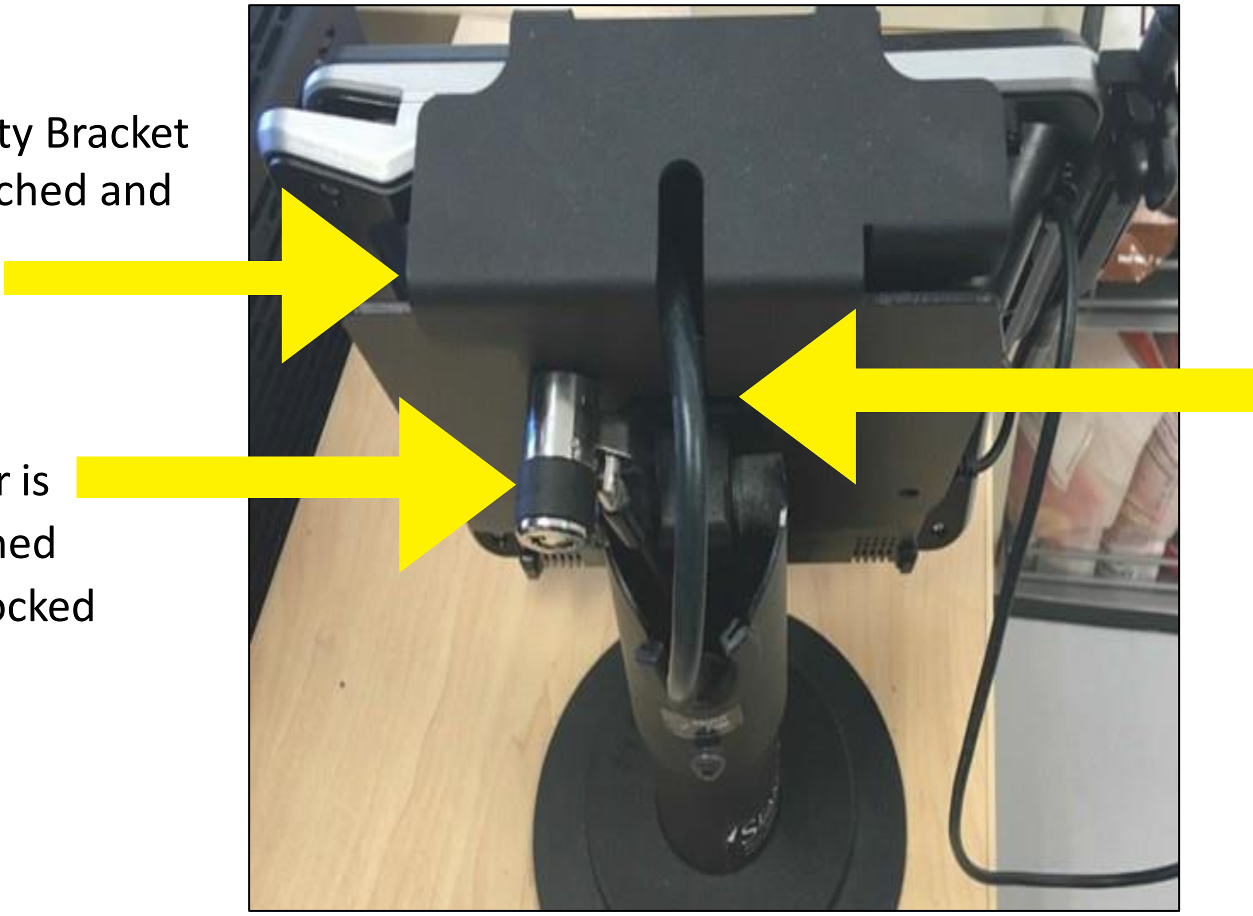
PIN PAD PROTECTION

All Cashiers must be aware of PIN pad security and keep it top of mind. PIN pads should never be installed, replaced, or returned without verification.

PROPER PIN PAD SETUP



Security Bracket is attached and locked

Cable is intact

Tether is attached and locked

PIN PAD PROTECTION

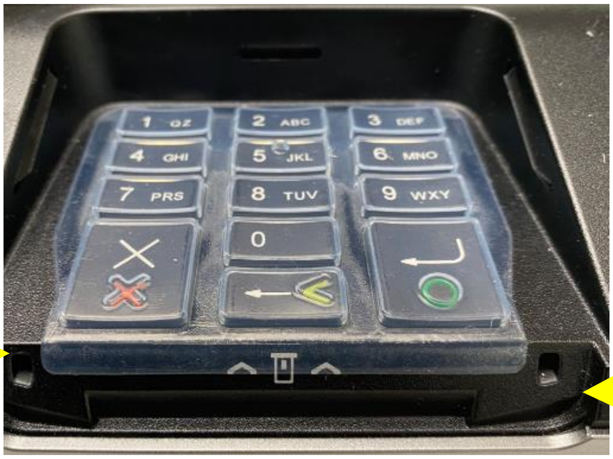
NOTICE

Be aware of suspicious behavior around PIN pads. Alert signals could include:

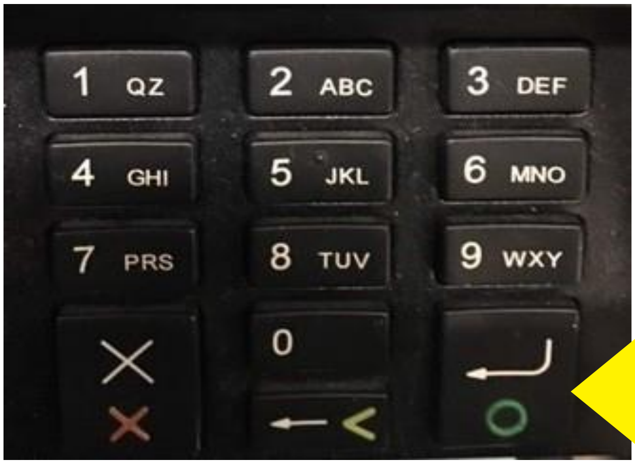
- Attempts by unknown persons to unplug or pry open devices
- Unknown persons loitering at unopened registers
- Multiple transactions (chip cards) that require swipe on same PIN pad

WHAT TO LOOK FOR

Check to make sure the keypad is not raised from the rest of the PIN pad, as this could be a sign of an overlay.



Check to make sure the keypad is different material. The keypad should feel like hard plastic and have the pin pad keypad cover installed.

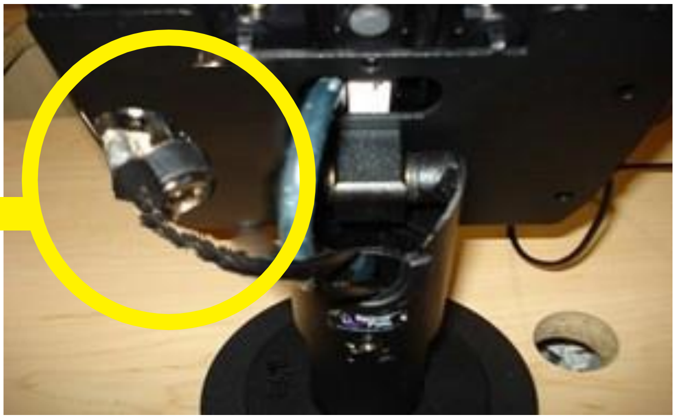


Check that the colors of the Cancel (X), Back (<), and Accept (O) buttons are red, yellow, and green respectively.

TJX U.S. | T.J.maxx Marshalls HomeGoods SIERRA HOMESENSE

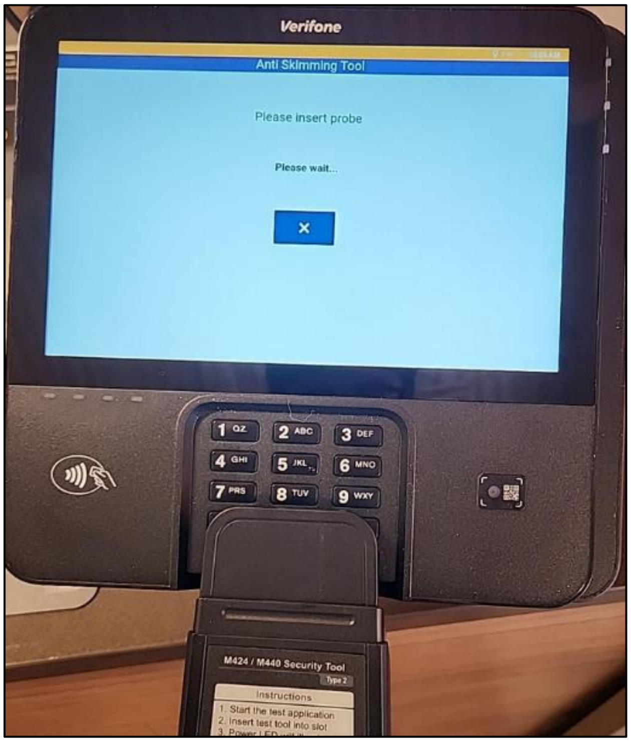
PIN PAD PROTECTION

WHAT TO LOOK FOR



Frayed tether and tampered lock

Look for other signs of tampering such as pry marks



Utilizing the Verifone Anti-Simmer device, ensure that nothing is blocking the chip reader. Red, alerts that the pin pad card reader has been tampered with

PIN PAD PROTECTION

TAKE ACTION

Report any suspicious behavior and indications of PIN pad tampering or substitution to a Manager or a Coordinator immediately!

Daily Pin Pad Protection Survey Questions (in Reflexis and ThinkTime).

Please completely and accurately respond to these questions.

- If for some reason you have answered "No" to questions 1-5 please notify your DM and DLPM and call the Systems Service Desk.
- If for some reason you have answered "Yes" to question 7 please reach out to the SOC@tjx.com, while copying (cc) your DM and DLPM immediately.

1. Are all Pin Pads free of any signs of tampering – i.e. any overlay on the keypad, unusual extension or thickness over card opening, any appearance of adhesive or pry marks?
2. While using the Anti-Skimmer device on ALL Pin Pads, are you able to insert the tool all the way?
3. The screen will display either "no overlay detected" with green light on skimmer or "overlay detected" with red light on skimmer.
4. Are the security brackets, cables, and tethers attached, locked and undamaged?
5. Is the Pin Pad key secured in the key lock box in the safe?
6. If you answered "NO" to any of the above questions, did you immediately suspend the use of that register(s) and notify your DM and DLPM and call the Systems Service Desk?
7. Was a Credit Card Skimmer found on a PIN Pad, a register stolen, or any non-physical tampering found to have occurred?