Reviewed April 2023

Point-to-Point Encryption (P2PE) Implementation Manual

Flex
Flex (2nd Generation)
Flex C405 (3rd Generation)
Mini (2nd Generation)
Station 2018
Station Solo
Station Pro
Mini C305 (3rd Generation)
Station Duo Terminal C505
Mini Terminal C506

Version 5.3

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	Clover - TransArmor P2PE Solution – RSA/PKI
Solution reference number per PCI SSC website:	TBD

1.2 Solution Provider Contact Information	
Company name:	Clover Network, LLC
Company address:	415 N. Mathilda Ave., Sunnyvale, CA 94085
Company URL:	www.clover.com
Contact name:	Customer Support
Contact phone number:	(855) 853-8340
Contact e-mail address:	p2pe@clover.com

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.

Clover payment terminals are distributed by Fiserv Hardware Services and authorized partners.

Ensure that you should be expecting to receive a Clover payment terminal and the received product matches the device ordered and described in the production activation e-mail.

In the United States, if ordering from Clover directly, the shipment origin address is either

FHS Marietta
1169 Canton Rd
Marietta, GA 30066
USA

FHS Roseville
8875 Washington Blvd Ste A
Roseville, CA 95678
USA

In Canada, if ordering from Clover directly, the shipment origin address is

FHS Mississauga
205 Export Blvd.
Mississauga, Ontario L5S 1Y4
Canada

If ordering from an authorized partner, contact the authorized partner for details about shipment origin address. Please contact p2pe@clover.com to confirm that you are using an authorized partner.

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

Clover payment terminals leave manufacturing and repair facilities with a device identity digital certificate and key material backing the certificate protected by tamper detection mechanisms that will wipe the key should a tamper be perceived. The tamper detection mechanisms are backed and powered by an embedded battery and help ensure that the device is not tampered in transit/before arrival.

Should the device arrive with a tamper notification, do not use and contact Clover support. Please refer to the PCI Security Policy for each Clover device type for instructions on verifying the tamper status of a Clover device. PCI Security Policy documents are available on the PCI website.

Clover devices use pinned private Certificate Authorities (CAs) to establish secure network communication through mutual authentication.

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.
Should there be a need to confirm the business need and/or identity of those seeking access to POI devices, please reach out to Clover Contact support. Additionally, you can email to p2pe@clover.com.

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

3.1 POI Device Details

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

Devices are only part of a P2PE solution if the device hardware and firmware versions match the versions enumerated in this document match the devices in use and if the merchant (and authorized partner) follow all applicable described procedures.

All POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
See section named "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):
4-40209	*Clover Network, Inc.*	*Clover Flex*	*1.XX* *2.00* *3.XX* *4.01*	*0 01.XX.XXXX 01.XX.XXXX (01.XXXXX) (SRED)* *0 02.XX.XXXX 02.XX.XXXX (01.XXXXX) (SRED)* *0 02.xx.xxxx 03.xx.xxxx (01.xxxxx) (SRED)*
4-30302	*Clover Network, Inc.*	*Clover Station Printer with customer facing contactless payments*	*1.XX*	*0 01.xx.xxxx 01.xx.xxxx (01.XXXXX)*

4-10248	*Clover Network, Inc*	*Clover Mini (2nd Generation)/C302; Clover Mini Enterprise/C303; Clover Station Pro Terminal/C503*	*3.XX* *4.01* *4.02*	*0 02.XX.XXXX* *02.XX.XXXX (01.XXXXX)*
4-40329	*Clover Network, Inc*	*Clover Mini C305; Clover Station Duo Terminal C505; Clover Mini Terminal/C506*	*1.x1 (C305);* *1.x2 (C505);* *1.x3 (C506)*	*0 02.XX.XXXX* *05.XX.XXXX (01.XXXXX)*
4-40338	*Clover Network, Inc*	*Clover Flex/C405*	*1.x1*	*0 02.XX.XXXX* *05.XX.XXXX (01.XXXXX)*
4-30298	*Clover Network, Inc*	*Clover Station, Clover Station Solo*	*1.XX* *2.XX* *3.XX* *4.XX*	*0 02.XX.XXXX* *05.XX.XXXX* *0 01.XX.XXXX* *01.XX.XXXX*

3.2 POI Software/Application Details

This P2PE solution does not utilize any P2PE applications.

