Point-Of-Sale
Device Tampering Training

COMPLIANCE MANAGEMENT
EAST CAROLINA UNIVERSITY

Last updated December 20, 2017
East Carolina University is committed to following the guidelines as set out by the Payment Card Industry Data Security Standards. The standards as outlined in various policies upholds the integrity of the university and provides security against wide-ranging threats to the Cardholder Data Environment.

The information in this presentation will inform you of the “Best Practices” to assist in your responsibilities to securing the devices and reducing the risk of Point-of-Sale Device Tampering.
Protection of Point-of-Sale Devices

- The point of sale device includes the Terminal and corresponding Pin Pad (if applicable)
- The devices are an important part of the Cardholder Data Environment
- Terminals and Pin Pads not in use should be secured in a location with minimal access
- Only authorized personnel within the various departments should be allowed access
  - Only ECU Compliance Management or ITCS staff should be allowed access to POS devices and must present proper identification
  - For First Data POS devices –
    - First Data will NEVER send technicians to perform maintenance
    - First Data will not call you unless you have called their help desk with a ticket request (do not provide terminal info over the phone unless you call First Data’s 1-800 number)
  - For third party POS devices – Vendor should present proper identification if requesting access to POS device(s)
  - Staff should document date, time and name of individual(s) who are provided access to POS devices
- Employees should inspect for physical tampering daily or at the beginning of their shift.
Protection of Point-of-Sale Devices

By protecting your POS devices and inspecting them for tampering, you:

- Protect the integrity of East Carolina University
- Protect the Personal Identifiable Information of clients/customers
- Secure the Cardholder Data Environment
- Reduce the risk of fraud
- Reduce the risk of device tampering
There have been many cases where criminals have:

- Stolen terminals from cash lanes and desks not in use.
- Broken into a store and compromised the terminals.
- Swapped a good terminal for a compromised terminal, using large items to block attendants’ line of sight.
- Swapped good terminals for compromised terminals or installed malware while posing as a service technician.
- Added overlays with skimming and key-logging hardware.
- Shipped compromised terminals to merchants under the guise of a terminal upgrade and required the good terminals to be returned to the criminal.
Examples of Terminal Fraud

Terminals will have a sticker attached to the underside, which provides details of the product and will include a serial number. The majority of terminals will also have a method of displaying the serial number electronically.

As part of your regular checks, note the serial number on the bank of the terminal and check this against the electronic serial number.

Additionally, run your finger along the label to check that it is not hiding a compromise.

Examples of Terminal Fraud

Changes to terminal connections can be difficult to spot.

In these images, the criminal completely changed the cable used to connect the terminal to the base unit.

This was to incorporate the additional wires required to capture card data.

Examples of Terminal Fraud

The modern digital cameras used to record the cardholder entering his or her PIN are very small when removed from their cases.

This makes them very easy to hide or disguise at the merchant location.

This type of miniature camera can easily be hidden in a ceiling tile above the terminal.
Examples of Terminal Fraud

Staff should also be aware of additional, unfamiliar electronic equipment connected to the terminal, the cash register, or the network connections. This device records and decrypts ISDN data.

Examples of Terminal Fraud

In this picture, the criminal entered the merchant location posing as a service engineer.

He stated that to prevent credit card fraud the terminal must be placed in this secure box. He then gave the staff a sheet of printed instructions.

The box contained a card skimmer and miniature camera.

Be cautious of unannounced service visits. Firstdata will NEVER come on site. Only ECU Compliance Management & ITCS staff or your POS vendor (If using a 3rd party) should be given access. If you are unsure ask your supervisor before allowing access, request to see the representatives identification and record the date and time of their visit.

Examples of Terminal Fraud

Staff should also be aware of the addition of overlays. An overlay can be a small sticker that forms to the device and covers the keyboard area.

Overlays may hide damage due to tampering or wires that can allow for keyboard logging. Overlays should not be used.

Examples of Terminal Fraud

In a Near Field Communication (NFC) attack, an NFC reader (in this case a smartphone) is placed between the terminal and the customer to capture the card data during a tap transaction.

Additional equipment should not be placed near or around terminals.
Examples of Terminal Fraud

EMV or Chip Cards are not immune to skimming. Staff and consumers should be aware of modifications or wires to the smartcard slot. If anything appears different with the device, it should be reported immediately.

Is the Terminal and Pin Pad in its designated location?

Is the Terminal and Pin Pad name and model number correct?

Is the color and condition of the Terminal and Pin Pad as expected, with no additional marks or scratches (around seams or 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 Terminal and Pin Pad as expected, with the same type and color of cables, and with no loose wires or broken connections?

Is the Terminal and Pin Pad only being used by the authorized representatives?

Verify there are no additional or unauthorized displays where a camera or NFC equipment could be hidden near the Terminal or Pin Pad.

Are there any unauthorized electronic devices (phones, iPods, etc.) near the Terminal or Pin Pad?

Inspect the ceiling area above the POS device for cameras.
What to do in the event of POS Device Tampering?

If you believe your POS device(s) have been subject to tampering, notify your supervisor and contact ECU Compliance Management immediately:

Phone: (252)737-5441
Email: ecommerce@ecu.edu