# Linfield College

## Protecting Your Credit Card Swipe Devices from Illegal Tampering

The threat of **Point of Sale (POS) terminal tampering is serious and worldwide. Every day criminals install skimmers, keyKatchers, and other devices that grab cardholder data.** The cardholder data is then used to create cloned cards or to break into bank accounts to steal money.

To help Linfield College users anticipate threats and to keep your POS devices safe from criminals, the Controller's Office has provided the following information, tips, and checklist.

## Point of Sale Device Protection

**Watch your POS Equipment**

- Examine your POS device that accept credit and debit cards, look for anything abnormal. Examples-Skimmers, Keykatchers, missing or broken seals, damage to the device, damageto external cable or broken port or other materials that could mask damage ortampering.
- The PCI best practice requires that you inspect your POS device and PIN- entry devices (PED) weekly. Check for the following:
    - Is the POS device and PED in its designated location?
    - Is the POS device's manufacturer name, model and serial number correct? Each merchant must maintain a record of the model and serial numbers for reference. The Controller's Office maintains a record of all POS devices wewell.
    - Is the color and condition of the POS device as expected with no additional marks, or scratches, especially around the seams of the terminal window display?
    - Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
    - Is the number of connections to the POS device as expected, with the same type of color of cables, and with no loose wires or broken connector?

## Physical Security

**Safeguard Your POS Equipment and Surrounding Areas**

- **All POS devices should be locked up in a secure area at the end of each business day** to prevent any unauthorized removal attempts from your merchant location.
- **Check your POS environment** for hidden cameras or recording devices. Merchants should:
    - Verify there are no additional or unauthorized displays where a camera could be hidden. Examples-adjacent walls, plaques or signs, brochure containers or personal items.
    - Inspect the ceiling area above the POS device.

## Staff Communication and Education

**Train your staff on POS Equipment Tampering Prevention**

- As part of card acceptance all staff (all users) will be trained annually on how to recognize noticeable signs of equipment tampering by the Controller's Office. It will be the responsibility of the **POS custodian in each office/department to train any new employees in their area to recognize signs of equipment tampering before they can process credit or debit cards.**
- Control POS device and PED access by service support representatives. Allow only validated and authorized service personnel to access POS devices and PED's. Unauthorized or unexpected individuals should not be allowed access to the POS device.
    - The Controller's Office is the only area that will provide support for your POS equipment. The Payment Card Coordinator will work directly with the POS custodian in your department on all equipment issues.
    - **Any third-party persons claiming to be repair or maintenance personnel are prohibited** from gaining access to your POS device. Report any personnel attempting to gain access to your POS device to the Payment Card Coordinator within the Controller's Office. Do not accept any replacement POS devices from third-party personnel or company.
    - Ensure that only authorized support personnel are escorted and monitored at all times while attending the equipment.

## What to Do In the Event of POS Tampering

**If you believe your merchant operation has been subject to device tampering, contact the Payment Card Coordinator (Amy at 503-883-2608, Vivian at 2780 or Carol at 2618) within the Controller's Office and the Campus Police Department.**

**Weekly Inspection Checklist for POS Terminal Tampering**

- Checked the device for **Skimmers and Keyloggers** (Figure 1)
- Checked for **missing or broken seals** (Figure 2)
- Checked for **damage, and damage to the external cables**
- Checked for **broken or damaged ports** (Figure 3)
- Device was **found in designated location**
- Checked **the model and serial number of device and matched** to the information on record
- Checked device for **marks or scratches around the seams and terminal window display**
- **Checked the number and color of cable connections with no loose wires or broken connectors**
- Checked POS **environment for hidden cameras.** (Figure 4)
    - Ceilings
    - Adjacent walls
    - Plaques and signs
    - Brochure containers
    - Personal items