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)
N/A	NA	NA	NA	NA	NA

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 Clover 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.

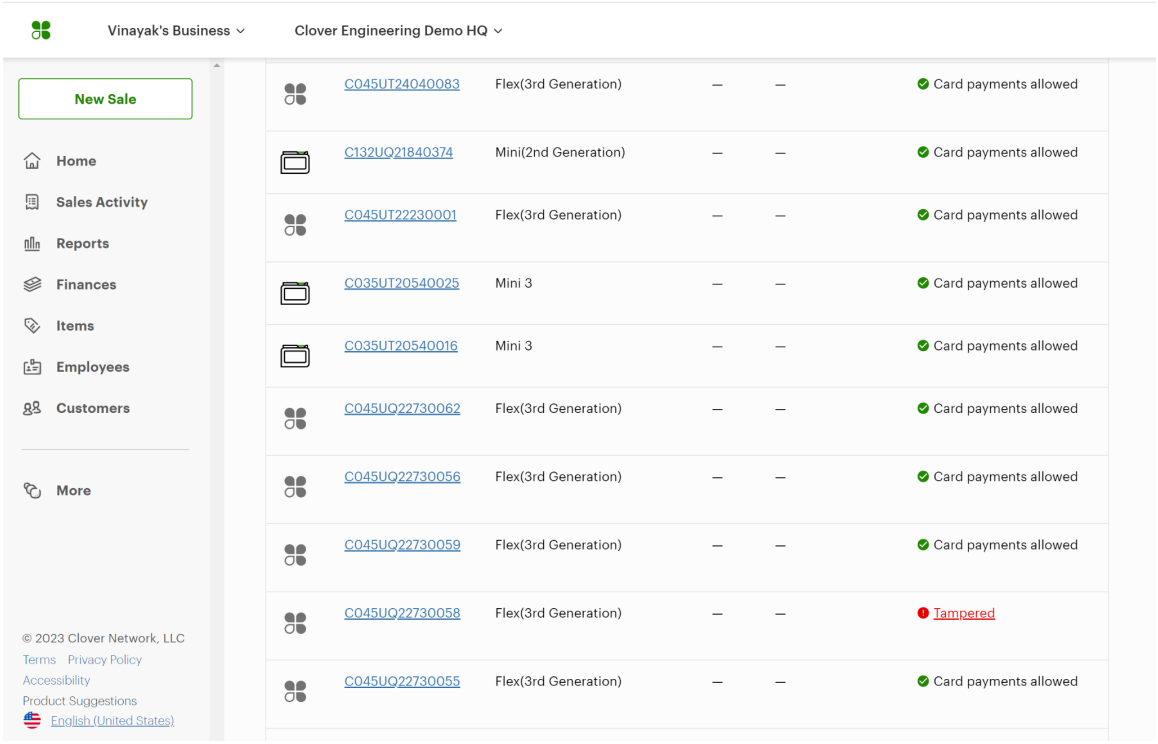
Merchants can verify the devices associated with their account using the Clover web management dashboard at https://www.clover.com/dashboard . Note that only the device types listed in this document are approved for use in this P2PE solution.

All registered Clover devices will appear in the Devices section of the dashboard. From here, you can regularly review your inventory.

To maintain participation in a P2PE solution, merchants must perform physical inspection of their devices by checking serial numbers upon receipt before use and on a regular basis. Records of the inspections should be maintained in an external document.

Missing payment devices should be reported to p2pe@clover.com. Unidentified payment devices should be removed and reported as well as any unexpected changes to the list of devices on the web dashboard.

The following image is an example of the Devices section on the Clover Web Management Dashboard.



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

For detailed physical installation and connection instructions, please refer to the Quick Start Guide (QSG) enclosed in the device package along with necessary cables and connectors.

Once the physical installation is complete, power on the Clover device to go through the process as described at https://www.clover.com/en-US/help/get-ready-to-use-clover.

Activate the device using activation information described at https://www.clover.com/en-US/help/find-your-device-activation-code.

