PROTECT YOUR MERCHANT TERMINALS FROM ILLEGAL TAMPERING

VISA

INSIGHT FROM VISA TO KEEP YOUR POINT-OF-SALE EQUIPMENT SECURE

KEEPING POINT-OF-SALE TERMINALS SECURE

By keeping your equipment safe and your staff trained — and by knowing what to do if there's a problem — you can prevent your business from falling prey to criminals out to steal payment card data and PINs from point-of-sale (POS) terminals.

The threat of terminal tampering is serious and worldwide. Every day, criminal gangs are out to illegally modify active POS terminals by inserting an undetectable electronic "bug" that gathers cardholder data and PINs during routine transactions.

The impact of this emerging crime can be significant to everyone in the payment industry. And it's not just the integrity of the overall payments network that suffers as a result. Acquirers, merchants and their processors who experience POS fraud feel the impact directly, with diminished trust in their businesses — and perhaps even the loss of their customers.

To help you anticipate threats and keep your POS terminals safe from piracy, Visa has assembled the following insights. Your business will not be negatively impacted or slowed by using them. Don't use just one; instead, use all that apply to your business.

Let these tips from Visa begin helping you stay safe today.

KEEP YOUR EQUIPMENT SAFE

There are several steps you can take to block thieves from tampering with your POS terminals.

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

- Track and monitor all POS terminals that accept Visa® cards.
- Simple abnormalities — a missing seal or screw, or extra wiring or holes, for instance — could be the first step to uncovering fraud. You should also look out for added labels, decals or other materials that may be masking damage inflicted by tampering.
- Only use approved PEDs and follow Visa's PED usage and retirement mandates detailed on www.visa.com/cisp under the PIN Security section.
- Comply with Visa's mandatory PED sunset dates.
- Rely on devices approved by the Payment Card Industry Security Standard Council, which provides a list at www.pcisecuritystandards.org. Click "Approved Companies & Providers," then go to the "Approved PIN Transaction Security" page. For the best protection, always purchase the highest version of PED available.
- Routinely inspect POS terminals and PIN-entry devices (PEDs) and secure terminals to counters to prevent removal.
- Implement a terminal authentication system to detect internal electronic serial number or connectivity changes.
- Use terminal asset tracking procedure for devices deployed, stored and shipped.
- At minimum, answer these questions each time as you do:
  - Is the POS terminal and its PED where it's supposed to be?
  - Is the manufacturer name and/or model number of the device correct? Merchants must maintain a record of all serial and model numbers assigned to each of their acceptance locations, including the register lane, if applicable.
  - Is the POS terminal serial number correct?
  - Does the number of POS terminals in use match the number of devices installed or assigned?
  - Is the color and condition of the POS terminal what you expect? Be sure to look for any additional marks or scratches — especially around the seams or terminal window display.
  - Do the manufacturer's security markings and reference numbers match those seen on the device?
  - Is the number of connections going to and from the POS terminal what you expect? Are the same types and colors of cables used? Are any wires loose or broken?

SECURE YOUR SALES AREA

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.

To keep the area surrounding your POS equipment safe and prevent terminal theft, follow these tips.

- Secure POS devices.
- Anchor your equipment with secure stands, tethers, or alarms to prevent devices from being replaced by substitutes and reduce the chance of tampering. Connector cables should also be safeguarded. Whenever possible, protect them by using a conduit, or contain them within a secure structure.
- Watch for hidden cameras or recording devices.
- Make sure unauthorized cameras aren't hidden in nearby displays, or embedded in ceilings above the POS device.
- Use a CCTV recording system.
- Install closed-circuit cameras to monitor all POS terminals. Position them so that they do not record customers' PIN-entry process, and in a manner consistent with access laws pertaining to the disabled.
- Review the CCTV footage regularly to ensure security measures are being followed.
- Retain the recordings for at least 90 days.

EDUCATE YOUR EMPLOYEES

Teach your employees how to spot possible tampering with POS devices and follow simple security procedures. Here are a few ways to reduce your risk.

- Teach your staff how to spot signs of POS equipment tampering.
- Ensure that POS tampering prevention is a priority that is shared by your staff. During orientation, tell new employees about the issue of POS tampering — and make them aware of their role in avoiding it.
- Allow only authorized service personnel to repair or modify POS terminals and PEDs. This can be helped by creating and following procedures to validate their identity, and remaining with them as they work.
- Implement employee screening policies. Where legally allowed, conduct background checks on new employees before they start working with you.

IF YOU SUSPECT TAMPERING

Contact your acquirer immediately if you believe a POS device has been compromised. Other tips and procedures are explained in *Visa Data Security: Tips and Tools for Small Merchant Businesses*, a downloadable .pdf available at www.visa.com.

MORE INFORMATION

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.

Visa PIN Security program details and other useful information for merchants can be found on www.visa.com/cisp in the PIN Security section.

Other best practices that can help small businesses avoid tampering have been gathered by the PCI Security Standards Council, and can be found online at: www.pcisecuritystandards.org/education/info_sup.shtml