

PROTECT YOUR CREDIT CARD TERMINALS AND DEVICES FROM ILLEGAL TAMPERING

KEEP YOUR EQUIPMENT SAFE

To safeguard your business tampering and fraud, follow these best practices:

- Track and monitor all terminals on a regular basis
- Watch for abnormalities such as missing seals or screws, extra wiring, holes or unusual labels/decals that could conceal tampering
- Routinely inspect the terminals by verifying the following:
 - o Is the terminal where it should be?
 - Is the manufacturer name and model number correct? Maintain accurate records of all serial and model numbers.
 - o Is the serial number correct?
 - o Is the device's color and condition consistent with expectations? Look for additional marks or scratches, especially near seams or the display.
 - o Are the connections to and from the terminal as expected?

EDUCATE YOUR EMPLOYEES

- Train staff how to recognize signs of equipment tampering.
- Reinforce that tampering prevention is a shared responsibility.
- Permit only authorized service personnel to repair or modify terminals.

IF YOU SUSPECT TAMPERING

• Follow your Incident Response Plan, ensuring that it includes updated contact information, responsible personnel, and emergency phone numbers.







EXAMPLES OF TERMINAL TAMPERING: FROM THE PCI STANDARDS COUNCIL

1. Internal Tampering Indicators

- Many terminals include a security label inside the receipt paper compartment, which contains the product's serial number.
- As part of routine inspections:
 - Verify the serial number against your records.
 - Run your finger along the label to ensure it is not covering or concealing hidden tampering.





2. Keypad Overlays

- Fraudsters may attach thin devices or stickers that sit on top of the keypad. These are called keypad overlays.
- These overlays can:
 - o Capture keystrokes, including PIN entry.
 - Conceal wires or other tampering devices.
- **IMPORTANT:** Overlays should never be used and staff should be trained to recognize and report them.

3. Terminal Connections

- Criminals may attempt to swap or modify terminal cables to capture card data.
- · As part of daily checks:
 - o Ensure all cables are securely connected.
 - o Verify that no additional or unauthorized connections have been added.
 - o Look for any signs of tampering on plugs, ports, or wiring.