Dojo P2PE Instruction Manual v1.2.2

DOJO

DOJO

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	Dojo
Solution reference number per PCI SSC website:	2023-01311.002

1.2 Solution Provider Contact Information

Company name:	Paymentsense Limited
Company address:	The Brunel Building, 2 Canalside Walk, London, W2 1DG
Company URL:	www.dojo.tech
Contact name:	Customer Support
Contact phone number:	0800 044 3550
Contact e-mail address:	support@dojo.tech

P2PE and PCI DSS

Merchants using this P2PE solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements

2. Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.

Dojo devices will only be sent from the following addresses:

- The Brunel Building, 2 Canal Side Walk, London, W2 1DG
- Prolog Fulfilment, Sherwood Park, Annesley, Nottinghamshire, NG15 0DJ

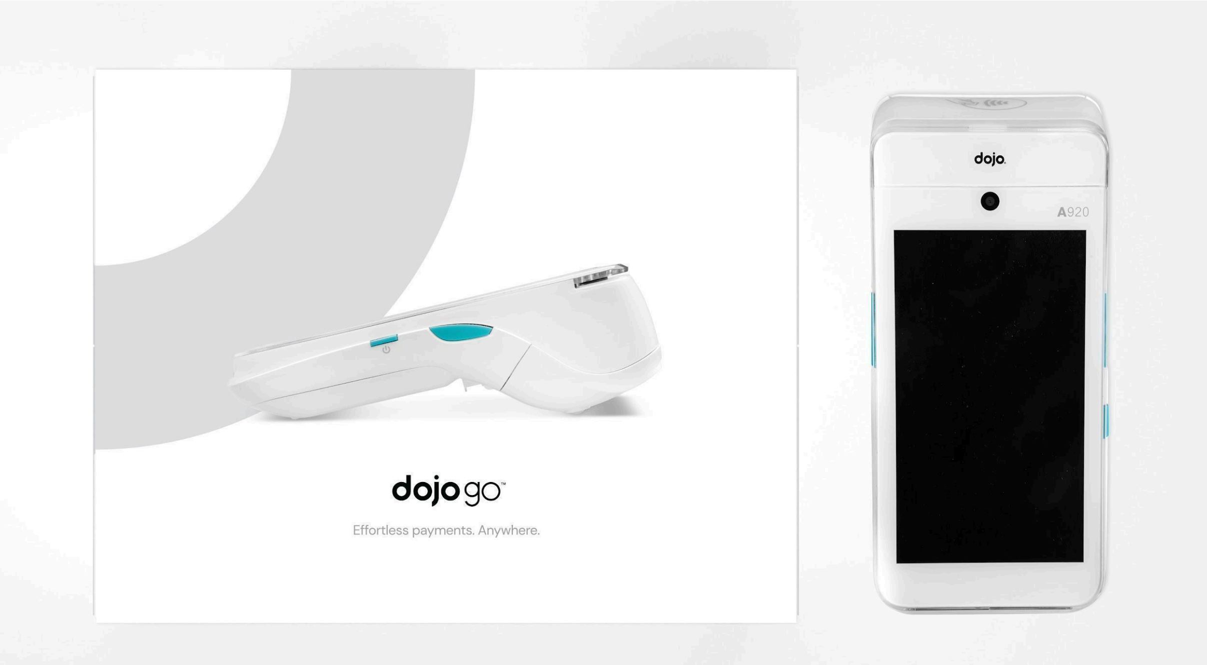
You may also receive the POI device directly from your authorised POS Partner.

If you receive a device that has arrived from a location not listed above, please let us know right away and don't use the device until Dojo has given written permission.

