Procedure for Periodically Inspecting Devices

The goal of this task is to detect tampering, skimming or substitution of card-reading devices and terminals.

During the periodic physical review of the asset inventory, the following checks should be performed to detect tampering where applicable to POS or Mobile POS devices:

1. Verify the serial number physically present on the device.
2. Inspect area around the devices to detect any rogue cameras, NFC readers or other recording devices that could try and capture sensitive data like PIN numbers.
3. Inspect the physical keypad (Pin Pad) or keyboard of the devices to ensure that no skimming devices / key-logging devices have been placed. These can look like they are part of the device itself, hence it is important to pay close attention while carrying out the inspection.
4. Inspect the card swipe to ensure that there has been no tampering with it.
5. If applicable verify that authorized CCTV cameras around the devices are working and angled correctly to detect any intruder trying to physically tamper with the devices.
6. Frequency and type of inspection of devices that are left unattended and / or subject to high transaction volumes should be higher as these are at a greater risk of being tampered with.
7. Verify that the security stickers, or company stickers placed over screw holes or seams have not been tampered with.
8. Ensure that the cables have not been changed to incorporate the additional wires required to capture card data.
9. Ensure telephone rooms, panels, routers, drops, and connections that support terminal infrastructure are adequately protected and have minimum access to outsiders.
10. For Mobile POS devices, check below the SIM card cover plate for skimming devices.
11. Mobile POS devices that are connected to a phone or tablet should be inspected to ensure that no malware is installed and that the PIN is entered on the PCI approved terminal and not directly on the mobile or tablet.
12. Any modifications or wires to the smartcard slot need to be checked on devices equipped to read EMV or chip cards.
13. Periodically rotate the individuals performing the device-checking to ensure nothing gets missed and to eliminate collusion