Once the activation code you received via email for your Clover device is entered on the device, you are all set to begin use of the Clover device.

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

Clover payment devices are approved for attended and semi-attended use only. Accordingly, the devices should be installed in locations where staff are able to oversee device use, but carefully positioned in such a way that sensitive authentication data is not visible when entered on the devices by others or security cameras.

4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

Merchants should physically secure the devices when possible to prevent any unauthorized removal or substitution.

It is recommended that devices be stored in a securely locked area when not in use.

Merchants can view all their deployed Clover devices on the Clover Web Dashboard and use the inventory to conduct regular checks for signs of tampering and removal/substitution.

5. POI Device Transit

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

Clover devices leave manufacturing and repair facilities with a device identity digital certificate and key material backing the certificate protected by tamper detection mechanisms that will wipe the key should a tamper be perceived. The tamper detection mechanisms are backed and powered by an embedded battery and help ensure that the device is not tampered in transit/before arrival.

This functionality also serves as a transport security measure. Should the device arrive with a tamper notification, do not use and contact Clover support.

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
Clover merchants are subject to underwriting requirements where business details are verified. Devices are shipped to merchants upon completion of underwriting.

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.

- Visual inspection
  - Before using the device, the user must conduct a regular inspection to check for evidence of tampering. The following is a partial list of procedures. Check the PCI website for the latest best practices.
    - Exterior should show no evidence of cutting or disassembly.
    - No evidence of unusual wires or overlays connected inside the ICC slot nor on or near the PIN entry area.
    - No changes to the resistance when inserting or removing a card from the ICC slot.
    - Discontinue use of the device and contact Clover immediately if your device is missing or appears to have been tampered with.
- Tamper detection mechanisms
  - If a tamper is perceived by the device, a message will be shown on the device and an e-mail message will be dispatched to the merchant when the tamper is reported to the Clover cloud. Should either notification be received, the device must be removed. If the provided guidance in the notifications are unclear, please reach out to Clover at p2pe@clover.com for assistance.
- Contact information
  - Enquiries can be submitted to p2pe@clover.com

6.2 Instructions for responding to evidence of POI device tampering

Please contact Clover immediately at p2pe@clover.com on account of any device tampering. Please be prepared to provide a description of the situation along with information identifying the device (e.g., serial), and merchant.

