Stripe Terminal

P2PE Instruction Manual (PIM)

V2.2

September 2025

1. P2PE Solution Information and P2PE Solution Provider Contact Information

1.1 P2PE Solution Information *(as per the listing on the PCI SSC website)*	
P2PE Solution Name:	*Stripe Terminal P2PE*
P2PE Solution Listing Reference Number (***Assigned by PCI SSC***)	*#: 2025-01212.002*
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	

1.2 P2PE Solution Provider Contact Information					
Company Name:	*Stripe, Inc*		Company URL:	*https://stripe.com/*	
Contact Name:	*Vignesh Karthikeyan*		Title:	*Program Manager*	
Telephone:	*(888) 963-8955*		E-mail:	*pci-contact@stripe.com*	
Business Address:	*354 Oyster Point Blvd*		City:	*South San Francisco*	
State/Province:	*CA*	Country :	*United States*	Postal Code:	*94080*

1.3 Communication Instructions
Instructions advising how to contact the P2PE Solution Provider, with consideration to establishing a trusted communication channel/session.
For any questions regarding this P2PE solution, you can connect with the Stripe Support team via 'Stripe Support' (https://support.stripe.com/contact/login) or by opening a support ticket via Stripe Dashboard ((https://dashboard.stripe.com/login).

PCI P2PE and PCI DSS

Merchants using this P2PE Solution may be required to validate PCI DSS compliance. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

Refer to FAQ 1158 on the PCI SSC Website.

2. PTS POI Device and Software Information

2.1 PTS POI Device Details

The following information lists the details of the PTS POI devices approved for use in this P2PE Solution.

All PTS POI device information can be verified by visiting the following on the PCI SSC Website and by referring to Table 2.4 below:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

For P2PE Applications and Non-Payment Software, use the PIM ID#s to cross reference to their respective tables below. The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the P2PE Applications and Non-payment Software that are used on the PTS POI devices denoted here. The 'PIM ID#'s are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

PCI PTS Approval #	PTS POI Device Vendor	PTS POI Device Model Name & Number(s)	PTS POI Device Hardware Version #(s)	PTS POI Device Firmware Version #(s)	P2PE Applications on PTS POI Devices *(PIM ID# from Table 2.2)*	Non-Payment Software on PTS POI Devices *(PIM ID# from Table 2.3)*
4-90102	*BBPOS*	*WisePOS E*	*WSC50xxx-xx-xxx*	*WSC50.xxxx-xxx-xxxx*	*N/A*	*SW1, SW2*
4-30378	*BBPOS*	*WisePAD3*	*WPC30xxx-xx-xxx*	*WPC30.xxx-xx*	*N/A*	*N/A*
4-30457	*Stripe*	*Stripe Reader M2*	*STRM2-0x*	*CHB3x.01.xxxxx*	*N/A*	*N/A*
4-30512	*Stripe*	*S700*	*STR&xxx-11-xxx*	*STR7X-11-XXXXX-XXXX*	*N/A*	*SW1, SW2*
4-30467	*BBPOS*	*S2001 (Shopify Go)*	*S2001A1-XXX*	*WTH11.XXXX-XXX-XXXX*	*N/A*	*SW1, SW2*

2.2 P2PE Application Details

The following information lists the P2PE Applications approved for use on the PTS POI devices in Table 2.1 for use in this P2PE Solution.

P2PE Applications by definition have access to clear-text account data. These applications **must** be denoted in the P2PE Solution listing.

The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the P2PE Applications denoted here that are used on the PTS POI devices denoted in Table 2.1. They are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

***Note**: P2PE Applications that have been assessed as part of the P2PE Solution and were chosen to not be separately listed are denoted as such as part of the P2PE Solution listing and will not have an independent PCI P2PE Application Listing Reference Number.*

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

PIM ID# (e.g., App#1, App#2, …)	P2PE Application Vendor	P2PE Application Name	P2PE Application Version(s)	PCI P2PE Application Listing Reference Number *(Assigned by PCI SSC)*
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

2.3 Non-Payment Software Details

The following information lists the Non-Payment Software approved for use on the PTS POI devices in Table 2.1 for use in this P2PE solution.

*P2PE Non-payment Software by definition **must not** have any access to clear-text account data. While this type of software is assessed as part of the P2PE Solution assessment, this software is not denoted on the PCI P2PE Solution Listing.*

The 'PIM ID#'s are numbers created and used by the P2PE Solution Provider solely for the purpose within this PIM to make it easier to cross reference the Non-payment Software denoted here that is used on the PTS POI devices denoted in Table 2.1. They are not assigned by the PCI SSC nor are they recognized by the PCI P2PE Program.

PIM ID# (e.g., SW#1, SW#2, …)	Non-payment Software Vendor	Non-payment Software Name	Non-payment Software Version(s)	Additional Information *(as needed)*
SW1	*Stripe*	*Stripe-Reader*	2.29.6.0	
SW2	*Stripe*	*Stripe-Updater*	2.29.6.0	

2.4 Verifying PTS POI Device Information

Verifying PTS POI device information is critical. This information is necessary to validate the information in this PIM, to cross-reference with the PCI PTS Listings as well as the PCI P2PE Solution Listing, in addition to inventory management, troubleshooting and incident reporting.

Instructions to confirm PTS POI device hardware, firmware, and the P2PE Application(s) and Non-payment Software present

WisePad 3

To check the hardware, firmware and any applications running on your device you should:

1. *Note the details from the label on the back of the device.*
2. *Press the menu button on the device and scroll using the up and down arrows:*
3. *This will cause the following to be displayed:*
    a. *Bootloader Version*
    b. *Hardware Version*
    c. *Firmware Version*
4. *These should match those on the label unless the device has undergone a firmware update since it was first deployed.*

Wise POS E

To check the hardware, firmware and any applications running on your device you should:
Note the details from the label on the back of the device.

To check the running firmware and configuration swipe in from the left edge of the screen and when the diagnostics menu is displayed tap ‘Settings’ and enter the admin code 07139.

The numbers displayed here should match that shown on the label unless the device has undergone a firmware update since it was first deployed.

Stripe Reader M2

To check the hardware, firmware and any application running on your device you should:

1. *Note the details from the label on the back of the device.*
2. *To check the running hardware and firmware versions, go to the host device and send the ‘Get device Info’ command to the reader via the Bluetooth or USB connection:*
3. *The information returned should match the hardware version shown on the label and the firmware should match that shown in the PTS approval for the device. This is available on the PCI SSC website:* *https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true for PTS approval number 4-30457*

S700

To check the hardware, firmware and any applications running on your device you should:

1. *Note the details from the label on the back of the device.*
2. *To check the running firmware and configuration swipe in from the left edge of the screen and when the diagnostics menu is displayed tap ‘Settings’ and enter the admin code 07139.*
3. *The numbers displayed here should match that shown on the label*

Shopify POS Go (S2001)

To check the hardware, firmware and any applications running on your device you should:

1. *Note the details from the label on the back of the device.*
2. *To check the running firmware and configuration swipe in from the left edge of the screen and when the diagnostics menu is displayed tap ‘Settings’ and enter the admin code 07139.*
3. *The numbers displayed here should match that shown on the label unless the device has undergone a firmware update since it was first deployed.*

2.5 PTS POI Device Inventory & Monitoring

- All PTS POI devices must be documented via inventory control and monitoring procedures, including device status (e.g., deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted PTS POI devices, must be reported to the P2PE Solution Provider via the contact information and instructions in Section 1 above.
- A sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Instructions on documenting and maintaining an inventory of the PTS POI Devices.

The merchant should keep a detailed inventory of the P2PE POI devices at the merchant’s location(s). Where multiple locations are involved either a separate inventory per location should be used, or if it is a combined inventory a mechanism should be in place to ensure logical groups of devices can be reported on. For example: separate tabs in an Excel Spreadsheet and then filtering on columns such that groups of devices by their status can be ascertained easily.

The inventory of devices should include at a minimum the type of information shown in the sample table below. That is:

- *Device Vendor – visible on the device label on back of the device*
- *Device Model – visible on the device label on back of the device*
- *Device Location – the store/shop where the device is present and additionally, as applicable, used to indicate where a device is stored, or physically where it is deployed with that location.*
- *Device Status – deployed, in-stock, broken, returned, destroyed.*

- *Device Serial Number – visible on the device label on back of the device*

The inventory should be updated when new devices are received and when devices change status. The inventory should also have a date control showing when updates were made and when an inventory review took place. Although a device inventory check is only required annually, where the merchant has a sizeable number of devices, Stripe recommend one is performed more frequently, either biannually or quarterly. Any devices found to be missing during an inventory check, or at any time, must be reported via the Stripe Dashboard to Stripe Support (as per section 2.1) immediately. Stripe will then ensure that the missing POI device is deactivated in the P2PE system and cannot be used.

