



Precautionary Steps to Avoid Verifone Pin Pad Failures

Over the last few weeks there has been a significant spike in failures of Verifone MX915 Pin Pads in the stores. The majority of the failures are associated with a "Tamper Detect" error.

What is a "Tamper Detect" error?

The Pin Pads have a security feature that is designed to disable the device if it senses anything that might indicate someone is tampering with it. The purpose is to prevent someone from trying to steal the device or manipulate the Chip Card Reader for criminal purposes.

What causes a "Tamper Detect" error?

Normally, the error is caused by someone trying to remove the device from the bracket or someone inserting a foreign object into the Card Reader. However, the recent spike in these errors might be evidence of something else.

- 1) With increased business the Pin Pad is having a greater number of transactions than normal.
- 2) In an effort to take care of your guests your team is doing everything possible to process transactions as quickly as possible.
- 3) In an effort to do everything possible to avoid spreading Covid-19, the Pin Pads might be cleaned more often than normal.

What happens when the a "Tamper Detect" error occurs?

Unfortunately, if the device senses anything it considers to be tampering, it shuts itself down making it inoperable. The device has to be sent to Verifone to have the error cleared and the device re-loaded.

Important Recommendations

Please advise your team members that the Verifone Pin Pads have a security feature that disables the device if it senses anything it interprets as being tampering.

Make sure all team members are aware that cleaning/disinfecting the Pin Pads requires a very delicate approach. First, if using a cleaning/disinfecting liquid, spray it on to a soft cloth or microfiber towel. Never spray liquid directly onto the Pin Pad. It is very important to gently brush the cloth over the Pin Pad. Aggressively rubbing the Pin Pad might activate the "Tamper Detect" error.