Payment Terminal Check Guide

(Physical Inspection Checklist)

MONEK Limited

Sterling House, City Wharf, Davidson Road,

Lichfield, England, WS14 9DZ

T: +44 (0) 345 269 6645

W: www.monek.com

Chip & Pin Device Checks

1. Serial numbers

All devices will have one or more unique serial numbers that identify it.

Do the serial numbers on the actual device you are using match the serial numbers that were recorded when the device was first issued?

If there is a base station – do the serial numbers match the numbers recorded when the device was first issued. Does the base station match the device it is being used with?

If there is a discrepancy notify your customer representative and don't use the device for payments until resolved.

2. Device stickers or labels

Are any labels lifting? Are any labels not aligned properly or look like they have been stuck down or tampered with?

Pay particular attention to any labels with asset numbers, terminal identification numbers (TID) or serial numbers.

If there is damage or labels lifting find out why – it could be wear and tear. Or it could be someone has tried to swap the labels between devices.

If in doubt, notify your customer representative and don't use the device for payments until resolved.

3. Physical damage

Is there any damage to the device, such as cracks to the casing, screws missing, plastic damaged?

Is this damage caused by dropping the device (you should be able to confirm that), or could the damage have been caused by someone trying to open or tamper with the device.

In the example picture, we're checking if there is damage to the plastic around a screw, suggesting tampering

If in doubt, notify your customer representative and don't use the device for payments until resolved.

4. Damage to screws or fastenings.

Physical damage to the screws or fastening that secures the casing of the device, would indicate that someone has attempted to, or actually has managed to open the device.

Look for marks on the screws/fastening for damage.

Chipped paint where screws/fastenings are painted is another indicator of attempted or successful tampering. (In the example picture, there is damage to the actual screw head during an attempt to open it.)

If in doubt, notify your customer representative and don't use the device for payments until resolved.

5. Cables – damaged or changed.

The device may be directly connected to a phone socket, network socket or EPOS. The supplied cables will vary from model to model and will get damaged from natural use.

Has a cable been damaged or had an apparent repair? An old cable suddenly been replaced? A curly cable replaced by a straight cable or vice versa?

Also check the connection where the cable connects to – has that been changed or damaged?

If in doubt, notify your customer representative and don't use the device for payments until resolved.

6. Display – Is the display operating as expected?

A change in the display of the device may be due to an upgrade, or it could indicate that the device has been changed.

Is the display showing the same content as the last time it was used?

Are amounts being displayed correctly and in the right currency?

Are the instructions that are displayed during the operation of the device consistent or has something changed?

If in doubt, notify your customer representative and don't use the device for payments until resolved.

7. Card Reader – Does it look ok?

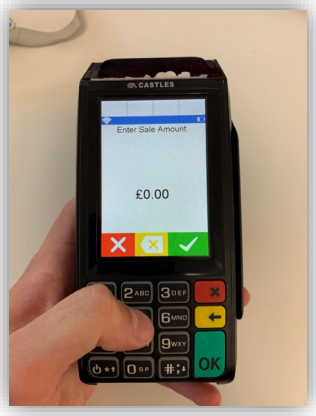
It is possible to use a skimmer that goes in the card reader slot. Is there any reason to be suspicious of the place you enter the card?

If in doubt, notify your customer representative and don't use the device for payments until resolved.

8. Card Reader – are the cards inserting correctly?

If the card either goes in too far or not enough, it is possible the terminal has been tampered with or a skimmer of some sort is present.

If in doubt, notify your customer representative and don't use the device for payments until resolved.



9. Operation - is it running as expected?

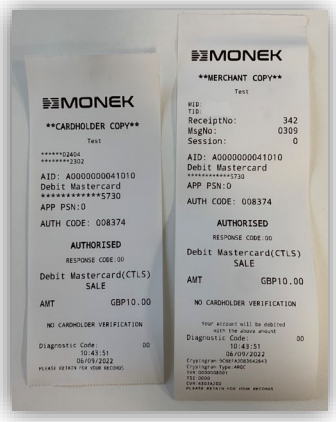
During the process of taking a payment.

