	Y	List of devices
Interview people	Y	People responsible for maintaining the list of devices





Requirement 9.9.2

Periodically inspect devices for evidence of tampering or substitution.



Requirement 9.9.2

Periodically inspect device surfaces to detect tampering *(for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).*



Requirement Guidance

- Regular inspections of devices will help organizations to more quickly detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices.
- The type of inspection will depend on the device. Device vendors may be able to provide security guidance and “how to” guides to help determine whether the device has been tampered with.
- **The frequency of inspections will depend on factors such as location of device and whether the device is attended or unattended.**

9.9.2 Testing Procedures

Observe/examine systems and settings	Y	Physical inspection process
Examine documentation	Y	Device inspection procedures
Examine records	!	Records of inspections
Interview people	Y	Responsible people





Requirement 9.9.3

Train in-store staff to recognise criminal attacks against devices.





Requirement 9.9.3

Provide **training** so **staff** are aware of any attempted **tampering or replacement of devices**, including:

- Verify the **identity of third-party persons** prior to granting access to modify or troubleshoot devices.
- **Do not** install, replace, or return devices **without verification**.
- Be aware of **suspicious behavior** around devices and report it.



Requirement Guidance

- Criminals will pose as authorized maintenance personnel to gain access to POS devices. All third parties requesting access to devices should always be verified before being provided access. Many criminals will try to fool personnel by dressing for the part, and could also be knowledgeable about locations of devices, so it's important staff are trained to follow procedures.
- Criminals may send a “new” POS with instructions for swapping it and “returning” the legitimate POS to a specified address. Staff must verify with their manager/supplier that a device is legitimate and trusted before installing it.



9.9.3 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Staff training materials
Examine records	!	Training records
Interview people	Y	Staff at POS locations





Requirement 9.10

Polices and Procedures





Requirement 9.10

Ensure that **security policies** and operational **procedures** for restricting physical access to cardholder data are **documented, in use**, and **known** to all affected parties.



Requirement Guidance

- Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.

9.10 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Security policies, Operational procedures
Examine records	-	
Interview people	Y	Responsible people and people who need to know



That's Fine in Theory