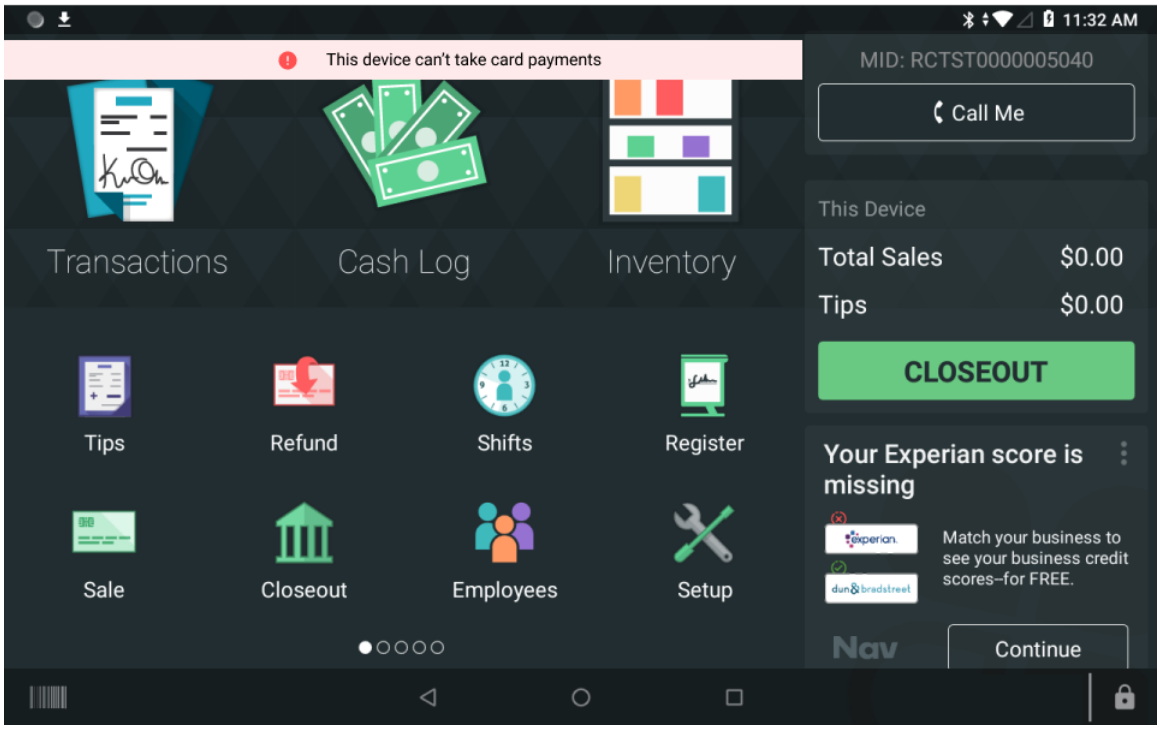
7. Device Encryption Issues

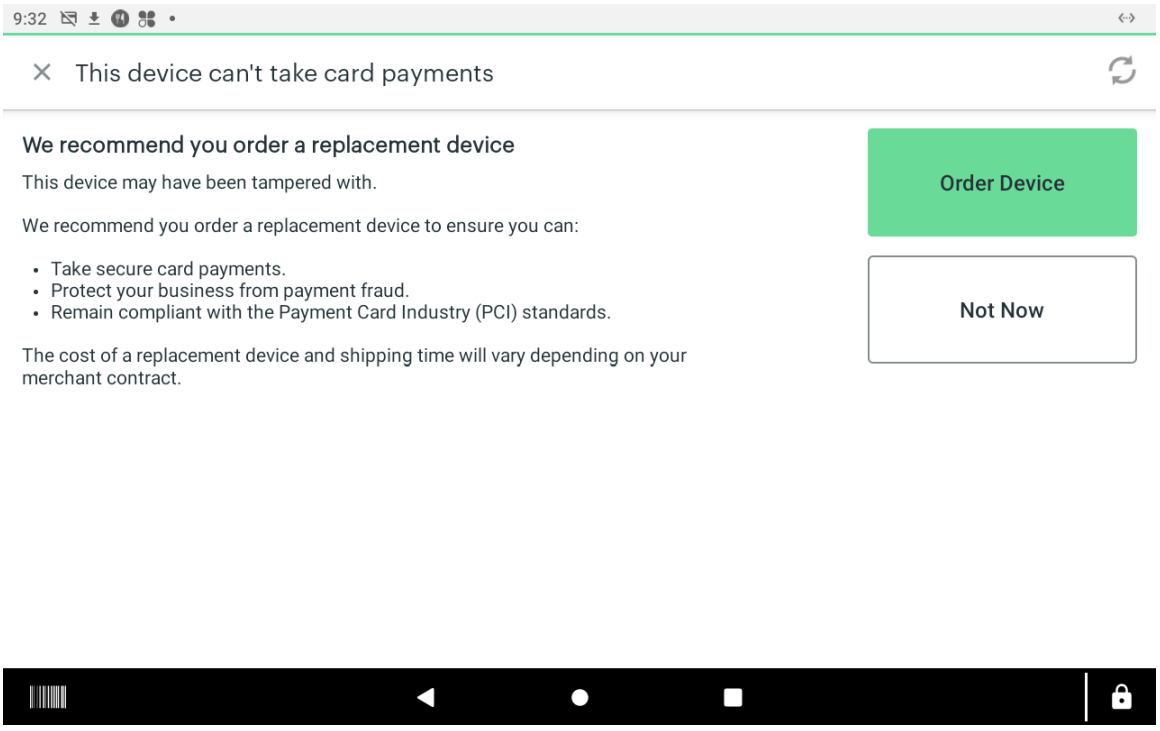
7.1 Instructions for responding to POI device encryption failures