If the merchant does not want to build their own independent inventory, they can use the tools available on the Stripe Dashboard under the merchant account to build their own on-line device inventory. However, whichever method is used the merchant must ensure that it is accurate and checked against the deployed and stored POI devices owned by the merchant.

Sample Inventory Table

PTS POI Device Vendor	PTS POI Device Model Name(s) and Number(s)	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory	Additional Notes (as needed)

3. Receipt of PTS POI Devices

3.1 Instructions for ensuring PTS POI devices originate from trusted sources/sites/locations

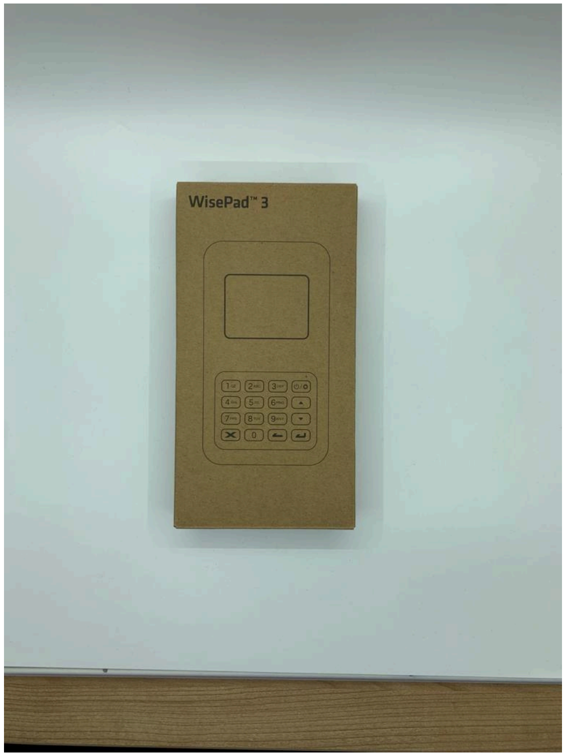
Regardless of whether the POI device(s) were ordered directly by the merchant, or via the Stripe Account Manager, when the devices are dispatched, the email address entered by the ordering party will receive an email with the courier tracking information. It is important that when the package is received the tracking information supplied in the email matches that of the package received.

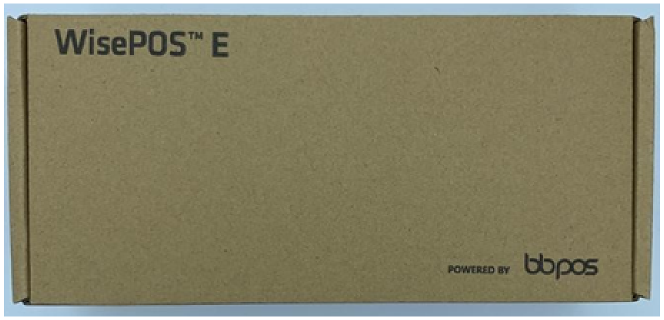
Any problems or discrepancies should be reported to 'Stripe Support' via the Stripe Dashboard (https://dashboard.stripe.com/login) using email, chat or by requesting a call back. The device must not be used until such time as Stripe give the all-clear or replace the device.

3.2 Instructions for confirming PTS POI device and packaging were not tampered with

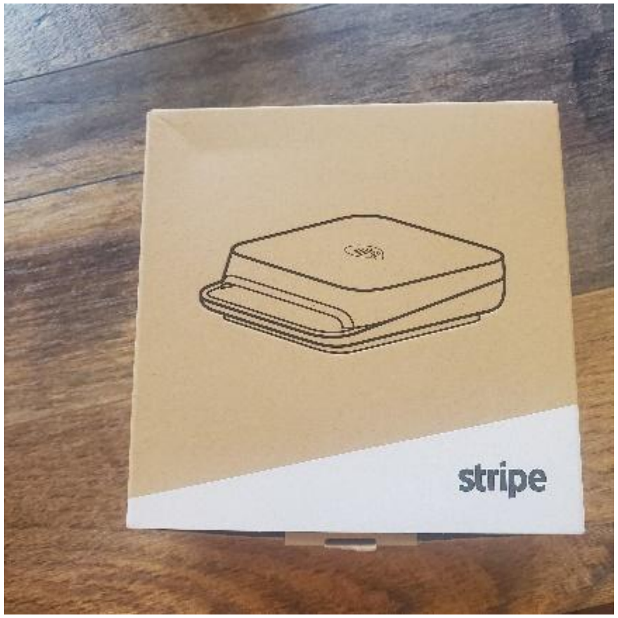
1. *When the package is received and verified as being correct as per 2.1 above, the integrity of the package and its contents should be verified.*
2. *Check the courier packaging shows no sign of damage or of having been opened.*
3. *Check that the device packaging looks as follows:*

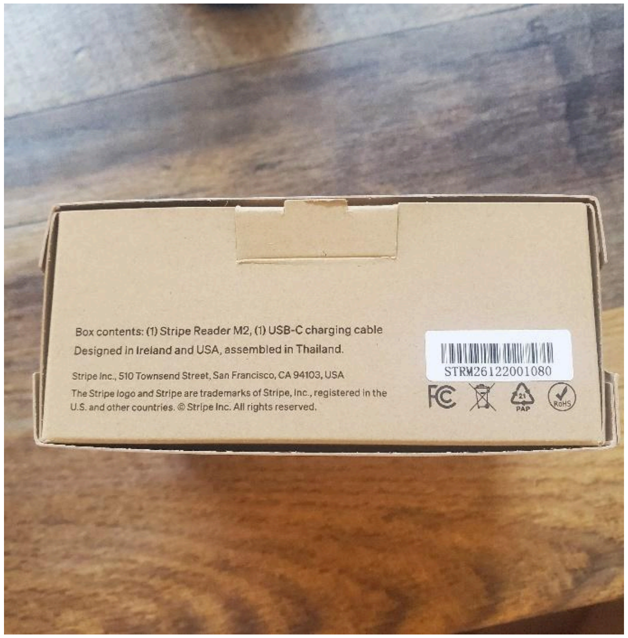
WisePad 3 (left) and WisePOS E (right)