Is the device connecting correctly to the service responsible for initializing the payment process?

Has the WiFi name changed? Is it one you recognize, is it connect to WiFi when it should be a wired connection?

Is it prompting for extra information, asking for an additional operator code or an unexpected key press by the operator before taking the payment?

Is the actual duration of taking a payment taking longer than is the normal? If in doubt, notify your customer representative and don't use the device for payments until resolved.

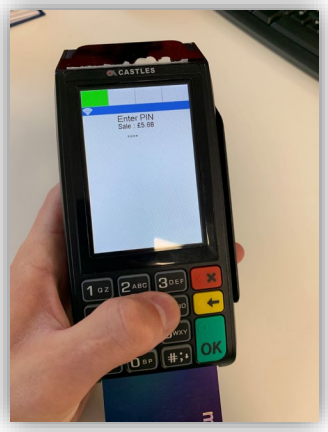


10. Receipts - have they changed?

Check for masking of Primary Account Number (PAN) on the merchant receipt (if applied).

- Is the merchant number on the receipt correct?
- Is the outlet name/institution name correct?
- Is the correct date/time appearing on the receipt?

If in doubt, notify your customer representative and don't use the device for payments until resolved.



11. Everything looks fine

Having checked the device before starting the payment and observing the device closely through the first few payments, checking the receipts produced and screen display. Does the device appear to be operating correctly?

At this point there should be no issues and you can begin to take payments.

Should something change or you have reason to suspect the device isn't operating correctly or has been tampered with, notify your customer representative and don't use the device for payments until resolved.

Tips to protect yourself from fraud.

1. **Regularly update software:** Ensure that your card payment machine's software is up to date with the latest security patches and firmware updates. These updates often include security enhancements that address known vulnerabilities.

2. **Implement PCI DSS compliance:** The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to protect cardholder data. Adhering to PCI DSS requirements helps ensure that your card payment machine and systems are secure.

3. **Protect the physical integrity** of your card payment machine by securing it in a locked location or using security cables to prevent theft or unauthorized removal. Restrict access to authorized personnel only.

4. **Train employees:** Educate your staff on card payment machine security and fraud prevention measures. Teach them to identify and report any suspicious activities, such as tampering with the machine, unusual error messages, or unfamiliar devices connected to the machine.

5. **Regularly inspect machines:** Routinely check your card payment machines for signs of tampering or skimming devices. Look for loose or mismatched parts, unusual wiring, or any modifications that may indicate tampering. If you suspect any tampering, immediately contact your payment processor or acquirer.

6. **Monitor transactions:** Regularly review transaction records and reports to identify any irregularities or suspicious patterns. Implement real-time transaction monitoring systems that can detect anomalies and notify you of potential fraud.

7. **Secure network connections:** If your card payment machine connects to the internet or a local network, ensure that the connection is secure. Use strong passwords for Wi-Fi networks and routers, and consider encrypting the data transmission between the machine and your network.

8. **Verify transactions:** Train your employees to verify the cardholder's identity when accepting payments, especially for high-value transactions. Check the card's security features, compare signatures, or request additional identification if necessary.

9. **Report suspicions promptly:** If you suspect fraudulent activity or encounter any issues with your card payment machine, report it immediately to your payment processor, acquirer, or local law enforcement. Prompt reporting can help prevent further fraudulent transactions.

By implementing these fraud prevention tips, businesses can enhance the security of their card payment machines and protect themselves and their customers from potential fraud or data breaches.

Contact Details

If you have any questions regarding the set-up or you have any issues with this device, please contact Monek via the details below.

Customer support:

Telephone: +44 0345 269 6645 (option 1)

Email: support@monek.com