Point-of-Sale Terminal Tampering Is a Crime . . . and You Can Stop It

Increasingly, criminals with sophisticated tools are actively targeting vulnerable merchant point-of-sale (POS) terminals to steal payment card data and PINs for counterfeit fraud purposes. That's the bad news! The good news is that all acquirers, merchants, and processors can take appropriate steps to eliminate POS terminal weaknesses and the possibility of POS tampering.

Criminal gangs worldwide are illegally accessing active POS terminals and modifying them by inserting an undetectable electronic "bug" that captures cardholder data and PINs during normal transaction processing.

The impact of this type of crime can be significant to all key parties involved in card acceptance. An attack can not only undermine the integrity of the payment system, but diminish consumer trust in a merchant's business. In response to this emerging threat, acquirers, merchants and their processors need to proactively secure their POS terminals and make them less vulnerable to tampering.

The following best practices have been created to help merchants maintain the highest level of POS equipment security and reduce the possibility of terminal tampering. Although there is a tendency to look for that "one best practice" or "silver bullet" that will stop POS terminal tampering incidents, the most effective strategy is to apply as many best practices as possible in the form of a layered approach that will not negatively affect the business operation.

POS Equipment Protection

Keep a Watchful Eye on Your POS Equipment

- **Continually track and monitor all POS terminals that accept Visa® cards.** This involves examining POS terminals to identify anything abnormal (e.g., missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels, decals or other materials that could be used to mask damage from tampering).
- **At a minimum, routinely inspect your POS terminals and PIN-entry devices (PEDs) for the following:**
  - Is the POS terminal and its PED in its designated location?
  - Is the POS terminal's manufacturer name and/or model number correct?
  - Is the POS terminal serial number correct? Merchants must maintain a record of all serial numbers along with model numbers assigned to each of its acceptance locations, by register lane if applicable.
  - Is the number of POS terminals in use the same as the number of devices installed or assigned?
  - Is the color and condition of the POS terminal as expected with no additional marks or scratches, especially around the seams or terminal window display?
  - Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
  - Are the manufacturer's security markings and reference numbers as described?
  - Is the number of connections to the POS terminal as expected, with the same type and color of cables, and with no loose wires or broken connectors?
  - Is the number of connections entering the POS terminal as expected?
- **Use approved PEDs.** Merchants should only use PEDs that are currently approved by the Payment Card Industry Security Standard Council (PCI SSC). A list of such devices can be found at: *www.pcisecuritystandards.org*. Click Approved Companies & Providers and then visit the Approved PIN Transaction Security page.

Treat your PEDs like cash. Keep them locked up and/or out-of-sight when not in use.

Physical Security

Safeguard Your POS Equipment and Surrounding Areas

- **Whenever possible, secure POS equipment to prevent any unauthorized removal attempts from your merchant location.** The use of secure stands, tethers, alarms or security cables is an accepted practice. This prevents the substitution of terminals and protects against the possibility of tampering. Where permitted by the design of the terminal, the cables connecting to terminals should be protected using a conduit, or they should be held within a physically secure structure.
- **Carefully 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.
  - Inspect the ceiling area above the POS device.
- **Use a CCTV recording system to deter criminals from removing or tampering with POS equipment.** Position the CCTV cameras so that they properly monitor all POS terminal locations, but do not record PIN-entry actions during the transaction process.
- **Review the CCTV images on a regular basis to make certain your security measures are being carried out correctly and that your POS equipment has not been tampered with or impaired in any way.**
- **Retain the CCTV recordings for at least 90 days.**
- **Make sure the methods used to secure your POS equipment are carried out in accordance with any relevant disability legislation for the country in which the equipment has been deployed.**

Criminals often install a miniature camera or video recording device in the area near the POS equipment to record a customer entering his or her PIN during a transaction. These cameras are usually hidden in displays, such as special offer boxes or pamphlet holders, or in the ceiling directly above a POS device.

CCTV recording in public areas must be conducted according to local laws and regulations.

Staff Communication and Education

Train Your Staff on POS Equipment Tampering Prevention

- **As part of card acceptance training, make sure your staff is up to speed on how to recognize noticeable signs of equipment tampering.**
- **Control POS terminal and PED access by service support representatives.** Allow only validated and authorized service personnel to access POS terminals and PEDs. Unauthorized or unexpected individuals should **not** be allowed access to the POS equipment.
  - Develop and implement a policy and procedures to assist staff members in validating the identity of all POS equipment service support and repair technicians.
  - Ensure that authorized support personnel and technicians are escorted and monitored at all times while attending to the equipment.
- **If possible, implement "new" employee screening policies.**
  - Where legally permissible, conduct a background check on all employees prior to hiring.
  - As part of the new employee orientation, clearly communicate merchant staff information security responsibilities and their role in protecting POS devices.

Staff awareness of POS equipment tampering schemes and skimming attacks can help reduce the possibility of fraud exposure and associated losses in your merchant operation.

What to Do In the Event of POS Tampering

If you believe your merchant operation has been subject to device tampering, contact your acquirer immediately. You should also review the document *Visa Data Security: Tips and Tools for Small Merchant Businesses*, available as a downloadable PDF on *www.visa.com*.

WANT TO LEARN MORE ABOUT ACCOUNT INFORMATION SECURITY?

The following resources are available to all Visa merchants through the PCI Security Standards Council:

- A list of PCI devices can be found at: *www.pcisecuritystandards.org*. (Click Approved Companies & Providers and then visit the Approved PIN Transaction Security page.)
- Skimming Prevention – Best Practices for Merchants at *https://www.pcisecuritystandards.org/education/info_sup.shtml*