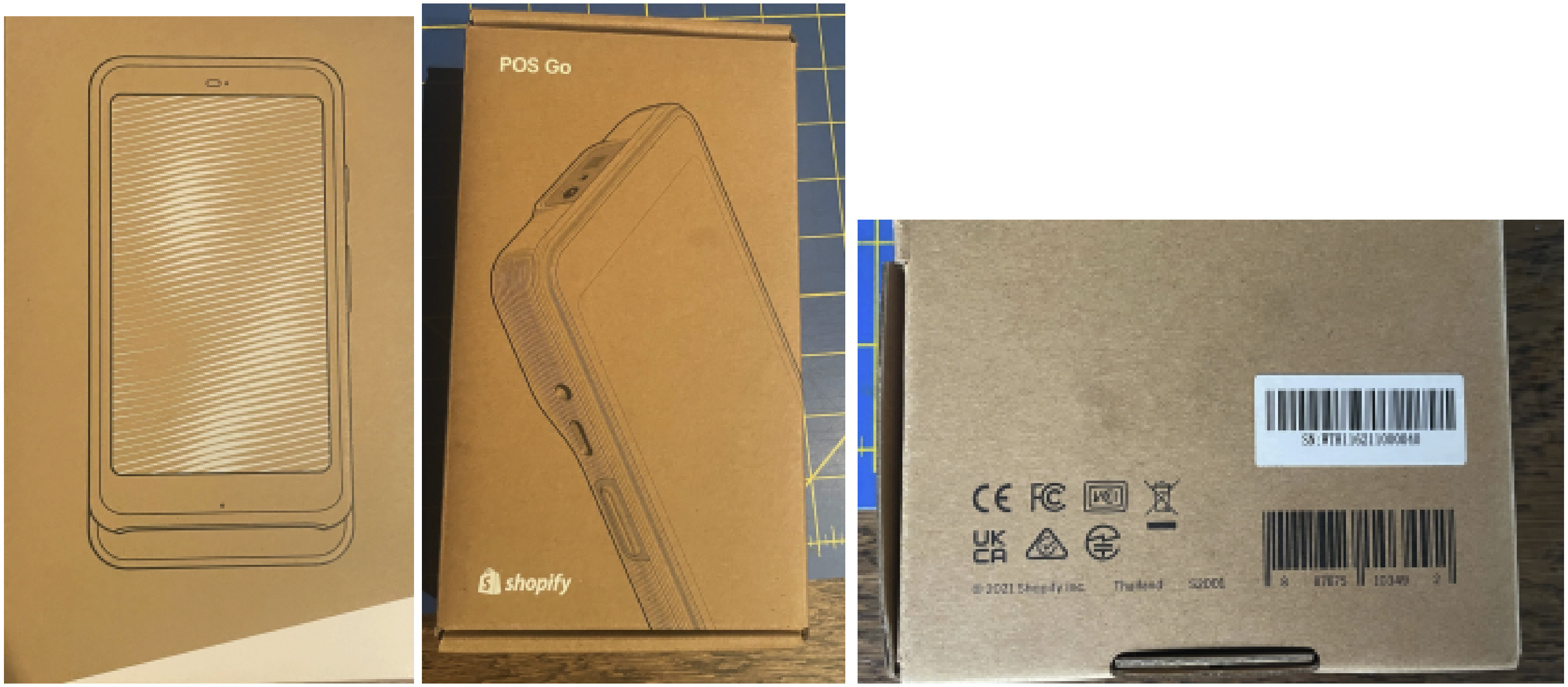


Stripe Reader M2

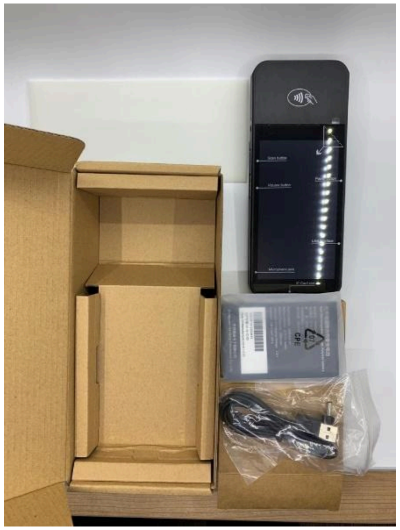



Box contents: (1) Stripe Reader M2, (1) USB-C charging cable
Designed in Ireland and USA, assembled in Thailand.
Stripe Inc., 510 Townsend Street, San Francisco, CA 94103, USA
The Stripe logo and Stripe are trademarks of Stripe, Inc., registered in the U.S. and other countries. © Stripe Inc. All rights reserved.
STRM26122001080
21
PAP
RoHS

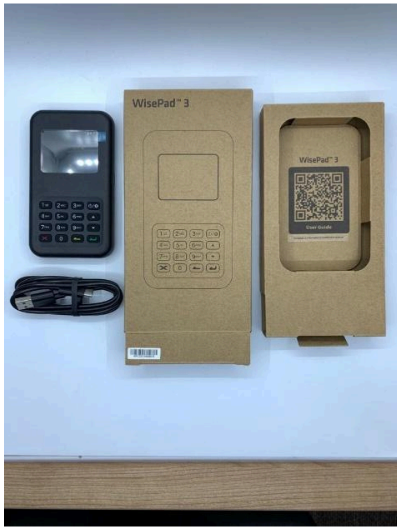
S700, S2001 (Shopify Go)



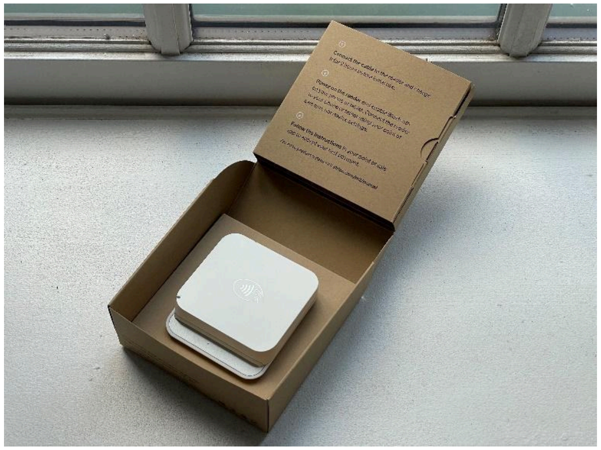
4. Open the package and check the integrity of the device.
   - Does it match the device that was ordered?
   - Are all cables and attachments present in the box?
   - Are there any unexpected attachments, e.g. plugs, cables, wires, inserts, overlays, etc.?
   - Are there any signs of damage or tampering? Is the device intact, are there any missing or loose screws, are there any cracks or holes, are labels intact and not torn, etc.?



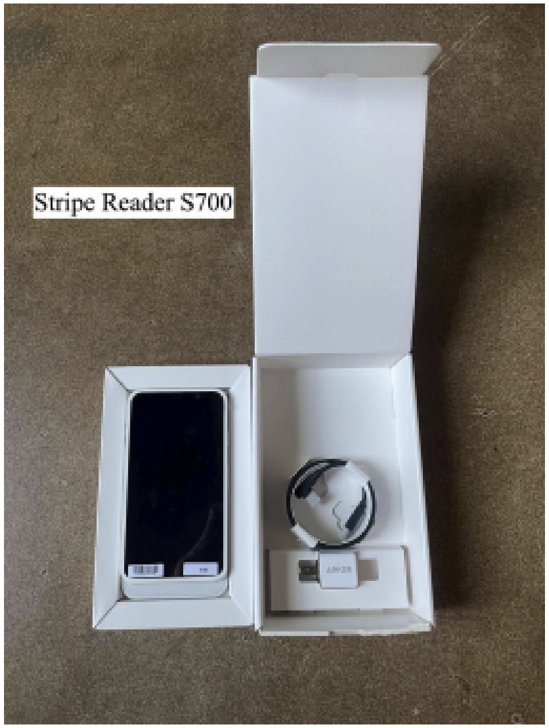
(Wise POS E)

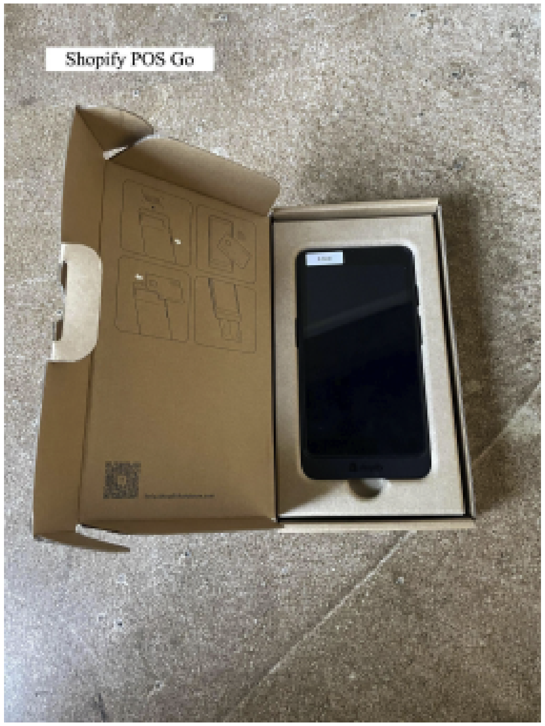


(WisePAD 3)



(Stripe Reader M2)





If any of the above checks fail then the merchant should not use the device and should notify Stripe Support immediately (as per details in section 2.1).

3.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be delivery, support, and/or repair personnel, prior to granting those personnel access to PTS POI devices.

Merchants should be aware that Stripe will not send any staff to the merchant's location, be they Stripe employees or third-party engineers, for the purposes of 'fixing' or 'updating' a POI device. Under no circumstances should a merchant allow an unknown person to access or manipulate the POI devices.

If there is a need to repair a device Stripe will send the merchant a return shipping label for the device and notify the merchant accordingly. The merchant should not hand over a device without first checking the validity of the person collecting it.

Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting for transport between sites/locations

4. Deployment and Installation of PTS POI Devices

Do not connect or otherwise use non-approved payment account data capture devices.

The P2PE Solution is approved to use specific PTS POI devices, as detailed above in Table 2.1, which must be denoted on the P2PE Solution Listing.

If any devices that are not in Table 2.1 are used to accept payment account data, it could affect the merchant eligibility to use SAQ P2PE – contact your acquirer or payment brands.

Do not change or attempt to change PTS POI device secure configurations or settings.

Changing secure PTS POI device configurations or settings may invalidate the P2PE Solution implementation and it could affect the merchant eligibility to use SAQ P2PE – contact your acquirer or payment brands.

