

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:
 - Is the terminal where it should be?
 - Is the manufacturer name and model number correct? Maintain accurate records of all serial and model numbers.
 - Is the serial number correct?
 - Is the device's color and condition consistent with expectations? Look for additional marks or scratches, especially near seams or the display.
 - 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.