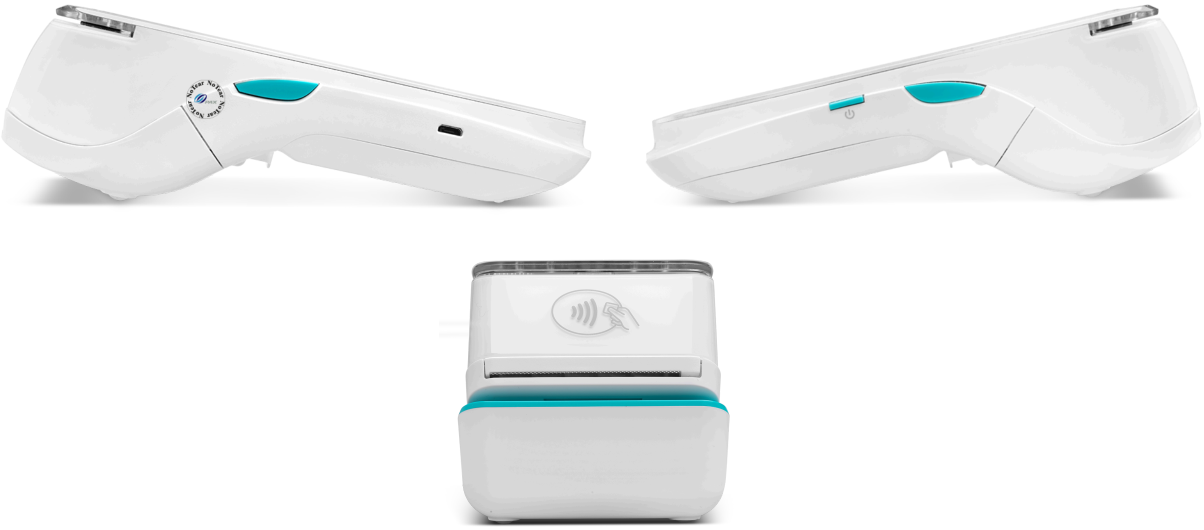
2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider.

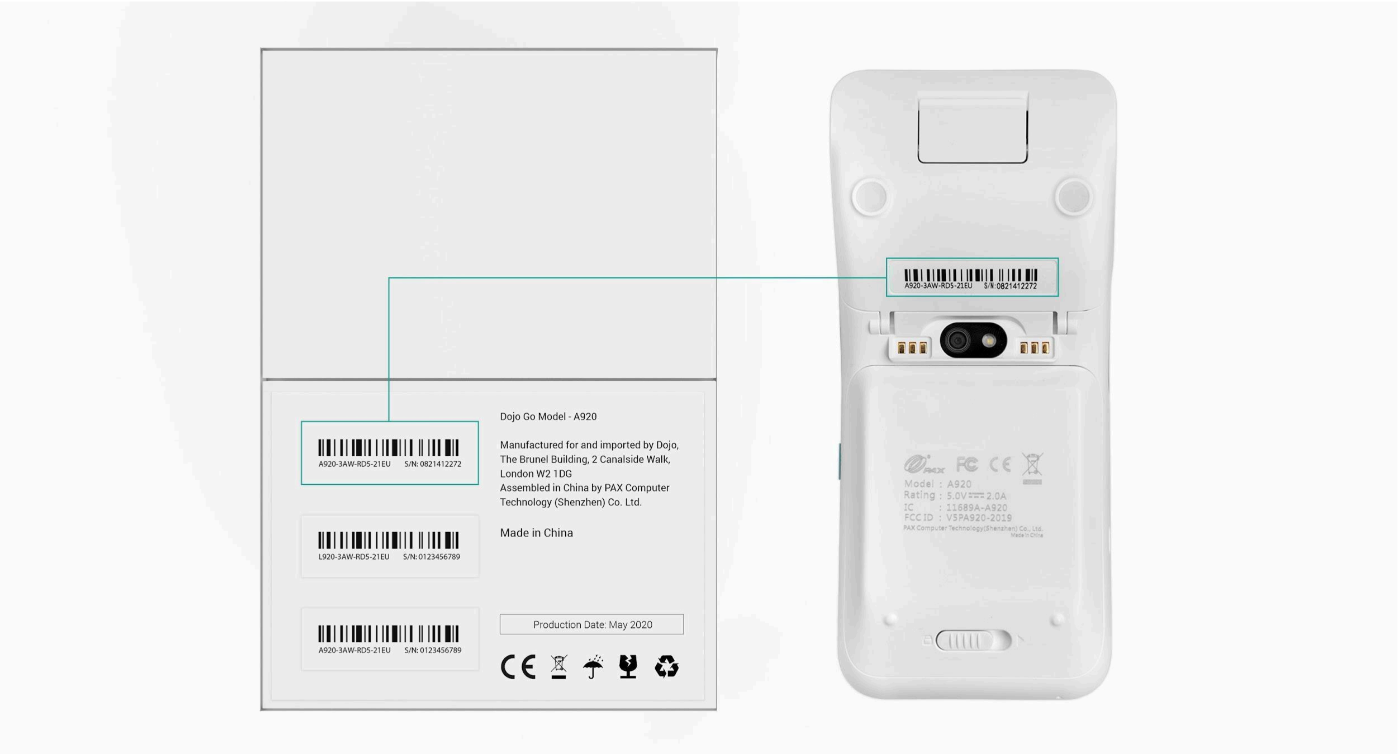
Dojo Go

Once you receive your Dojo Go, you should check it looks as expected and doesn't show any signs of tampering:



Check that the foil seal hasn’t been removed and is still intact:





A920-3AW-RD5-21EU S/N: 0821412272
L920-3AW-RD5-21EU S/N: 0123456789
A920-3AW-RD5-21EU S/N: 0123456789
A920-3AW-RD5-21EU S/N:0821412272
PAX
Model : A920
Rating : 5.0V ⎓ 2.0A
IC : 11689A-A920
FCC ID : V5PA920-2019
PAX Computer Technology(Shenzhen) Co., Ltd.
Made in China

Dojo Go Model - A920

Manufactured for and imported by Dojo,
The Brunel Building, 2 Canalside Walk,
London W2 1DG
Assembled in China by PAX Computer
Technology (Shenzhen) Co. Ltd.

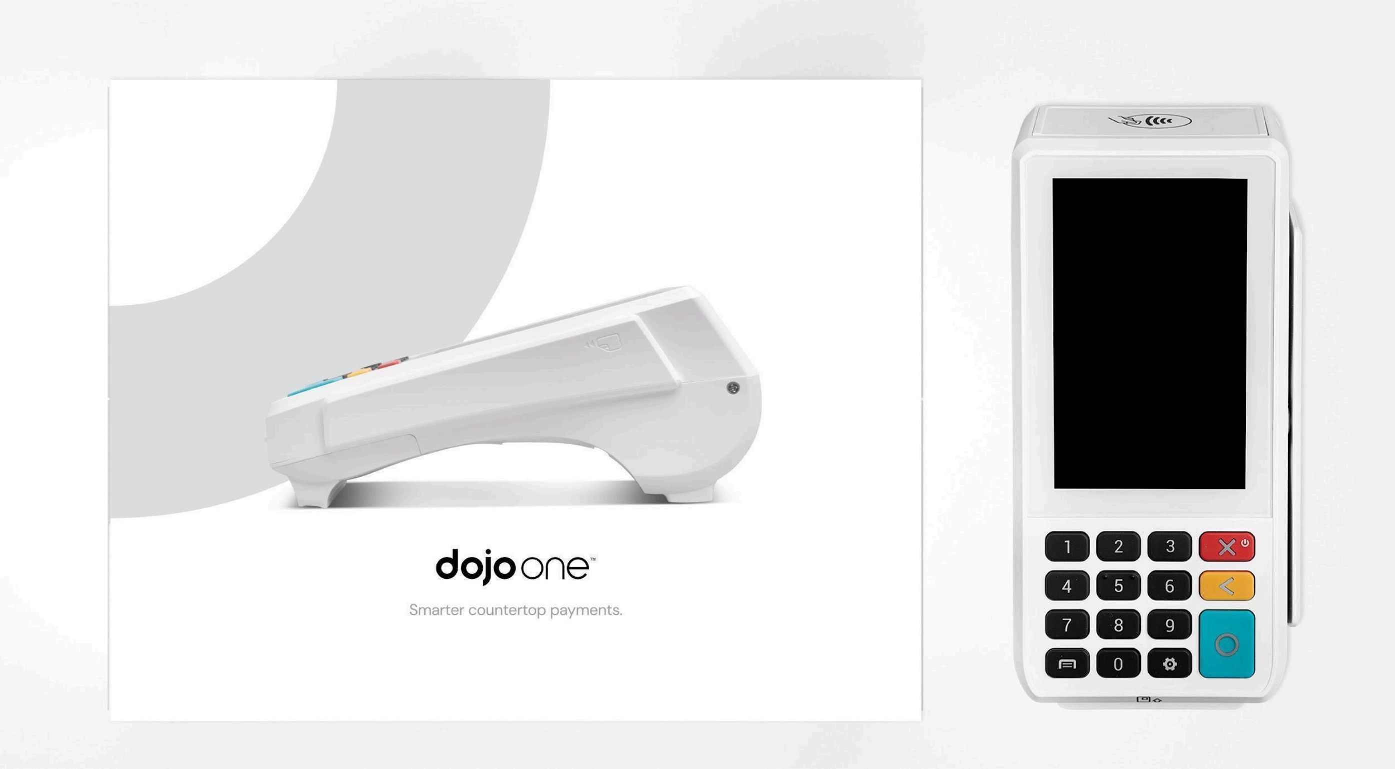
Made in China

Production Date: May 2020

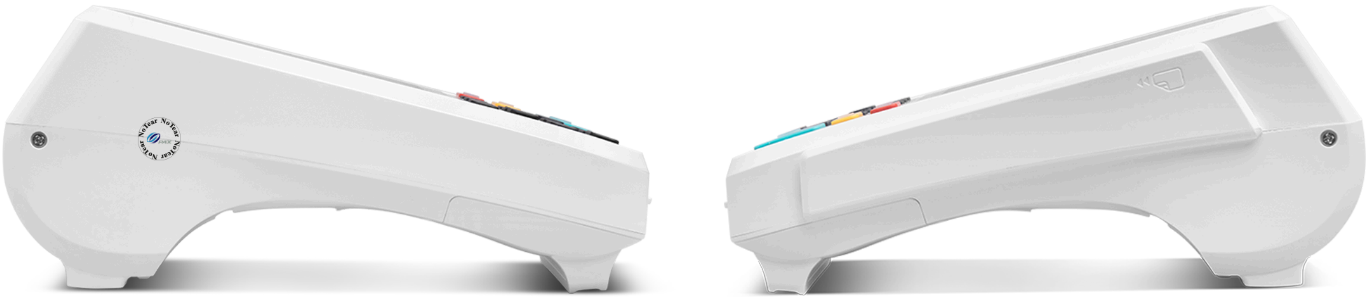
Check that the serial number printed on the box matches that on the device:

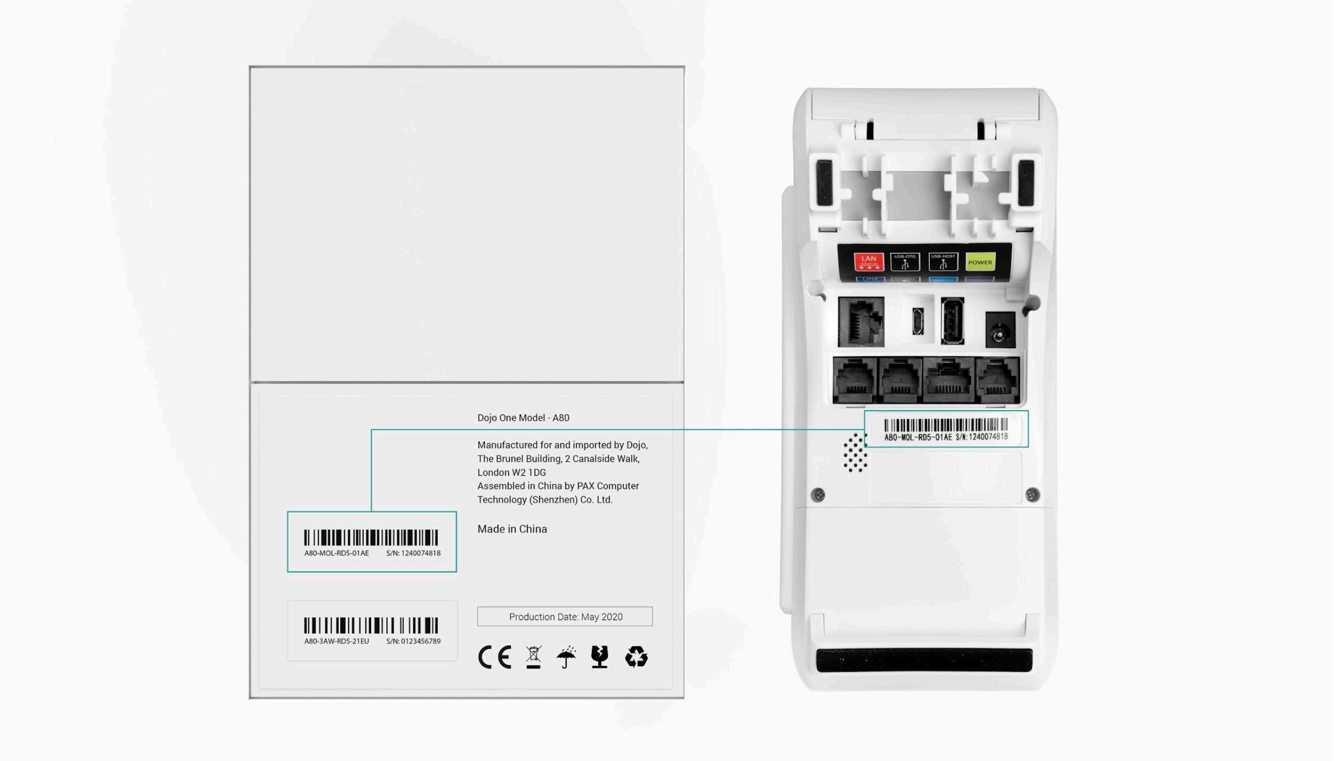
Dojo One

Once you receive your Dojo One, you should check it looks as expected and doesn't show any signs of tampering:



Check that the foil seal hasn't been removed and is still intact:



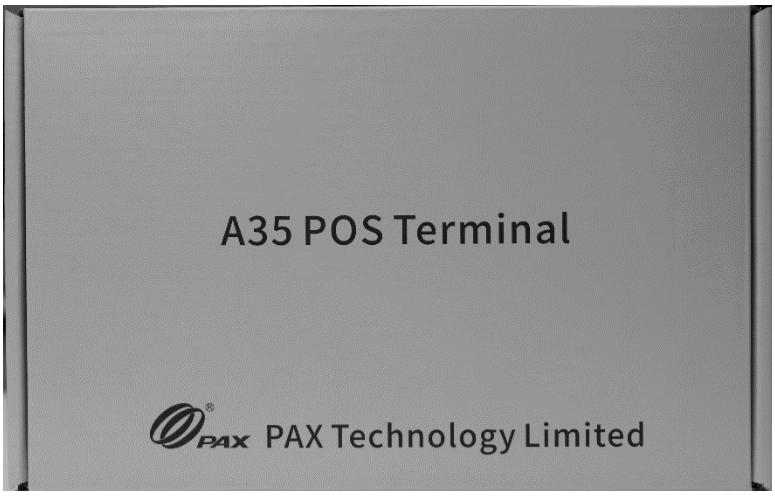

Dojo One Model - A80
Manufactured for and imported by Dojo,
The Brunel Building, 2 Canalside Walk,
London W2 1DG
Assembled in China by PAX Computer
Technology (Shenzhen) Co. Ltd.
Made in China
A80-MOL-RD5-01AE S/N: 1240074818
A80-3AW-RD5-21EU S/N: 0123456789
Production Date: May 2020
CE
LAN
USB-OTG
USB-HOST
POWER
A80-MOL-RD5-01AE S/N:1240074818

Check that the serial number printed on the box matches that on the device:

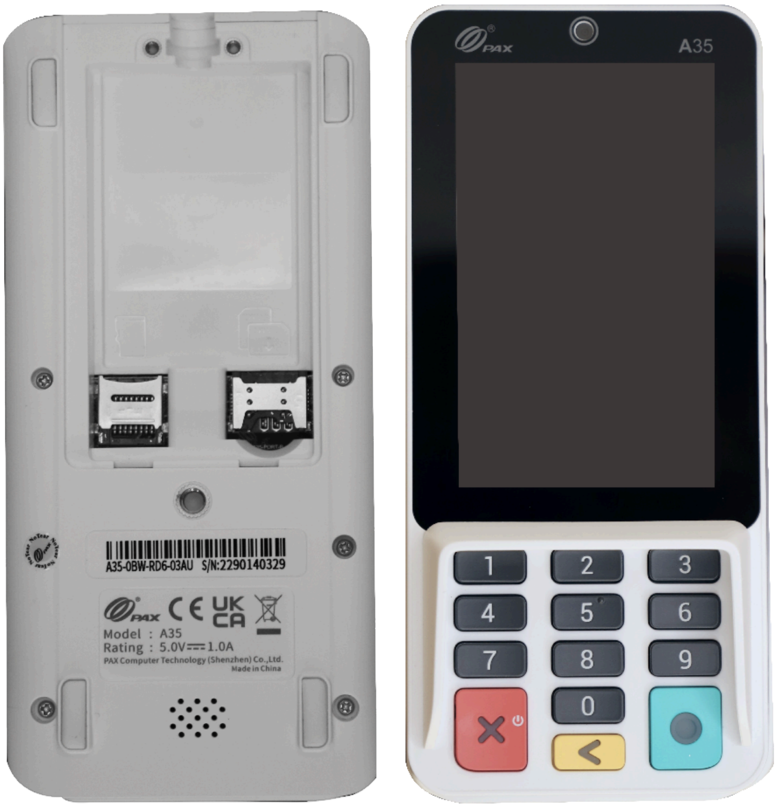
DOJO

Dojo A35

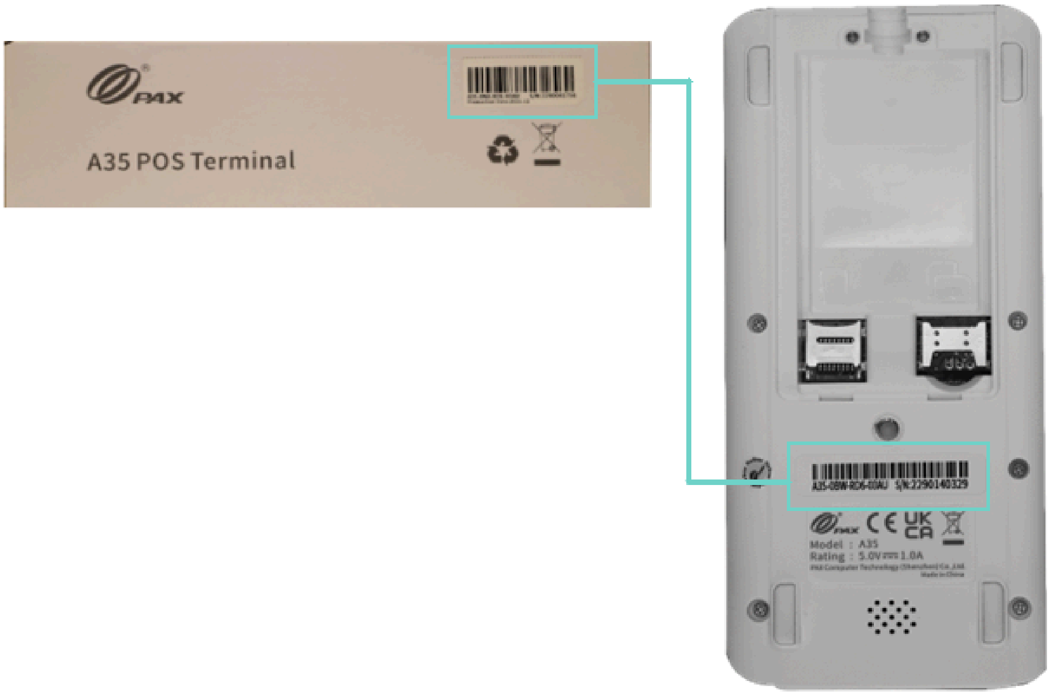
Once you receive your Dojo A35, you should check it looks as expected and doesn't show any signs of tampering:



Check that the foil seal hasn't been removed and is still intact:


A35-0BW-RD6-03AU S/N:2290140329
PAX
UK CA
Model : A35
Rating : 5.0V⎓1.0A
PAX Computer Technology (Shenzhen) Co.,Ltd.
Made in China
PAX
A35
1
2
3
4
5
6
7
8
9
0

Check that the serial number printed on the box matches that on the device:


PAX
A35 POS Terminal
A35-0BW-RD6-00AU S/N:2290140329
PAX
CE
UK CA
Model : A35
Rating : 5.0V 1.0A
PAX Computer Technology (Shenzhen) Co.,Ltd
Made in China

You can find a detailed list of your devices (make, model) and serial numbers in your Dojo account. Make sure these details are correct and let us know if you spot a mistake.

Physically secure POI devices in your possession, including devices:

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

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

Dojo will let you know in advance if a member of our team will be visiting your business to carry out any repairs to the device. We'll confirm the date and expected time of the visit, as well as the name of the engineer.

You should check their details and get in touch with our support team if there are any problems.

3. Approved POI Devices, Applications/Software, and the Merchant Inventory

3.1 POI Device Details

The following list details the PCI-approved POI devices for use in this P2PE solution.

All POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See also Section 9.2, "Instructions for how to confirm hardware, firmware, and application versions on POI devices."

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):
4-40305	PAX Computer Technology	PAX A35	A35-xxx-Rx6-0xxx (CTLS reader), A35-xxx-0x6-0xxx (No CTLS reader), A35-xxx-Rx6-Axxx (CTLS reader), A35-xxx-0x6-Axxx (No CTLS reader)	26.00.xxxx
4-30301	PAX Computer Technology	PAX A80	A80-xxx-Rx5-0xxx (with CTLS), A80-xxx-0x5-0xxx (without CTLS), A80-xxx-Rx5-1xxx (with CTLS), A80-xxx-0x5-1xxx (without CTLS), A80-xxx-Rx5-1xxx (with CTLS)	25.00.xxxx, 25.01.xxxx, 25.02.xxxx
4-40215	PAX Computer Technology	PAX A920	A920-xxx-0x5-0xxx, (Non CTLS), A920-xxx-Rx5-0xxx (CTLS), A920-xxx-0x5-1xxx, A920-xxx-Rx5-1xxx (CTLS), A920-xxx-0x5-2xxx (NON-CTLS),	25.00.xxxx, 25.01.xxxx, 25.02.xxxx, 25.03.xxxx

			A920-xxx-Rx5-2xxx (CTLS), A920-xxx-0x5-3xxx (NON-CTLS), A920-xxx-Rx5-3xxx (CTLS)	

3.2 POI Software/Application Details

Below are the details of the software/applications (both P2PE applications and P2PE non-payment software) featured on POI devices using P2PE.

All applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.

Application Vendor, Name, and Version #	POI Device Vendor	POI Device Model Name(s) and Number:	POI Device Hardware & Firmware Version #	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-text Account Data (Y/N)
Name: BroadPOS P2PE Version: v1.01.xx Ref: 2022-00841.003	PAX Computer Technology	PAX A35	Hardware: A35-xxx-Rx6-0xxx (CTLS reader), A35-xxx-0x6-0xxx (No CTLS reader), A35-xxx-Rx6-Axxx (CTLS reader), A35-xxx-0x6-Axxx (No CTLS reader) Firmware: 26.00.xxxx	Y	Y
	PAX Computer Technology	PAX A80	Hardware: A80-xxx-Rx5-0xxx (with CTLS), A80-xxx-0x5-0xxx (without CTLS), A80-xxx-Rx5-1xxx (with CTLS), A80-xxx-0x5-1xxx	Y	Y

			(without CTLS), A80-xxx-Rx5-1xxx (with CTLS) Firmware: 25.00.xxxx, 25.01.xxxx, 25.02.xxxx		
	PAX Computer Technology	PAX A920	Hardware: A920-xxx-0x5-0xxx, (Non CTLS), A920-xxx-Rx5-0xxx (CTLS), A920-xxx-0x5-1xxx, A920-xxx-Rx5-1xxx (CTLS), A920-xxx-0x5-2xxx (NON-CTLS), A920-xxx-Rx5-2xxx (CTLS), A920-xxx-0x5-3xxx (NON-CTLS), A920-xxx-Rx5-3xxx (CTLS) Firmware: 25.00.xxxx, 25.01.xxxx, 25.02.xxxx, 25.03.xxxx	Y	Y

PLEASE NOTE: You must use only PCI-approved P2PE devices to process transactions. If you process any transactions using devices that are not P2PE validated you will no longer be considered PCI compliant.

3.3 POI Inventory & Monitoring

- All POI devices must be documented via inventory control and monitoring procedures, including device status (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 POI devices, must be reported to us via the contact information in Section 1.2 above.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

You can access information about all of your devices, including the make, model, location, serial number and status in your account or the Dojo app.

You should regularly check this information and let us know immediately if it needs updating or where you've made a change (for example, if you've moved a device from one location to another). You're responsible for making sure this is maintained and updated.

You should keep a log to confirm the date of each check for your own records. If you wish to, you can maintain a comprehensive inventory log like the example provided below.

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory

4. POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in Table 3.1 are allowed for cardholder data capture.

If a merchant's PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

- The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.

Do not change or attempt to change device configurations or settings.

Changing device configurations or settings may invalidate the PCI-approved P2PE solution in its entirety. Examples include, but are not limited to:

- Enabling any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device.
- Altering security configurations or authentication controls on the POI device.
- Physically opening the POI device.
- Attempting to install unauthorized applications onto the POI device.

4.1 Installation and connection instructions

All of the Dojo devices listed within table 3.1 are P2PE enabled. To activate the P2PE encryption key you'll need to complete the device set up.
Once you've received the device, you'll need to follow the steps below:

1. Check the device for any tampering
2. Switch it on
3. Connect the device to the internet (either through Wi-Fi, Ethernet or using mobile data from a SIM card). The screens on the device will guide you through this

4. Continue to follow the setup guide on the device, entering your activation code when requested (this will have been emailed to you).

Once setup is complete control of the device is yours. It's your responsibility to protect and maintain the device in line with this document and the Data Security Policy.
If there are any issues during the setup process please let us know.

Note: Only PCI-approved POI devices listed in the PIM are allowed for use in the P2PE solution for account data capture.

4.2 Guidance for selecting appropriate locations for deployed devices

It's down to you to control public access to POI devices. Access must be limited to the parts of the POI device a customer needs to use to complete a transaction (for example, PIN pad and card reader). You must keep a close eye on the device at all times, including when a customer is using it.

Training should be provided to staff to make sure only authorised personnel use the device and know how to spot suspicious behaviour. Training guidance can be found in Appendix A of the Data Security Policy.

4.2 Guidance for selecting appropriate locations for deployed devices

Make sure the location of the device enables anyone operating it to be able to observe and monitor the device at all times, including when a customer is interacting with it.