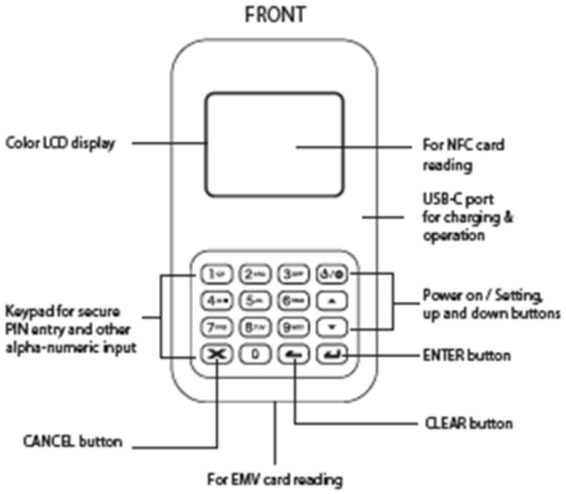
Examples include, but are not limited to attempting to perform the following on the PTS POI devices:

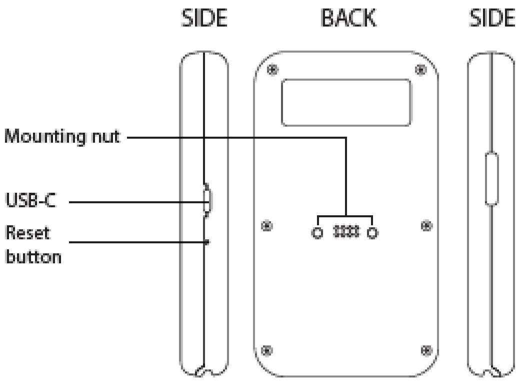
- Enabling any device interfaces or data-capture mechanisms that are disabled
- Altering security configurations or authentication controls
- Physically opening the device
- Attempting to install unauthorized applications/software

4.1 Installation and connection instructions for the PTS POI devices

WisePAD3

The device is designed for handheld walkabout type environments in mobile-host mode. That is it connects remotely via Bluetooth to a mobile-host device such as a tablet or smartphone. However, it can also be used via a USB connection directly to the mobile-host device.


FRONT
Color LCD display
For NFC card reading
USB-C port for charging & operation
Keypad for secure PIN entry and other alpha-numeric input
Power on / Setting, up and down buttons
ENTER button
CLEAR button
CANCEL button
For EMV card reading



1. *Using the USB cable provided with the device, connect using the USB port on the right-hand side of the device and charge.*

2. *Once charged use the Power On button on the top right-hand corner of the keypad.*

3. *The device will start-up with Bluetooth LE enabled. Do not change this setting, if you do the device will no longer be compliant for use with the Stripe Terminal P2PE Solution.*

4. *If using Bluetooth, pair the device with the mobile-host device.*

5. *If using a direct connection use the USB cable to connect directly to the mobile-host device.*

6. *The device should now be visible to and communicate with the mobile-host device.*

WisePOS E

Is an integrated Android based device and does not require connections to any other device for its operation.

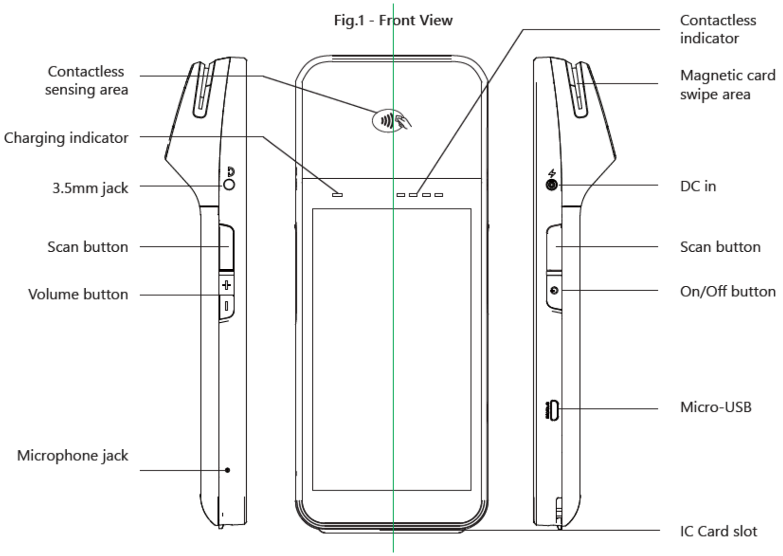
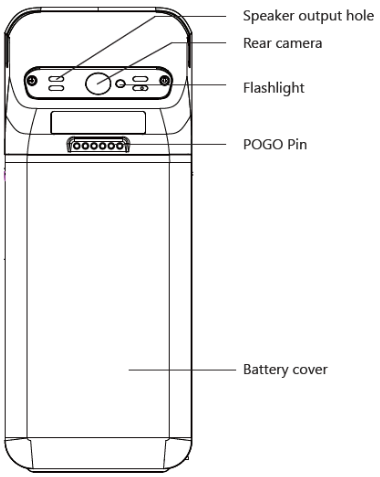
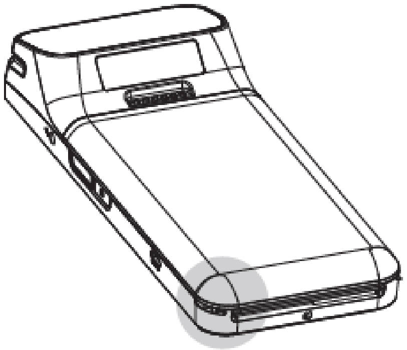


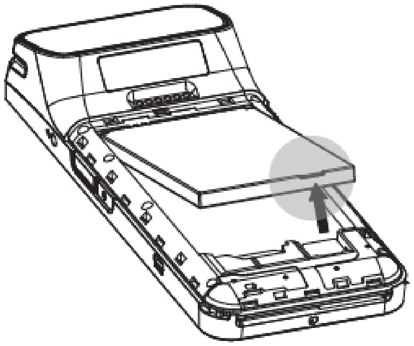
Fig.2 - Rear View



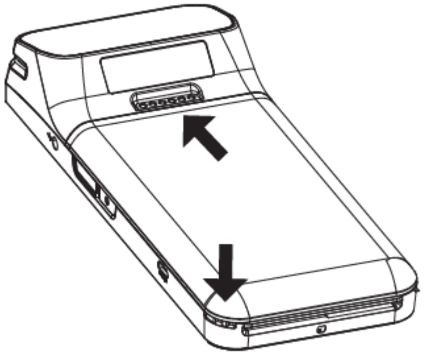
1. *Turn the device on its front and open the battery door from the bottom left-hand corner:*



2. *Once open remove the battery.*



3. *Replace the battery and replace the back cover by pushing up and locking into the bottom left-hand corner.*



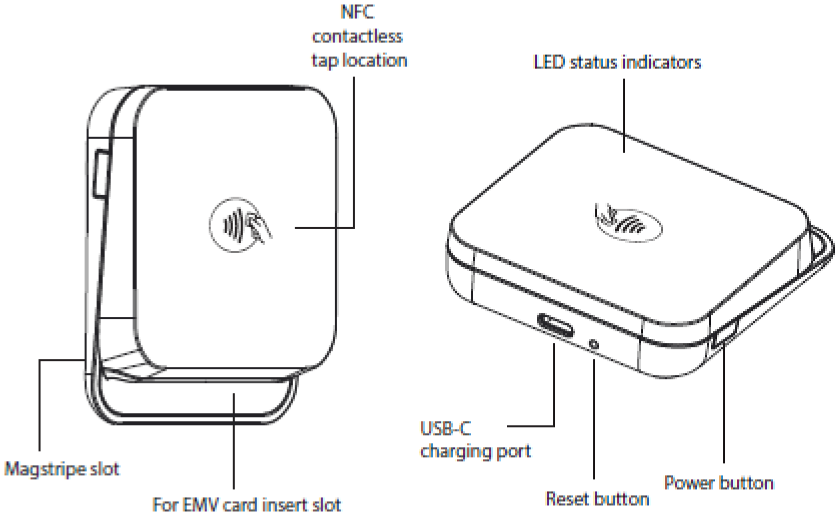
4. *Using the provided USB to DC cable charge the device. The charging indicator on the front of the device will turn green when the battery is fully changed.*

5. *Once charged use the Power On button on the right-hand side of the device to turn the device on. The device is ready for use.*

6. *Tap on the app and follow the instructions.*

Stripe Reader M2

This is a reader device that can be connected to a COTS device (Host Device – phone or tablet) by either Bluetooth or USB to create a secure payment terminal. It should always be used in attended environments.