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

Signature:_____ Date: _____

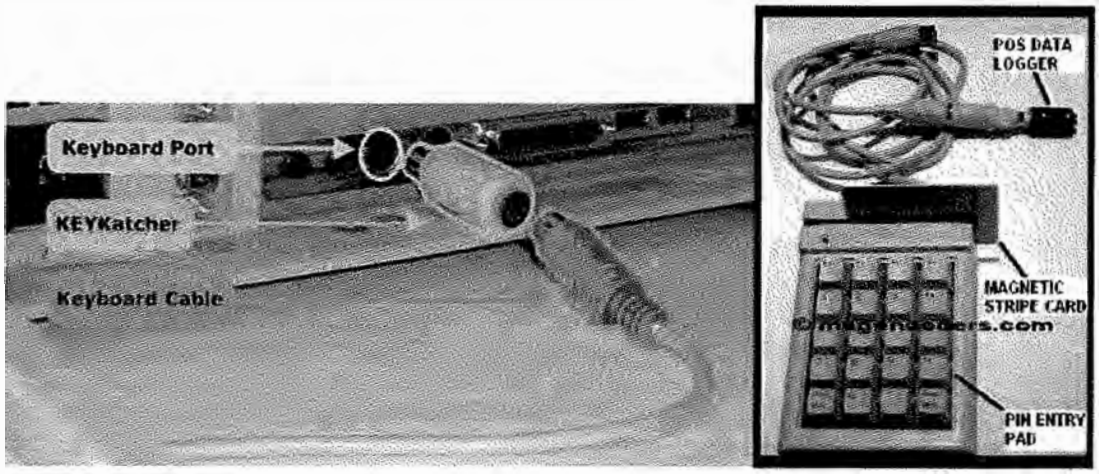
Signature:_____ Date: _____

Signature:_____ Date: _____

**Figure 1 - Keyloggers and Skimmers Explained:**

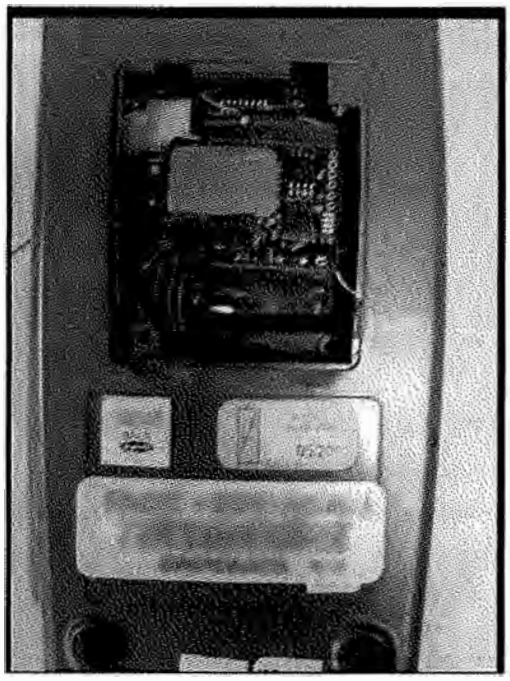
A keylogger is a piece of software or a hardware device — that logs every key you press on your keyboard. It can capture personal messages, passwords, credit card numbers, and everything else you type.

Keylogger Images:




A skimmer is used to collect data from the magnetic stripe of a credit or debit card.

Skimmer Image:



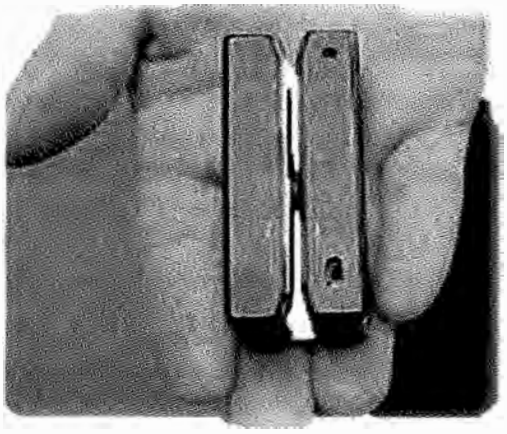


**Figure 2 – Missing or Broken Seals**

**Figure 3 – Damage to device or damage to ports**

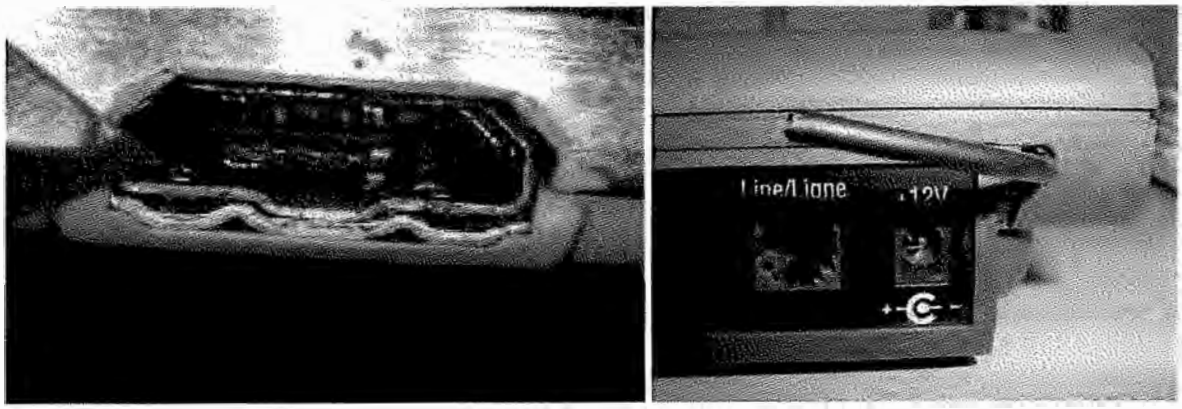
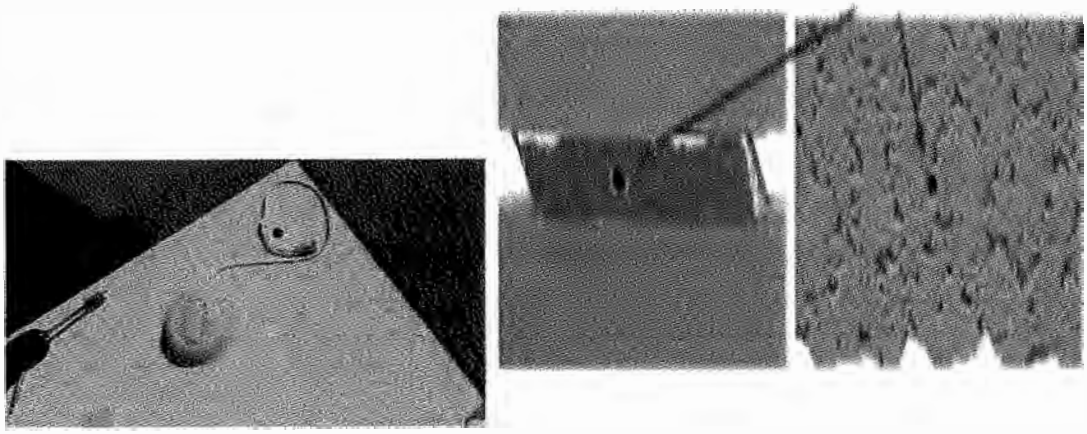


**Figure 4 – Hidden Cameras**



**PCI DSS 3.0 became effective January 1, 2015. As of July 1, 2015 PCI DSS 9.9 changed from a best practice to a requirement. Below is the overview of the 9.9 PCI DSS requirements.**

| PCI DSS Requirements | Guidance |
|---|---|
| 9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.<br><br>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.<br><br>Note: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement. | Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. For example, they will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card information every time a card is entered. Criminals will also try to add "skimming" components to the outside of devices, which are designed to capture payment card details before they even enter the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card details are captured twice: once by the criminal's component and then by the device's legitimate component. 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. |
| 9.9.1 Maintain an up-to-date list of devices. The list should include the following:<br>• Make/model of device<br>• Location of device (for example, the address of the site or facility where the device is located)<br>• Device serial number or other method of unique identification. | 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. |
| 9.9.2 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).<br><br>Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. | 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—for example, photographs of devices that are known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also 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. For example, devices left in public areas without supervision by the organization's personnel may have more frequent inspections than devices that are kept in secure areas or are supervised when they are accessible to the public. The type and frequency of inspections is determined by the merchant, as defined by their annual risk-assessment process. |
| 9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:<br>• 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.<br>• Do not install, replace, or return devices without verification.<br>• Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).<br>• Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). | Criminals will often pose as authorized maintenance personnel in order to gain access to POS devices. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POS maintenance company (such as the vendor or acquirer) for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work wear), and could also be knowledgeable about locations of devices, so it's important personnel are trained to follow procedures at all times. Another trick criminals like to use is to send a "new" POS system with instructions for swapping it with a legitimate system and "returning" the legitimate system to a specified address. The criminals may even provide return postage as they are very keen to get their hands on these devices. Personnel always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business. |
| 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. | 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. |