PIN PAD SECURITY POLICY

EXPECTATIONS

Store Management is responsible for the physical security of the pin pad equipment during Store hours.

GUIDELINES

Prior to Store Opening

- Complete the Daily Pin Pad Security Survey
  - Manager or Coordinator must carefully inspect each pin pads daily for tampering prior to opening (see the Daily Pin Pad Security Survey in Reflexis or for Sierra in ThinkTime).
  - Utilizing the Verifone Anti-Skimmer device, check each pin pad daily to ensure they have not been tampered with.
    - Utilize the Anti-Skimmer Device job aid for directions on use of the Anti-Skimmer Device (refer to Knowledge Base or for Sierra refer to the Summit)

If there no obstruction of the card slot, the tool will show **GREEN** with "No Overlay Detected" (see photo).

If there is an obstruction of the card slot, the tool will show **RED** with "Overlay Detected" (see photo).

PIN PAD SECURITY POLICY

GUIDELINES

- If you identify any issues with a pin pad:
  - Immediately suspend the use of that register(s)
  - Notify your DM and DLPM
  - Contact the Systems Service Desk at **1-888-444-4848** and select Option 2. Advise the Service Desk Agent you would like to report a "security concern or event with a pin pad" and provide the following:
    - Division
    - Store #
    - Register #
    - A brief description of the potential issue

If a “Overlay Detected” displays on a PIN Pad email the SOC@tjx.com while copying (cc) your DM and DLPM

SECURING EQUIPMENT AND SUPPLIES:

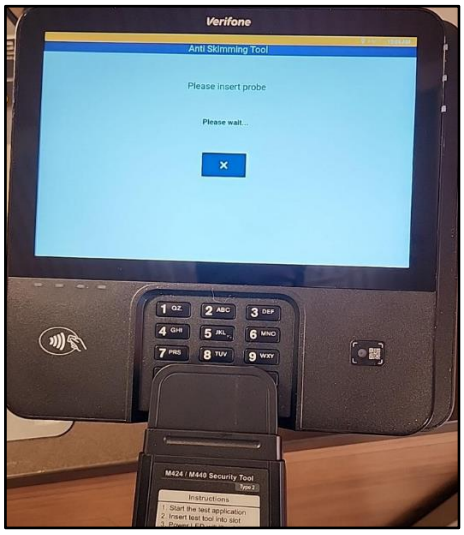
- Pin pads must be secured by a tether.
  - There are two methods of securing a pin pad:
    - Immobile- On a base with a tether (Majority of Registers).
    - Mobile- Without a base, but is tethered to the counter (Register 1).
  - Verifone Anti-Skimmer Device should be kept at the frontline in the locked change fund drawer.
  - Pin pad keys must be always kept in the key lock box in the safe.
  - If a pin pad key(s) is lost or stolen, contact your District Manager and District Loss Prevention Manager **IMMEDIATELY**.
- Access to ports on the pin pads must be blocked by a steel security plate. Report any unblocked ports to the Systems Service Desk.
  - If a Credit Card Skimmer was found on the PIN Pad, a register was stolen, or anything other than a PIN Pad/register/test tool needing to be repaired or replaced-
    Email SOC@tjx.com and cc your District Manager and District Loss Prevention Manager.
    In the email include
    - Store number, city and state
    - Register number, serial number
    - A brief description of the potential issue

PIN PAD SECURITY POLICY

SECURING EQUIPMENT AND SUPPLIES:

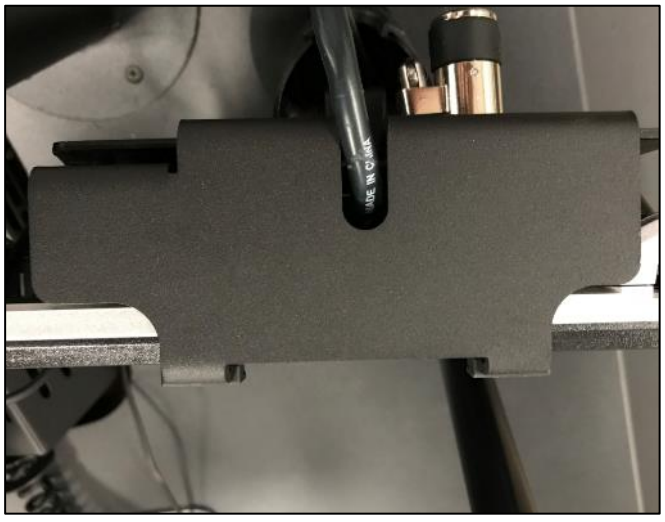
Front of Pin Pad
Note no signs of tampering

- No Pry Marks
- No Scratches
- No Damage



Directly below the keypad is the insert slot where chip credit cards are inserted

Access to ports are blocked by
a steel plate as seen in this top-down view



Card Reader – used by the customer to swipe Credit Card
Make sure area is clear and free of tampering devices

- All register rear covers must be securely locked except for stores that have a distributed register setup. A distributed setup is where the register drawer and "brain" are housed on separate shelves below the countertop.