1. *Take the USB cable from the package and connect to the USB-C charging port. Leave the device to charge for at least 2 hours before initial use or until all 4 green LEDs are lit to indicate fully charged.*

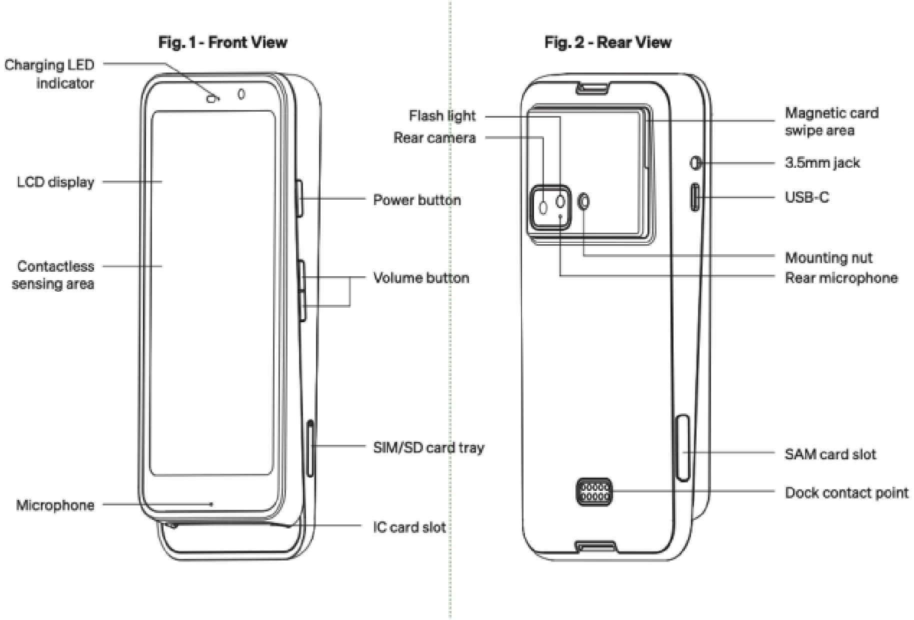
2. *Use the Power Button to turn on the device.*

3. *Enable Bluetooth on the host device (phone or tablet) and start the POS application.*

4. *Through the application connect the reader to the host device. DO NOT USE THE HOST DEVICE SETTINGS.*

S700

Is an integrated Android based device and does not require connections to any other device for its operation.



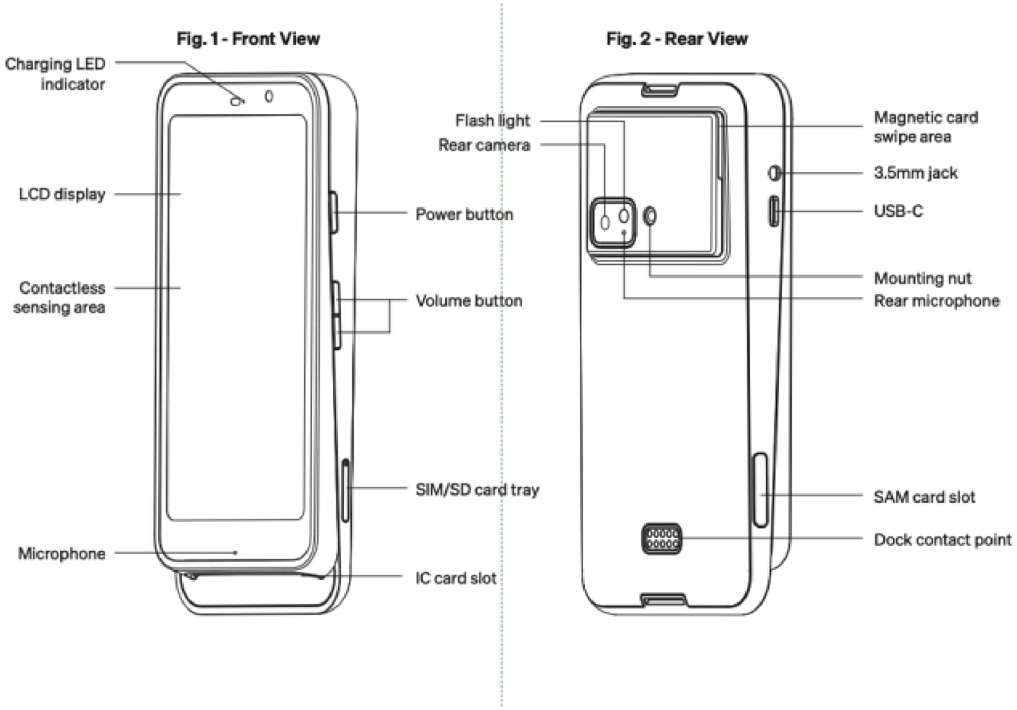
1. *1. Using the provided USB to USB-C cable charge the device. The charging indicator on the front of the device will turn green when the battery is fully changed.*
2. *Once charged use the Power On button on the right-hand side of the device to turn the device on. The device is ready for use.*
3. *Tap on the app and follow the instructions.*

Shopify POS Go (S2001)

Is an integrated Android based device and does not require connections to any other device for its operation.

Fig. 1 - Front View

Fig. 2 - Rear View



1. *Using the provided USB to USB-C cable charge the device. The charging indicator on the front of the device will turn green when the battery is fully changed.*
2. *Once charged use the Power On button on the right-hand side of the device to turn the device on. The device is ready for use.*
3. *Tap on the app and follow the instructions.*

4.2 Guidance for selecting appropriate locations to deploy PTS POI devices

Mounted Devices (WisePad3 option)

These devices should be deployed:

- *In an area that is generally manned and visible to the staff.*
- *In a location and position that is comfortable for both staff and customers to use.*
- *Using a mounting stand that allows for the device to be tilted for ease of use and to provide a level of privacy for PIN entry.*
- *Close to the mobile-host device and a power outlet.*
- *In a location that is well ventilated and in an ambient environment: not close to heat sources, excessive cold, damp or water sources, etc.*
- *Such that customer keyboard entries are not visible to CCTV, via mirrors, or to staff.*
- *Such that staff can easily inspect the device.*

Handheld devices (WisePad3, WisePOS E and Stripe Reader M2, S700, and Shopify POS GO (S2001))

These devices should be deployed as appropriate to the environment in which they will be used taking into account the following guidelines:

- *When in use they should be in the possession of an authorized member of staff.*
- *When not in the physical possession of an authorized member of staff, the device should be kept out of sight. For example, below the counter or in a drawer and in an area where staff gather and is normally manned.*
- *At the end of the day the device should be taken and locked in a cupboard accessible to only authorized staff.*

4.3 Guidance for physically securing deployed PTS POI devices to prevent unauthorized removal and/or substitution

Mounted devices

- *These devices should be securely locked into a cradle or mounting stand using the mounting nuts on the back of the device.*
- *The mounting nuts should not be easily accessible and locked tightly.*
- *Consider using security seals to provide quick visual proof that the mount and/or device has not been tampered with or substituted,*
- *The device location should be covered by CCTV but such that keyboard entries are not visible.*

Handheld Devices

- *These devices should only be available to those that need to use them.*

- *The device should only be used by staff authorized to do so, and when in use the merchant staff member should ensure that the device is under their direct control except for when a customer is entering their PIN.*

  When not in the physical possession of an authorized member of staff, the device should be kept out of sight. For example, below the counter or in a drawer. This should be in an area that is usually manned, or staff gather, such that strangers in the area would be quickly spotted Outside working hours devices should be securely locked in a cupboard or drawer such that only authorized staff have access.

NOTE: All devices should be accounted for at the end of the day. Any missing devices should be reported to Stripe Support as per section 2.1.

5. Continual Monitoring and Inspection of Deployed PTS POI Devices

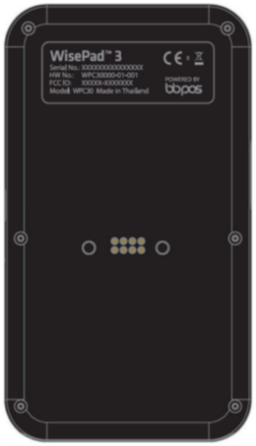
5.1 Instructions for inspecting PTS POI devices for signs of tampering and responding to suspected tamper incidents

When taking delivery of the POI device it should be carefully checked to ensure it has not been subject to substitution of tampering. This checking should be repeated regularly to ensure the ongoing health of the device.

