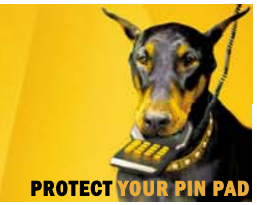
Recommended Checklist for Integrated Point of Sale Devices



Manager: _____ Date: _____

Check the card reader, if the card swipe is integrated into the keyboard, compare it to a photograph of a keyboard that has not been tampered with. Is anything different?

- ❑ Do the serial numbers match?
- ❑ Has the keyboard been tampered with or opened?
- ❑ Is there an additional keyboard?
- ❑ Are there any unexplained wires near the card reader?
- ❑ Is the same number of cords plugged into the outlets?
- ❑ Is there more than one read head in the card reader?
- ❑ Does the area around the card reader look like it has been wiped clean?
- ❑ Does the back of the PIN pad look like it has been replaced with a new back? Feel if a communication port has been installed at the back (Figure 3 on next page).
- ❑ Are there any key catchers (Figure 4 on next page) plugged in between the cable of the keyboard and your computer hard drive?

Check the surrounding area for pin-hole cameras

- ❑ Are there any cameras that could be used to capture PINs in the following locations:?
  - In the ceiling (see Figure 5B)
  - On adjacent walls, plaques or signs
  - In any brochure containers or personal items
  - In the displays behind the cash desk
  - In a cigarette package or other sales product
  - At least once a week, check behind the ceiling panels above the PIN pad where camera equipment could be installed. Are there any extra wires? Check storage areas, washrooms and other low traffic areas behind the sales area. Are there any extra wires? Are there any recording devices such as MP3 players, flash drives, DVDs or VCRs?

An example of how PIN pads are stolen in order to tamper them...

Fraudsters have been purchasing bulky items most likely at end-of-day using the bulky items to block the cashiers view while an accomplice switches a PIN pad with a dummy PIN pad (see Figure 1). The fraudsters usually return first thing the next day switching back the now tampered PIN pad with the dummy pad.

Educate staff

- ❑ Were there any unusual distractions? Was there any unusual activity you noticed?
- ❑ Hand PIN pad to customers only for PIN entry.
- ❑ Scratch test - some merchants have chosen to put a unique mark on PIN pads to recognize their own device.

Check surveillance cameras

- ❑ Does everything look the same today as it did in previous surveillance footage?

Service Staff Identification

- ❑ Did service staff present identification before servicing the device? Did service staff arrive at an agreed-upon time? Did they introduce themselves? Was there anything unusual about their visit?

See over for visual clues to look for...

FOR MORE INFORMATION, PLEASE CONTACT YOUR ACQUIRER OR SERVICE PROVIDER

Visual Clues to Look For...

PROTECT YOUR PIN PAD

Be aware:

- Two or more people shopping together
- Buying bulky items
- Switching legitimate PIN pad with fake
- Know the location of your PIN pad at all times
- Make sure the PIN pad is secured when unattended

Figure 1: Footage of fraudsters switching PIN pads at a merchant location

Figure 2: Card skimming devices may be very small – make sure to look for them under counters and behind cash registers. They may even be carried by employees.

Figure 3A: Back of standard device. Run your fingers along the sticker on the back of the device to feel if the device may be compromised.

Figure 3B: Compromised device with a Communication Port and DIP Switch behind sticker.

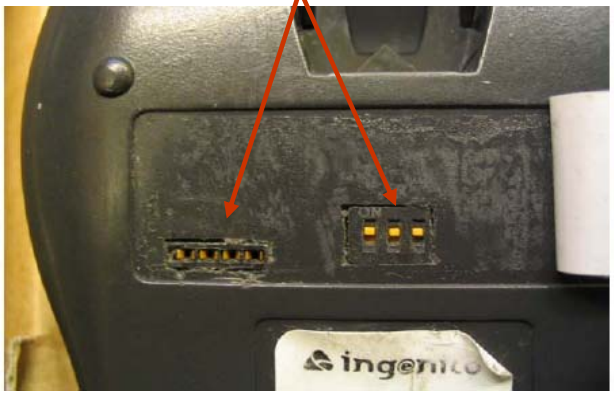
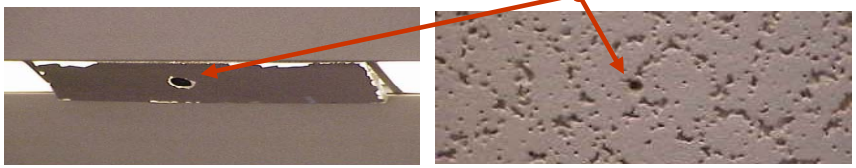


Figure 4: Keycatcher - this is a device that can be connected to a keyboard to record all the keystrokes.

Figure 5A: Wires in ceiling tile

Figure 5B: Pin-hole cameras in ceiling tiles



What if you discover something suspicious on or inside the device?

- Do not disturb the potential crime scene.
- Carefully move any PIN pads to a secure area.
- Contact local law enforcement and your Acquirer immediately (process to be defined by each merchant—could be corporate security, local law enforcement and your Acquirer).