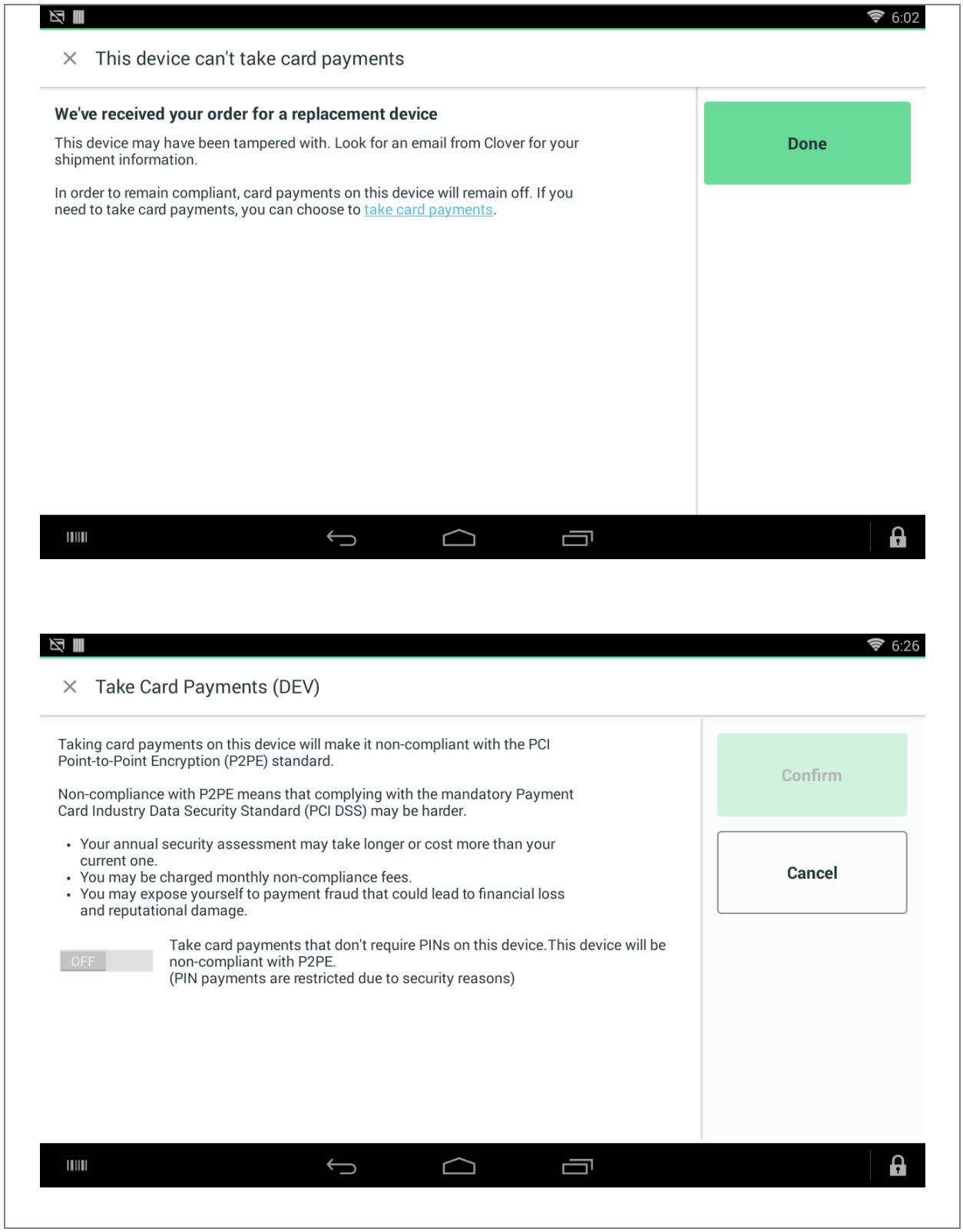
Clover devices are designed to not allow encryption to be disabled.