WisePAD3

*At a minimum the **following checks should be made on receipt and where applicable daily** according to the Vendors Security Policy for this device:*

1. *On receipt check the packaging to ensure it shows no signs of damage or forced entry and verify the details against the received tracking and/or invoice information.*
2. *Retrieve the device from the packaging and verify that the label on the back is intact and looks as follows:*



3. *Run your fingers over the label to ensure it is smooth and not hiding any defects.*

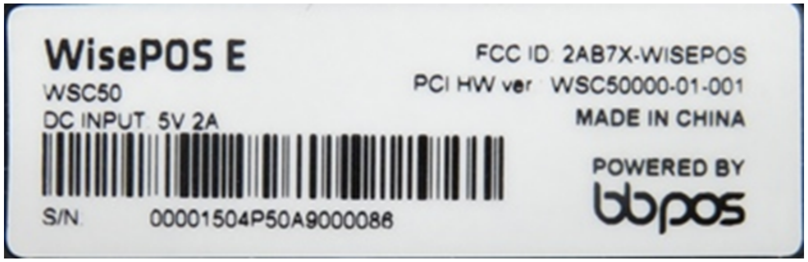
4. Check that there are no other labels on the device, these shouldn’t be there and could be hiding holes drilled in the device.
5. While examining the back of the device check that the screws appear to be intact and in place and there is no sign of scratching on the device surface that might indicate an attempt to open the device or remove the screws.
6. Look carefully around the back of the device for any tiny holes or cracks in the surface.
7. If after all the checks you are satisfied that the device is OK then it can be used – any issues found should be investigated and resolved before the device is considered fit to use,.

If this is the first inspection take photos of the front, back, and card insertion areas and post these in the area where the device will be used to provide staff with a quick and easy reference when doing the regular daily checks.

WisePOS E

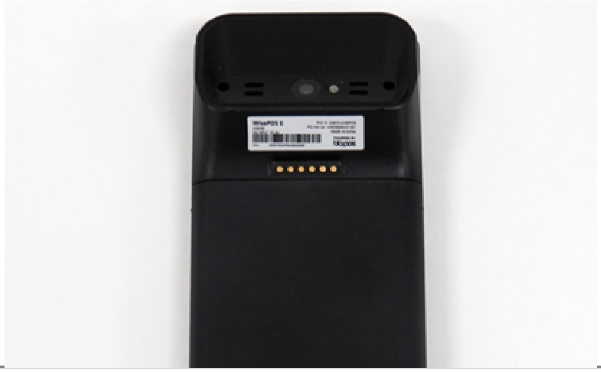
At a minimum the following **checks should be made on receipt and where appropriate daily** according to the Vendors Security Policy for this device:

1. On receipt check the packaging to ensure it shows no signs of damage or forced entry and verify the details against the received tracking and/or invoice information.



2. Retrieve the device from the packaging and verify that the label on the back is intact and looks as follows:

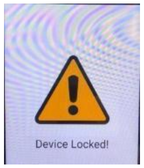
3. Run your fingers over the label to ensure it is smooth and not hiding any defects.



4. *Check that there are no other labels on the device, these shouldn't be there and could be hiding holes drilled in the device.*
5. *While examining the back of the device check that the screws appear to be intact and in place and there is no sign of scratching on the device surface that might indicate an attempt to open the device or remove the screws.*
6. *Look carefully around the back of the device for any tiny holes or cracks in the surface.*
7. *If after all the checks you are satisfied that the device is OK then it is OK to use – and issues found should be investigated and and resolved before the device is considered fit to use,*

If this is the initial inspection, take photos of the front, back and card insertion areas and post these in the area where the device will be used to provide staff with a quick and easy reference when doing the regular daily checks.

NOTE: if the device tamper mechanisms have been triggered you will see this screen:



Device Locked!

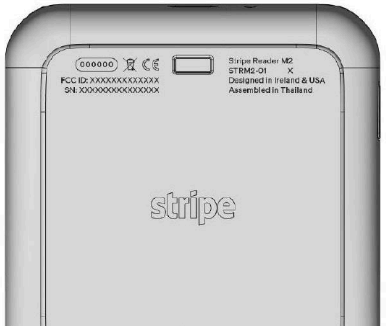
In this case the device will not be operable and should be securely stored in case it is required for forensic analysis.

Stripe Reader M2

At a minimum the following ***checks should be made on receipt and where appropriate daily*** *according to the Vendors Security Policy for this device:*

1. *On receipt check the packaging to ensure it shows no signs of damage or forced entry and verify the details against the received tracking and/or invoice information.*

2. *Retrieve the device from the packaging and verify that the information etched on the back looks as follows:*



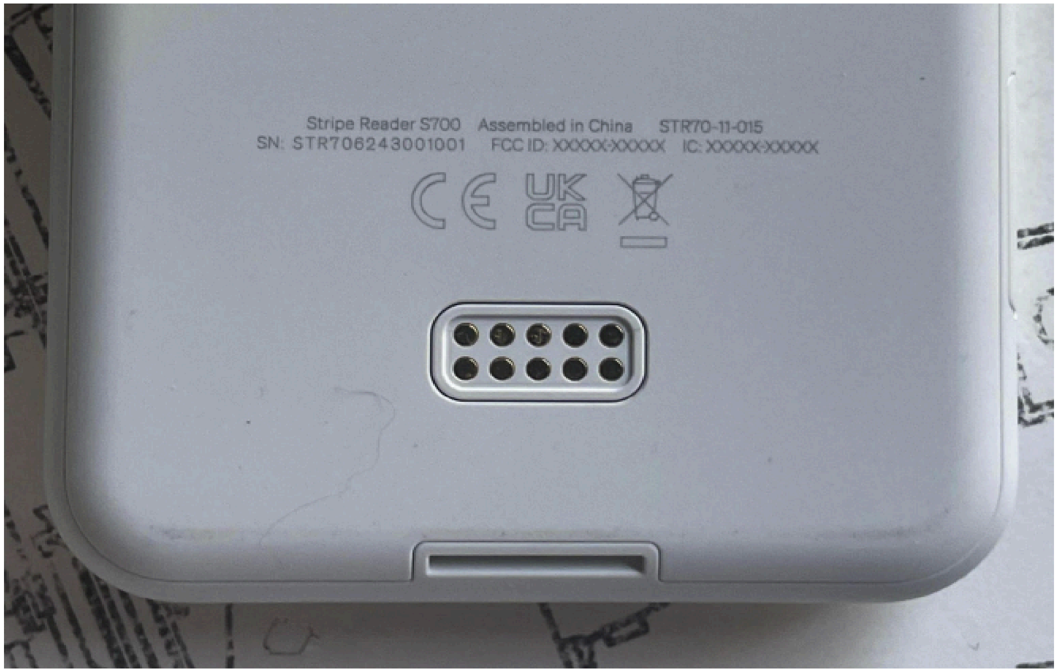
Back of Device

3. *Check that the serial number on the device matches that supplied by Stripe on order and shipping information.*
4. *Check that there are no other labels on the device, these shouldn't be there and could be hiding holes drilled in the device.*
5. *While examining the back of the device check that everything appears to be intact and in place and there is no sign of scratching on the device surface that might indicate an attempt to open the device*
6. *Look carefully around the back of the device for any tiny holes or cracks in the surface.*
7. *If after all the checks you are satisfied that the device is OK then it is OK to use – and issues found should be investigated and and resolved before the device is considered fit to use,*

If this is the initial inspection take photos of the front, back and card insertion areas and post these in the area where the device will be used to provide staff with a quick and easy reference when doing the regular daily checks.

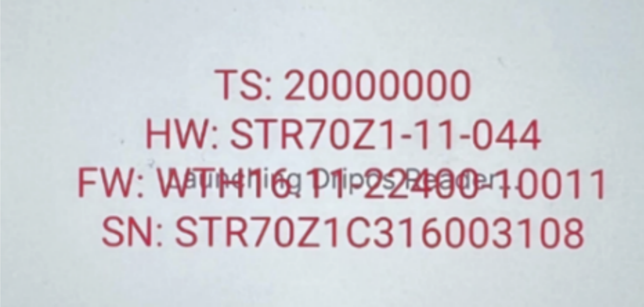
S700

At a minimum the following checks should be made on receipt and where appropriate daily according to the Vendors Security Policy for this device:


Stripe Reader S700 Assembled in China STR70-11-015
SN: STR706243001001 FCC ID: XXXXX-XXXXX IC: XXXXX-XXXXX
CE
UK CA

1. *On receipt check the packaging to ensure it shows no signs of damage or forced entry and verify the details against the received tracking and/or invoice information.*
2. *Run your fingers over the engraving to ensure it is smooth and not hiding any defects.*
3. *Check that there are no labels on the device, these shouldn't be there and could be hiding holes drilled in the device.*
4. *While examining the back of the device check that the screws appear to be intact and in place and there is no sign of scratching on the device surface that might indicate an attempt to open the device or remove the screws.*
5. *Look carefully around the back of the device for any tiny holes or cracks in the surface.*
6. *Turn the device over and check the front:*

If this is the initial inspection take photos of the front, back and card insertion areas and post these in the area where the device will be used to provide staff with a quick and easy reference when doing the regular checks.



