

PED Check Guide

Physical Inspection Checklist

Support | Achieve | Maintain

PCI DSS
SIG



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 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, 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 they have been stuck down or tampered with?

Pay particular attention to any labels with asset numbers, TID numbers 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 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 (you should be able to confirm that), or is the damage been caused by someone trying to open or tamper with the device.

In the example picture, there is damage to the plastic around a screw, suggesting tampering

If in doubt don't use the device for payments until resolved.



4. Damage to screws or fastenings.

Physical damage to the screw or fastening that secures the casing of the device, would indicated 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 don't use the device for payments until resolved.



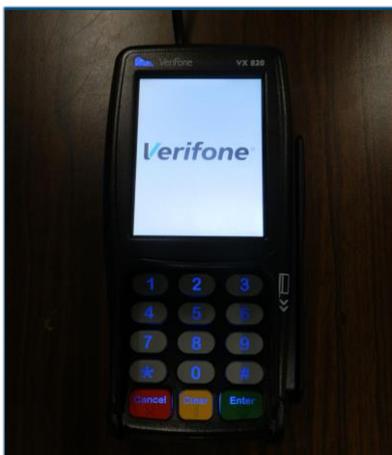
5. Cables – damaged or changed.

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 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?

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

If in doubt do not use for payment until the doubts have been 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?

In the wire indicates some sort of tampering has taken place.

If in doubt do not use for payment until the doubts have been resolved.



8. Card Reader – are the cards inserting correctly?

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

In the example the PED on the left has a skimmer fitted, and the card goes in further than normal. The one on the right is untampered.

If in doubt do not use for payment until the doubts have been resolved.



9. Operation - is it running as expected?

During the process of taking a payment.

Is the device connecting correctly to service for taking initialising the payment process?

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 the taking a payment taking longer than is the normal?

If in doubt do not use for payment until the doubts have been resolved.



10. Receipts - have they changed?

Check for Masking of PAN on the merchant Receipt (if applied). The Customer receipt is the PAN masked?

- Is the Merchant no on the receipt correct?
- Is the Outlet name/institution name is it correct?
- Is the correct date/time on appearing on the receipt?

If in doubt do not use the device for further payments until the doubts have been 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 hopefully yes.

Should something change or you have reason to suspect the device isn't operating correctly or has been tampered with, contact your PCI DSS team immediately for further support.