

SpotSkim

Inspect - Inventory - Document

Comply with PCI DSS 3.0, Requirement 9.9







The third revision of the PCI Data Security Standard (DSS) took effect January 1, 2015 and included the new requirement 9.9, which deals with the security of "devices that capture payment card data via direct physical interaction with the card" as a measure to prevent tampering, substitution, and skimming. Until June 30, 2015, this requirement is a best practice. On July 1, 2015, it becomes enforceable and merchants will be measured against it in their Report on Compliance (ROC).

While a small subset of the overall standard, compliance with 9.9 can be a huge endeavor requiring new policy and changes in organizational behavior.

The purpose of this document is to show how SpotSkim supports these changes and makes compliance with requirement 9.9 as easy as possible by reviewing each item listed on the ROC.

PCI DSS Requirement 9.9 - Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

Note: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.

ROC Requirement 9.9 - Examine documented policies and procedures to verify they include:

- **Maintaining a list of devices.**

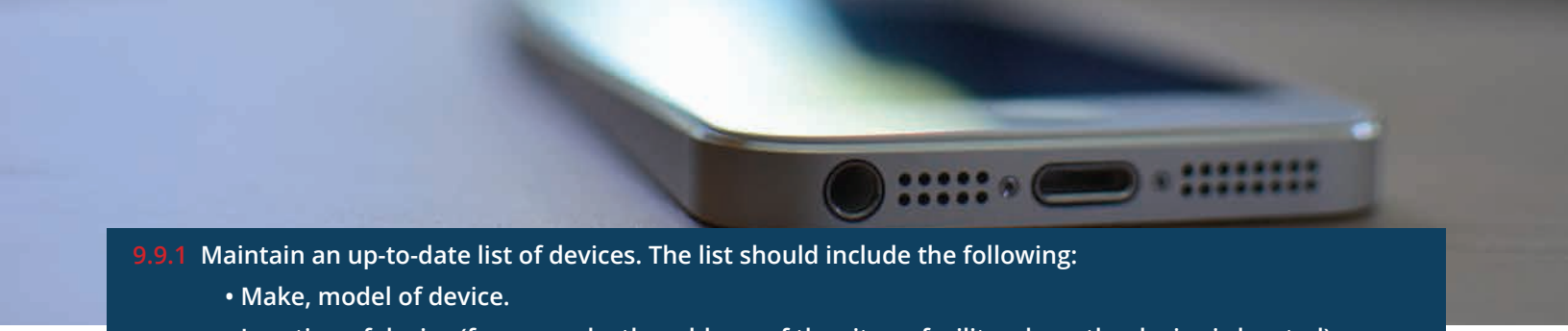
SpotSkim provides a default policy that requires the list be maintained or it allows customers to upload their own policy. SpotSkim reporting enables real-time tracking of a merchant's devices by making this list accessible at the push of a button.

- **Periodically inspecting devices to look for tampering or substitution.**

Spotskim's default policy requires this. It is enabled in practice when the merchant answers the "Location Risk" assessment for their locations thereby setting the inspection period for the devices.

- **Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices.**

SpotSkim provides a default video training within the app that covers how to perform an inspection, what to look for on the device and in the surrounding environment, and how to mark a device as compromised if they suspect tampering/substitution.



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.

9.9.1 a Ensure the list of devices includes:

- 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

SpotSkim tracks each device's make and model, where the device is currently located as well as where is has been, and a unique "Asset Tag" that identifies each device. All of this information is accessible at the click of a button with the built-in reporting.

9.9.1 b Provide a sample of devices from the list and observe device locations to verify that the list is accurate and up-to-date.

SpotSkim ensures that this list will always be both as accurate and up-to-date as the most current inspection of the devices. Simple reporting allows this device list to be pulled at the click of a button.

9.9.1 c Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc.

SpotSkim tracks the meta-data on all devices and inspections including who added the device, when it was added, the current location and location history, and whether the device is in-service, out of service, under maintenance, or compromised.

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).

9.9.2 a Examine documented procedures to verify processes are defined to include the following:

- Procedures for inspecting devices.

SpotSkim provides a default device inspection policy and video training which instructs users on how to perform an inspection on a device and the environment surrounding the terminal.

- Frequency of inspections.

SpotSkim's "Location Risk" feature allows merchants to assess an individual location's risk and set a default inspection frequency for each device within that location. This creates a balance of efficiency and effectiveness by ensuring that the amount of inspections performed is appropriate for the risk of tampering presented at that location. Built-in alerts and escalation procedures ensure that no device inspections will be missed.

9.9.2 b Interview responsible personnel and observe inspection processes to verify:

- Personnel are aware of procedures for inspecting devices.

SpotSkim's tracks when a user reviews both the device inspection policy and the training video and makes this data available as a built-in report, ensuring staff responsible for inspection are equipped with the tools and training they need and management can track and follow up with staff that have not reviewed the tools.

- All devices are periodically inspected for evidence of tampering and substitution.

SpotSkim sets the inspection period via the "Location Risk" feature and tracks all device inspections across a merchant's organization including date, time, who inspected the device, pictures of the device in-state, answers to device inspection questions, device status, and the risk of compromise/tampering based on all the inspection data. Additionally, alerts are generated when device inspections are missed, with escalation to management and organization administrators.