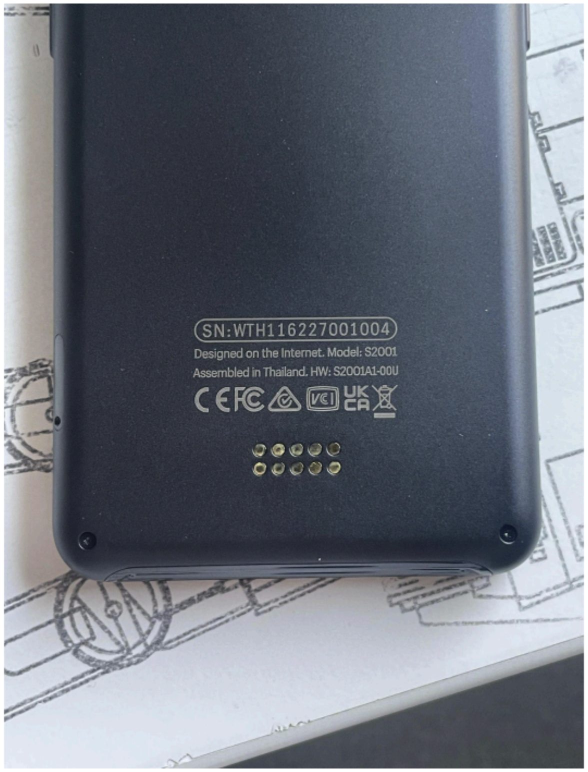
TS: 20000000
HW: STR70Z1-11-044
FW: WTH16.11-22400-10011
Launching DripOS Reader...
SN: STR70Z1C316003108

NOTE: if the device tamper mechanisms have been triggered you will see this screen:

In this case the device will not be operable and should be securely stored in case it is required for forensic analysis.

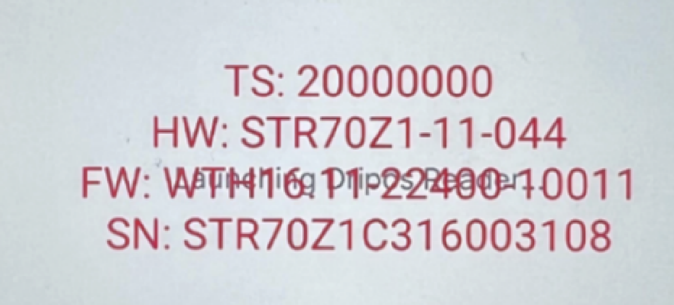
Shopify POS Go (S2001)

At a minimum the following checks should be made on receipt and where appropriate daily according to the Vendors Security Policy for this device:


SN:WTH116227001004
Designed on the Internet. Model: S2001
Assembled in Thailand. HW: S2001A1-00U

1. On receipt check the packaging to ensure it shows no signs of damage or forced entry and verify the details against the received tracking and/or invoice information.
2. Run your fingers over the engraving to ensure it is smooth and not hiding any defects.
3. Check that there are no labels on the device, these shouldn't be there and could be hiding holes drilled in the device.
4. While examining the back of the device check that the screws appear to be intact and in place and there is no sign of scratching on the device surface that might indicate an attempt to open the device or remove the screws.
5. Look carefully around the back of the device for any tiny holes or cracks in the surface
6. If this is the initial inspection, take photos of the front, back and card insertion areas and post these in the area where the device will be used to provide staff with a quick and easy reference when doing the regular daily checks.

NOTE: if the device tamper mechanisms have been triggered you will see this screen:



TS: 20000000
HW: STR70Z1-11-044
FW: WTH16.11-22400-10011
Launching DipOS Reader...
SN: STR70Z1C316003108

In this case the device will not be operable and should be securely stored in case it is required for forensic analysis.

If the merchant detects any signs of tampering or has any suspicions regarding the POI device – either when initially received or once deployed they should not use the device. They should contact Stripe Support immediately (as per section 2.1) :

Be prepared to provide the following information when contacting Stripe:

- *Merchant Name and Location where the device is located.*
- *The type of device: make and model.*
- *Device ID: serial number from the device*
- *Details of what you have found that is making you suspicious.*

Stripe Support will contact the merchant to follow-up and determine the status of the device. If after investigation tampering is still suspected Stripe will send the merchant a replacement device and in the box with that device will be a courier shipping label. The merchant should use this to return the suspect device to the distribution warehouse

5.2 Instructions for inspecting PTS POI devices for skimming devices and responding to suspected skimming detection

Additional guidance for inspecting PTS POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants,* available at https://www.pcisecuritystandards.org/document_library/

*At a minimum the **following checks should be made on receipt and where applicable daily** according to the Vendors Security Policy for this device:*

WisePad3

1 QZ
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PRS
8 TUV
9 WXY
0

1. *Run your fingertips across and around the keypad to see if you can identify an overlay. These are thin, fine sheets that sit over the actual keyboard and can record keyboard activity.*
2. *Run your fingertips across and around the screen to ensure it is solidly in place and shows no sign of having been tampered with.*
3. *Look for any signs of small holes or cracks on the front surface of the device.*
4. *Turn the device flat, keyboard up and towards you, and examine the card insertion area at the bottom of the device. Make sure there are no 'wires' or anything else that would indicate that a skimmer has been inserted. Also look for cracks, holes, scratches, or other signs of damage in that area.*
5. *Check the sides of the device by looking closely for holes, scratches, and other damage. Use your fingertips to feel for possible changes in the surface.*
6. *If after all the checks you are satisfied that the device is OK then it can be used – any issues found should be investigated and resolved before the device is considered fit to use.*

WisePos E

1. *Turn the device to the front side*
2. *Run your fingertips across and around the surface of the device to see if you can identify any uneven surfaces, small holes or cracks.*
3. *Turn the device flat, front up and bottom of the device towards you, and examine the card insertion area at the bottom on the device. Make sure there are no 'wires' or anything else that would indicate that a skimmer has been inserted. Also look for cracks, holes, scratches, or other signs of damage in that area.*
4. *Turn the device so you can see the card reader at the top of the device. Examine that area for wires, inserts, etc. Along with any damage such as scratches or chips that could indicate that there has been an attempt to modify and tamper with the device.*
5. *Inspect the sides of the device and ensure that there are no signs of unexpected attachments, scratches, small drill holes, etc. that would indicate an attempt to modify or tamper with the device.*
6. *If after all the checks you are satisfied that the device is OK then it is OK to use – and issues found should be investigated and and resolved before the device is considered fit to use,*

Stripe Reader M2

1. *Turn the device to the front side*
2. *The surface should be clean and clear and there should be no sign of scratches, tiny holes, or any other damage.*
3. *Holding the device turn it flat so that you can clearly see the card insert and card swipe areas at the bottom of the device,*

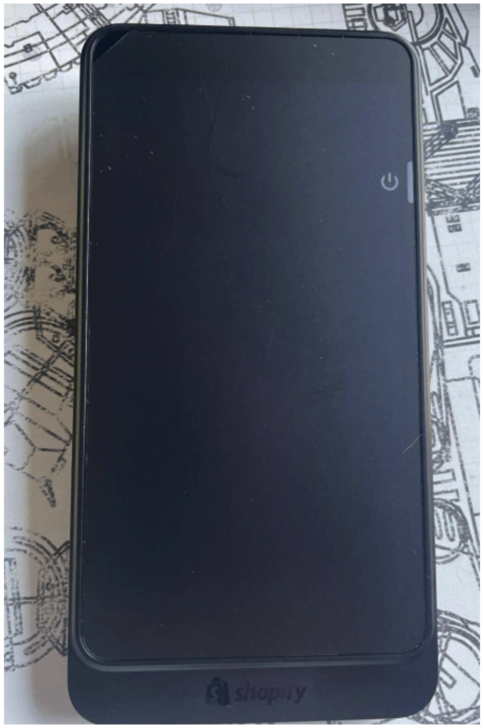
4. *Check for any signs of scratching, tiny holes, or other damage, and for any wires or skimming type devices.*
5. *If after all the checks you are satisfied that the device is OK then it is OK to use – and issues found should be investigated and and resolved before the device is considered fit to use,*

S700

1. *Run your fingertips across and around the surface of the device to see if you can identify any uneven surfaces, small holes or cracks.*
2. *Turn the device flat, front up and bottom of the device towards you, and examine the card insertion area at the bottom of the device. Make sure there are no ‘wires’ or anything else that would indicate that a skimmer has been inserted. Also look for cracks, holes, scratches, or other signs of damage in that area.*
3. *Turn the device so you can see the card reader at the top of the device. Examine that area for wires, inserts, etc. Along with any damage such as scratches or chips that could indicate that there has been an attempt to modify the device.*

4. *Inspect the sides of the device and ensure that there are no signs of unexpected attachments,*
5. *scratches, small drill holes, etc. that would indicate an attempt to modify or tamper with the device.*
6. *If after all the checks you are satisfied that the device is OK then it is OK to use – and issues found should be investigated and and resolved before the device is considered fit to use,*

Shopify POS Go (S2001)



1. Run your fingertips across and around the surface of the device to see if you can identify any uneven surfaces, small holes or cracks.
2. Turn the device flat, front up and bottom of the device towards you, and examine the card insertion area at the bottom on the device. Make sure there are no 'wires' or anything else that would indicate that a skimmer has been inserted. Also look for cracks, holes, scratches, or other signs of damage in that area.
3. Turn the device so you can see the card reader at the top of the device. Examine that area for wires, inserts, etc. Along with any damage such as scratches or chips that could indicate that there has been an attempt to modify and tamper with the device.
4. Inspect the sides of the device and ensure that there are no signs of unexpected attachments, scratches, small drill holes, etc. that would indicate an attempt to modify or tamper with the device.