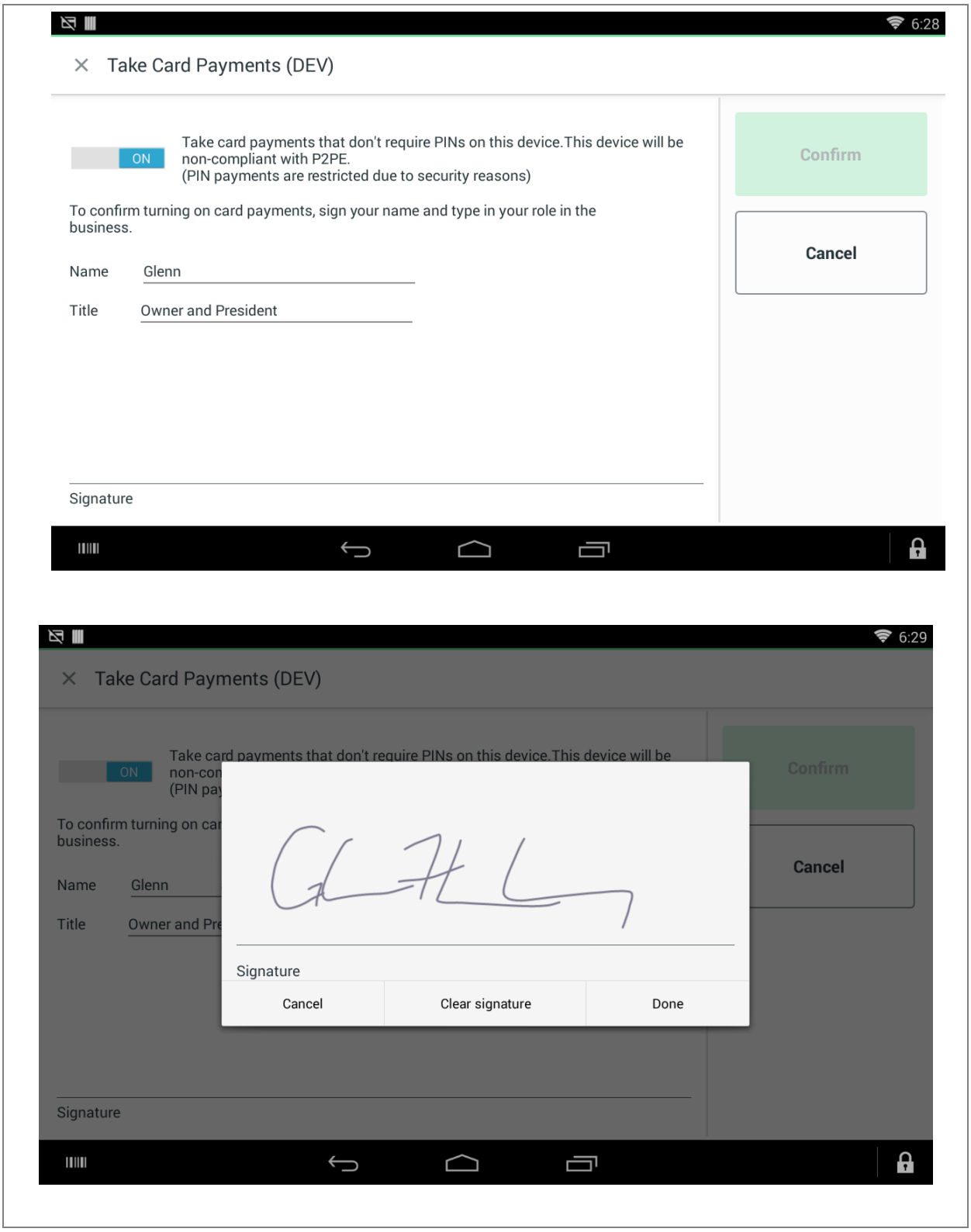
In any case, should there be a suspicion that a device encryption failure has taken place, discontinue use of the device immediately and reach out to Clover at p2pe@clover.com and/or Clover support to report and describe the situation.