9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

9.9.3.a Review training materials for personnel at point-of-sale locations to verify it includes training in the following:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.

The training video provided with SpotSkim stresses the importance of verifying the identity of any one who is attempting to access the organization's devices.

- Not to install, replace, or return devices without verification.

The training video included with SpotSkim instructs users to validate any devices before installing, removing, replacing or returning the device.

- Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

Both the training materials and process of inspection with SpotSkim instruct users to be aware of the environment around and access to the devices.

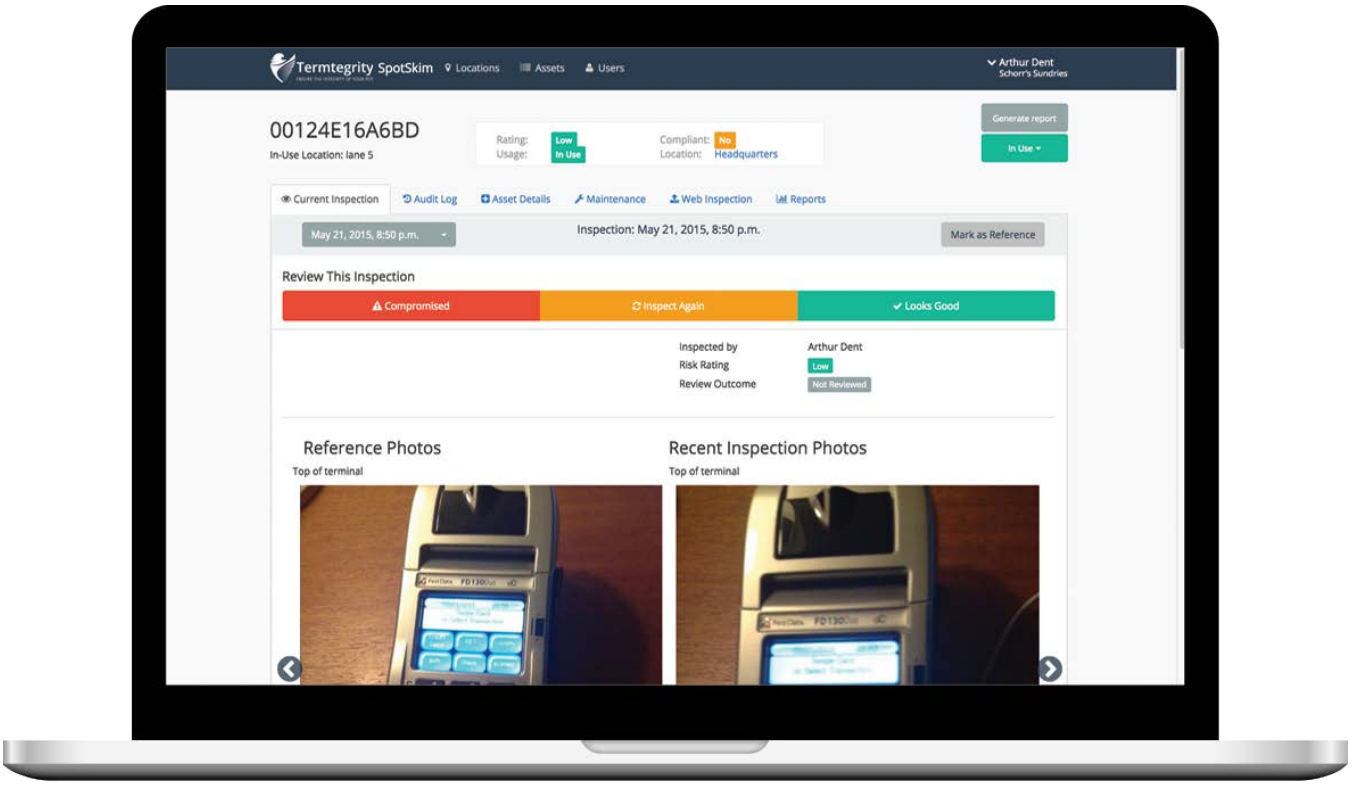
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

All SpotSkim's training materials and the device inspection process while using the solution, instruct users to log any suspicious behavior or suspected tampering in the tool and then report their concerns to management immediately.

9.9.3.b Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Not to install, replace, or return devices without verification.
- Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer

SpotSkim's tracks when a user reviews both the device inspection policy and the training video and makes this data available as a built-in report, ensuring staff responsible for inspection are equipped with the tools and training they need and management can track and follow up with staff that have not reviewed the tools.



SpotSkim is the only automated, visual POS inspection tool available and can be purchased directly from Termtegrity or through our network of partners.

Visit **termtegrity.com** for more information.

ABOUT TERMTEGRITY

Termtegrity provides innovative solutions to help merchants protect their businesses and their customers' information by ensuring the integrity of their point-of-sale environment.

Termtegrity

Termtegrity, Inc.
312.768.8376
termtegrity.com
@termtegrity

©2015 Termtegrity, Inc. All Rights Reserved.