5. If after all the checks you are satisfied that the device is OK then it is OK to use – and issues found should be investigated and and resolved before the device is considered fit to use.

5.3 Instructions for detecting and responding to PTS POI device account data encryption failures

The devices used by Stripe in this P2PE Solution are designed such that any failure in the Secure Reading and Exchange of Data (SRED) encryption would stop the device working and cause a fatal error. Such a case should be reported to Stripe Support through the Stripe Dashboard.

It should be noted that it is not possible to turn-off encryption on these devices and should a merchant wish to stop using encryption they would have to cease using the Stripe Terminal P2PE Solution.

5.4 Instructions for troubleshooting a PTS POI device

WisePad 3

Problem	***Recommendation***
Device cannot be paired	● *Press and hold the power on/off button to restart the device.* ● *Check that the WisePad 3 serial number appears in the 'Scanned Device List' on the mobile-host device.*
Display turned off automatically	● *The display may have gone into 'sleep mode' – press the power on/off button to restart the device* ● *The battery may be flat, connect the USB cable and recharge.*
Device has lost connection with the mobile-host device	● *Press and hold the power on/off button to turn on the device again. The device should automatically reconnect.* ● *The battery level may be low. Connect the USB cable and recharge.* ● *Ensure the POI device and the mobile-host device are within Bluetooth range.*
Device cannot read a card successfully via NFC (Contactless)	● *Check the card in use supports NFC (Contactless Payments)* ● *Ensure the card is within 4cm of the NFC marking on the front screen of the device.*
Device cannot read a card successfully	● *Check the device has power and is connected to the mobile-host device.* ● *Check there is no obstacle in the card slot.* ● *Make sure the chip card is inserted in the correct direction.* ● *Ensure the mobile-host device is a supported model.* ● *Insert the card smoothly and at a constant speed.*

Device has no response	- *Reboot by using the end of a paperclip or similar to press the reset button on the side of the device.*

Wise POS E

Problem	***Recommendation***
Device cannot read a card successfully	- *Check the device has power.* - *Check the device instructs to swipe or insert/dip the card.* - *Check there is no obstacle in the card slot.* - *Make sure the card is inserted or swiped in the correct direction.* - *Insert or swipe the card smoothly and at a constant speed.*
Device cannot read a card successfully via NFC (Contactless)	- *Check the card in use supports NFC (Contactless Payments)* - *Ensure the card is within 4cm of the NFC marking on the front screen of the device.* - *Remove the card from wallet or purse when using.*
Device has no response	- *Check rechargeable battery is correctly inserted.* - *Check the device is fully charged.* - *Use the Power on/off button for 6 seconds to restart the device.*
Device is frozen	- *Use the Power on/off button for 6 seconds to restart the device.*

Stripe Reader M2

Problem	***Recommendation***
Device cannot be paired	- *Press the power on button to restart your device.* - *Check if you can find the device's "Serial Number" (Shown on the back of device) in the "Scanned Device List" of your smartphone or tablet.*
Device lost the connection with your smartphone or tablet when the device is auto-off	- *Press the power on button to turn on the device again. The device will automatically connect with your smartphone or tablet again.* - *The device may be at lower battery level, use the USB cable to recharge it, then retry.* - *Ensure the device or smartphone/tablet is within the reception range.*
Device does not work with your phone or tablet	- *Ensure the Bluetooth® function of your smartphone or tablet is turned on.* - *Check the version of your operating system is supported for this device's operation.*

Device cannot read your card successfully	● *Press the power on button to turn on the device again. The device will automatically connect with your smartphone or tablet again.* ● *The device may be at lower battery level, use the USB cable to recharge it, then retry.* ● *Ensure the device or smartphone/tablet is within the reception range.* ***When Swiping or inserting card*** ● *Check if the device has power when operating and ensure devices are connected.* ● *Check if the application instructs to swipe, insert or tap card.* ● *Ensure that there is no obstacle in the card slots.* ● *Check if the magstripe or chip of the card is facing the right* ● *direction when swiping or inserting card.* ● *Ensure that your phone/ tablet is a supported model for this* ● *device's operation.* ● *Swipe or insert card with a more constant speed.* ***When Tapping Card*** ● *Check if the card supports NFC payment.* ● *Ensure if the card is placed within 4 cm range on top of the NFC marking.* ● *Take the NFC payment card out from wallet or purse to avoid any interference.*
Device has no response	● *Please use a paper clip to press the reset button at the bottom of the reader for reboot.*
S700	
Problem	***Recommendation***
Device cannot read a card successfully	● *Check the device has power.* ● *Check the device instructs to swipe or insert/dip the card.* ● *Check there is no obstacle in the card slot.* ● *Make sure the card is inserted or swiped in the correct direction.* ● *Insert or swipe the card smoothly and at a constant speed.*

Device cannot read a card successfully via NFC (Contactless)	● Check the card in use supports NFC (Contactless Payments) ● Ensure the card is within 4cm of the NFC marking on the front screen of the device. ● Remove the card from wallet or purse when using.
Device has no response	● Check the device is fully charged. ● Use the Power on/off button for 6 seconds to restart the device.
Device is frozen	● Use the Power on/off button for 6 seconds to restart the device.
Shopify POS GO (S2001)	
Problem	**Recommendation**
Device cannot read a card successfully	● Check the device has power. ● Check the device instructs to swipe or insert/dip the card. ● Check there is no obstacle in the card slot. ● Make sure the card is inserted or swiped in the correct direction. ● Insert or swipe the card smoothly and at a constant speed.
Device cannot read a card successfully via NFC (Contactless)	● Check the card in use supports NFC (Contactless Payments) ● Ensure the card is within 4cm of the NFC marking on the front screen of the device. ● Remove the card from wallet or purse when using.
Device has no response	● Check the device is fully charged. ● Use the Power on/off button for 6 seconds to restart the device.

Device is frozen	● *Use the Power on/off button for 6 seconds to restart the device.*

If the information provided regarding POI Device Troubleshooting doesn’t help then please go to the Stripe Dashboard and contact Stripe Support.

6. Transporting / Shipping PTS POI Devices

6.1 Instructions for ensuring PTS POI devices are shipped to trusted sites/locations only, as needed (e.g., for repair)

Regardless of whether the POI device(s) were ordered directly by the merchant, or via the Stripe Account Manager, when the devices are dispatched, the email address entered by the ordering party will receive an email with the courier tracking information. It is important that when the package is received the tracking information supplied in the email matches that of the package received.

Any problems or discrepancies should be reported to 'Stripe Support' via the Stripe Dashboard (https://dashboard.stripe.com/login) using email, chat or by requesting a call back. The device must not be used until such time as Stripe give the all-clear or replace the device.

6.2 Instructions for securing PTS POI devices intended for, and during, transit to other locations (e.g., to a repair facility)

Merchants should be aware that Stripe will not send any staff to the merchant's location, be they Stripe employees or third-party engineers, for the purposes of 'fixing' or 'updating' a POI device. Under no circumstances should a merchant allow an unknown person to access or manipulate the POI devices.

If there is a need to repair a device Stripe will send the merchant a return shipping label for the device and notify the merchant accordingly. The merchant should not hand over a device without first checking the validity of the person collecting it.

7. Additional Guidance / Instructions

7.1 Additional guidance for merchants regarding the P2PE Solution (as needed).
If you have additional questions regarding your POI Device, please go contact Stripe Support for additional support.