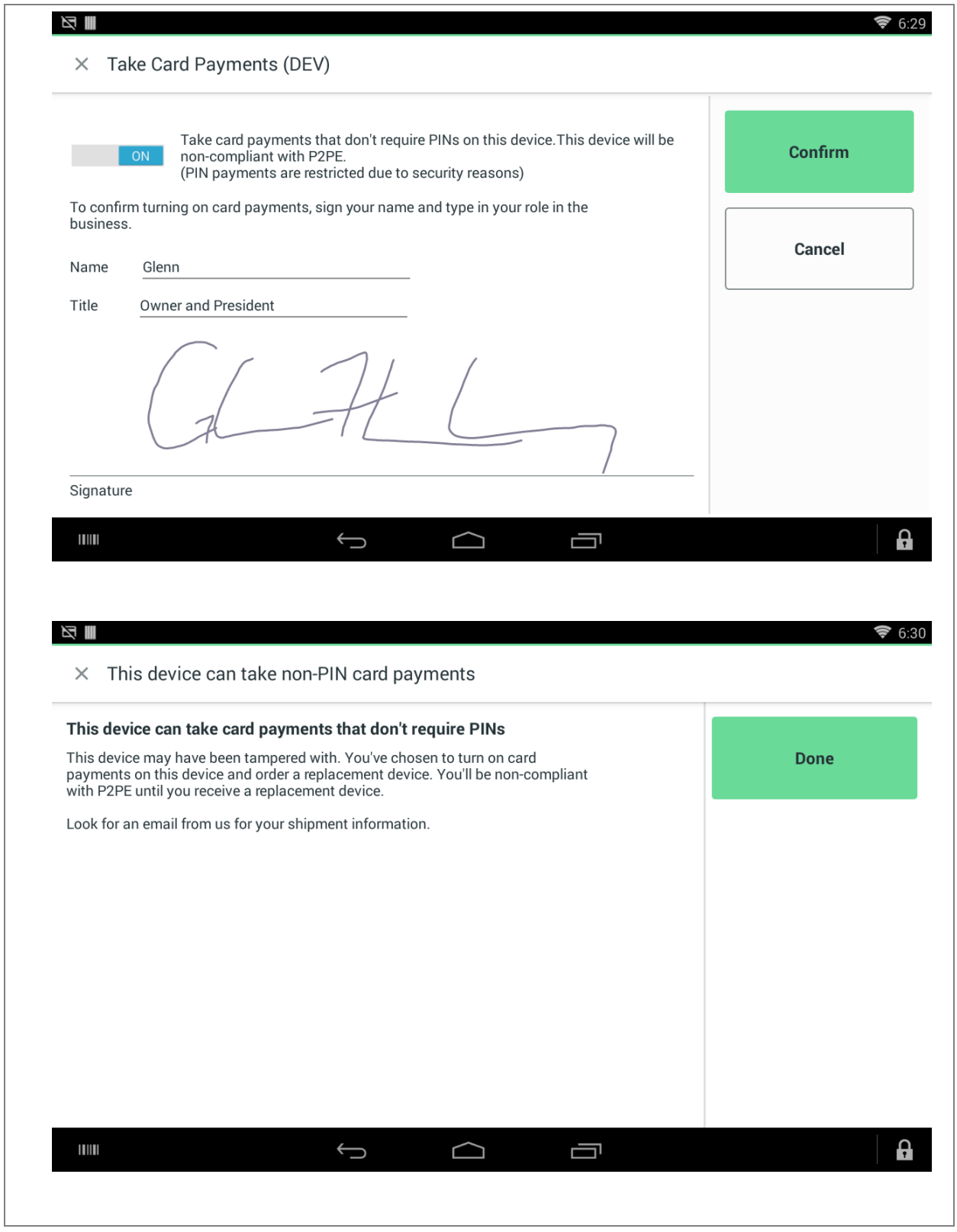
- Removal from P2PE solution
    - Below screens will be displayed on the device should there be any tamper. The merchant is provided a choice to order a device replacement and/or to end their participation in P2PE compliance. It is highly recommended to stop using the tampered device and order a replacement device immediately.
    - If the merchant signs an agreement to continue operating the device in a non-P2PE compliant mode and allow non-PIN transactions the version number of the device firmware will change and will not match any certified/verified PCI firmware version number approved for use in this solution. From this point the operator will no longer be P2PE compliant.











8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

The POI device contains no user serviceable components with an exception of an user replaceable battery on the applicable products. If a device appears to be malfunctioning, contact Clover support for assistance. Please be prepared to provide the device serial number and a description of the issue.

9. Additional Guidance

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

Hardware version information can be found on the serial label. Firmware version information can be found by opening the Settings app and selecting About Device. Scroll down for the build number. This is the firmware version for the device.
Clover devices do not support P2PE applications.