When the device is not in use it should be stored securely in a locked room or drawer that only authorised staff can access.
Responsibility for the security of the device should only be given to authorised staff. If the device is stored away securely, you should record a log of staff date/time in and staff date/time out for a clear audit trail.

If an unexpected third-party is requesting access to the device for maintenance, the request should be denied, even if the third-party is from a Dojo authorised courier or present themselves as part of the Dojo team. You should get in touch with Customer Support straight away to report this.

Training should be provided to staff to make sure they're able to check the device and identify any tampering, removal or substitution. Training guidance can be found in Appendix A of the Data Security Policy.

5. POI Device Transit

5.1 Instructions for securing POI devices intended for, and during, transit

There could be a few reasons why a device needs to be returned to us:

- Technical issues
- Device upgrade
- Account closure

If you need to return the device, please follow the steps below:

- Contact Dojo Customer Support
- A member of the team will walk you through the device deactivation process
- Once the device is deactivated and wiped clean, it should be packaged with all the accessories in a taped cardboard box
- A returns label will be emailed to you and should be attached to the package
- We'll send an email to confirm the courier details, including when they're due to collect the package (make sure you verify the device collection)
- Once we've received it, we'll update your account device information. You should also make an inventory note for your own records to confirm the deactivation, shipping information and return of the device

Your device must be collected by an authorised courier that you arrange through Dojo. They'll need a signature and provide confirmation of collection.

Dojo authorised couriers are listed below::

- Yodel
- DPD

Physically secure POI devices in your possession, including devices:

- Awaiting deployment

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

5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only

Dojo will only ship devices to an address that a business is either registered to and/or trading at. We'll email your activation code to the named contact at the business for each device and location.

Once we've shipped your device to your specified location, you'll need to let us know if you need to move it to a different location so that we can update your account. When shipping the device, make sure you do this under the supervision of authorised staff. Checks should then be completed at the new location to make sure the device hasn't been tampered with or substituted. You should also keep a note of this for your own records.

6.**POI Device Tamper & Modification Guidance**

6.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

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

You or an assigned staff member will need to perform regular inspections of the device to make sure that it has not been tampered with.

You'll need to check for the following:

- All device connections are secure (cabling, any peripherals etc.)
- The manufacturer seal has not been breached
- No error messages are present on the screen to indicate a security issue
- Any physical alterations to the device, such as holes in the device or other material changes that could hide damage or tampering
- No foreign objects have been attached to the device

If these checks can't be carried out physically, you should use other resources to do so. For example, using video surveillance to prevent any unauthorised activity.

If you spot any evidence of tampering or suspicious activity, you must stop using the device immediately, remove it from service and call Dojo on 0800 044 3550 for return authorisation.

Training guidance that can be distributed to your staff is provided in Appendix A of the Data Security Policy.
You can find more information about preventing skimming (the unauthorised capture and transfer of payment data) by going to www.pcisecuritystandards.org and selecting 'Document Library' and searching for '*Skimming Prevention: Overview of Best Practices for Merchants'* and/or *Skimming Prevention: Best Practices for Merchants*

6.2 Instructions for responding to evidence of POI device tampering

If you spot any evidence of tampering or suspicious activity having taken place you must stop using the device immediately, remove it from service and notify Dojo Customer Support on 0800 044 3550 for return authorisation. You'll need to follow the steps outlined in 5.1 when returning the device.

Suspicious activity and tampering include, but are not limited to the following:

- Physical damage to the device
- Unidentified stickers or objects attached to the device
- The device has gone missing for a while and then reappeared

Training guidance that can be distributed to your staff is provided in Appendix A of the Data Security Policy.

7. **Device Encryption Issues**

7.1 Instructions for responding to POI device encryption failures

If the encryption within your device fails, you should remove it from service and contact Dojo to report it.

We'll then investigate to find out what the issue is. You shouldn't use the device until we've confirmed that the issue has been resolved and P2PE encryption has been restored, or we authorise for it to be returned. If we authorise a return of the device you'll need to follow the steps in 5.1.

8. **POI Device Troubleshooting**

8.1 Instructions for troubleshooting a POI device

If your device is not working as expected, please follow these troubleshooting instructions:

1. Restart the device

2. Check the device is still connected to the internet and you have a stable connection

3. Complete a 1p transaction to test the device

4. Otherwise, contact Dojo Customer Support

9. **Additional Guidance**

9.1 Instructions for troubleshooting a POI device

See section 8.1 for troubleshooting information. Dojo Customer Support will help with any technical issues if you aren't able to fix the problem.

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices

If you want to confirm the hardware, firmware and application version on your device, please contact Dojo Customer Support.