Guidance for Inspecting Payment Card Devices

"Skimming devices" sweep up customers' card data as it enters a payment terminal. It's vital that you and your staff know how to spot a skimming device, what your payment terminals should look like, and how many you have. You need to regularly check your payment terminals to make sure they have not been tampered with. If there is any suspicion that a terminal has been tampered with, DO NOT USE it, and report this immediately to the PCI Committee.

The Following steps should be taken to mitigate the risk of device tampering:

Keep a List of all payment devices, record the serial numbers, and take pictures of the device (front, back, cords, and connections) to document what they are supposed to look like. A list of all those authorized to use the devices should also be maintained.

Look for Obvious Signs of tampering, such as broken seals over access cover plates or screws, odd/different cabling, or new devices or features you don't recognize, such as a different serial number. The PCI Councils' guide: Skimming Prevention – Overview of Best Practices for Merchants offers more information on skimming and preventive measures to take.

Protect Devices by keeping them out of customer's reach when not in use and restrict public viewing of the screens. Make sure devices are secure while the office is closed.

Control Repairs by only allowing payment terminal repairs from authorized repair personnel, and only if you are expecting them. Monitor any third-parties with physical access to your payment terminals, even if they are there for another reason, to make sure they do not modify your payment devices.

Call Student Accounts immediately if any tampering is suspected of college-issued devices. For devices issued by a third-party, the procedures outlined in the agreement must be followed and the Finance Office should be contacted.

Complete the PCI Inspection Log regularly by verifying devices have not been tampered with, replaced, or changed. Depending on how often the devices are used and where they are stored will determine if they are inspected daily, weekly, or monthly. Below is a suggested guide on how often the devices should be inspected.

Frequency Used	Location of Device	Suggested Inspections
Daily	In Public Area or Secure Location	Daily
Weekly	In Public Area	Daily
Weekly	In Secure Location	Weekly
Monthly	In Public Area	Daily
Monthly	In Secure Location	Monthly

FSC PCI Device Inspection Log

All devices that can accept credit card payments should be inspected regularly, including those not issued by the College. Inspections should verify that the device serial number matches what is on file, and that the device shows no evidence of tampering and has not been altered in any way. Depending on how often the devices are used and where they are stored will determine if they are inspected daily, weekly, or monthly.

Please print a hard copy of this form to complete and keep on file for each payment card device. A copy of this log will be requested annually for PCI Compliance.

Department	
Device Location	
Merchant ID	

Device Make/Model	Serial Number	Date Inspected	Signs of Tampering	Inspected By

Farmingdale State College
State University of New York
Farmingdale State College
2350 Broadhollow Road
Farmingdale, New York 11735
934-420-2000
farmingdale.edu

Device Make/Model	Serial Number	Date Inspected	Signs of Tampering	Inspected By

Farmingdale State College
State University of New York
Farmingdale State College
2350 Broadhollow Road
Farmingdale, New York 11735
934-420-2000
farmingdale.edu