PCI Point-to-Point Encryption (P2PE) 3.1

Instruction Manual (PIM)

Canada Version 1.0

April 2025

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	*Global Payments P2PE*
Solution reference number per PCI SSC website:	*2022.00056.003*

1.2 Solution Provider Contact Information	
Company name:	*Global Payments Canada GP*
Company address:	*3381 Steeles Avenue East* *Suite 200* *Toronto, ON M2H 3S7*
Company URL:	*globalpayments.com/en-ca*
Contact name:	*Global Payments Customer Care*
Contact phone number:	*1-888-682-3309*

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
Global Payment Companies take all the necessary precautions to ensure devices are not tampered with or compromised prior to being shipped to you. However, there are steps that you must undertake to ensure that devices have not been tampered with during transit. First you must confirm that shipment of devices originated from our PCI P2PE Validated KIF or trusted deployment facility listed here: Global Payment Canada GP 151 Carlingview Drive, Unit 16 Etobicoke, M9w5S4 In some replacement instances, Global Payments installers will install the devices. Please confirm with them that they have the correct devices for your setup. Confirmation that devices were shipped from an authorized source may be performed by comparing the providers shipping information with the information listed above. If you receive POI devices from another provider, you must contact Customer Care (see section 1.2) for confirmation. We will take the necessary steps to communicate any updates to our KIF listing.

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

Inspection upon Receipt: All devices within this program are shipped from authorized distribution partners in tamper-evident packaging. Examples of tamper evident packaging can be tamper evident tape (on seams of box or tamper bag (containing the P2PE device).

Inspect the packaging and device(s) to make sure there is no tampering. If there are any concerns that a tamper bag has been opened during shipment, or other suspicion of tampering, follow all instructions in Section 6.2 to respond to the potential tamper. Devices that are suspected of tamper should not be removed from the tamper bag unless so instructed by Global Customer Care. Before enabling a device, merchants must conduct a physical inspection of the device to validate that no tampering has occurred, as described in Physical Inspection instructions below.

Tamper-evident labels are placed over all sensitive device screws and seams, which will provide visual indication when tampered, as shown in the embedded files below:

Physically secure Point-of-Interaction (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
Access to POI devices by third-party personnel for repair/maintenance must be monitored. This monitoring is required to ensure there is no unauthorized access to the device that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you should have a policy in place that requires the following steps: • Maintenance/repair of the device must be pre-arranged with date and time frame of third-party personnel defined. Unexpected visits for repair/maintenance must be verified. If they cannot be verified, access to the device must be denied. • Prior to granting access to a device, personnel must be identified and authorized to access the device. • Third-party personnel access must be recorded and include personnel name, company, time of access, and purpose of access. Log must be maintained for no less than one year. • Personnel must be escorted and observed at all times • Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.

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. Note 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
4-30400	Verifone Inc	T650P	H561-07-aa-0Nx-xxx-A 1 (a=0-9; A to F)	Android: 2.0C.x SP Core DLL: T650-A-D-1A.x.x SP Core: T650-A-P-2A.x.x SP Core: T650-A-P-3A.x.x SP Core: T650p-A-P-1A.x.x SP Driver: T650P-A-S-1A.x.x SP Driver: T650p-A-S-1A.x.x SRED 1.0.0.xxx Android: 1A.x.x SRED 1.x.x.xxx
4-30392	Verifone Inc	T650C	H560-07-aa-0Nx-xxx-A 1 (a=0-9; A to F)	Android: 2.0C.x SP Core DLL: T650-A-D-1A.x.x SP Core: T650-A-P-2A.x.x SP Core: T650-A-P-3A.x.x SP Core: T650C-A-P-1A.x.x SP Driver: T650C-A-S-1A.x.x SP Driver: T650C-A-S-1A.x.x SRED 1.0.0.xxx Android: 1A.x.x SRED 1.x.x.xxx
4-80062	Verifone Inc	P630	H565-0007-xxxx-xxx-xx x-A1	VOS3: 01.xx.xx, VOS3: 02.xx.xx, Vault: APFW_01.01.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPBL_01.01.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.01.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: SPFW_01.04.xx.xx,Android: 3.00D.xx,Android: 3.01D.xxVOS3: 01.xx.xx: 31 Dec 2025,Android: 3.01D.xx: 31 Dec 2025,Vault: SPFW_01.04.xx.xx: 31 Dec 2025,VOS3: 02.xx.xx: 31 Dec 2025,Android: 3.00D.xx: 31 Dec 2024,Vault: SPBL_01.01.xx.xx: 31 Dec 2024,Vault: SPFW_01.01.xx.xx: 31 Dec 2024,Vault: APFW_01.01.xx.xx: 31 Dec 2024,Vault: SPBL_01.02.xx.xx: 31 Dec 2024,Vault: SPFW_01.02.xx.xx: 31 Dec 2024,Vault: APFW_01.02.xx.xx: 31 Dec 2024

3.2 POI Software/application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution.

Note that 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)
Global Payments Direct Inc Unified Payment Application (UPA) V 02.*.*.*-* (2023-00056.007) Verifone Secure Data Interface (VFISDI):1.6X (2022-00154.108)	Verifone Inc	T650P	*HW #: H561-07-aa-0Nx-xxx-A1 (a=0-9; A to F)* *FW #: Android: 2.0C.x* *SP Core DLL: T650-A-D-1A.x.x* *SP Core: T650-A-P-2A.x.x* *SP Core: T650-A-P-3A.x.x* *SP Core: T650p-A-P-1A.x.x* *SP Driver: T650P-A-S-1A.x.x* *SP Driver: T650p-A-S-1A.x.x* *SRED 1.0.0.xxx* *Android: 1A.x.x* *SRED 1.x.x.xxx*	Y	Y
Global Payments Direct Inc Unified Payment Application (UPA) V 02.*.*.*-* (2023-00056.007) Verifone Secure Data Interface (VFISDI):1.6X (2022-00154.108)	Verifone Inc	T650C	*HW #: H560-07-aa-0Nx-xxx-A1 (a=0-9; A to F)* *FW #: Android: 2.0C.x* *SP Core DLL: T650-A-D-1A.x.x* *SP Core: T650-A-P-2A.x.x* *SP Core: T650-A-P-3A.x.x* *SP Core: T650c-A-P-1A.x.x* *SP Driver: T650C-A-S-1A.x.x* *SP Driver: T650c-A-S-1A.x.x* *SRED 1.0.0.xxx* *Android: 1A.x.x* *SRED 1.x.x.xxx*	Y	Y
Global Payments Direct Inc Unified Payment Application (UPA) V 02.*.*.*-* (2023-00056.007) Verifone Secure Data Interface (VFISDI):1.6X (2022-00154.108)	Verifone Inc	P630	*HW #: H565-0007-xxxx-xxx-xxx-A1* *FW #: VOS3: 01.xx.xx, VOS3: 02.xx.xx, Vault: APFW_01.01.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPBL_01.01.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.01.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: SPFW_01.04.xx.xx,Android: 3.00D.xx,Android: 3.01D.xxVOS3: 01.xx.xx: 31 Dec 2025,Android: 3.01D.xx: 31 Dec 2025,Vault: SPFW_01.04.xx.xx: 31 Dec 2025,VOS3: 02.xx.xx: 31 Dec 2025,Android: 3.00D.xx: 31 Dec 2024,Vault: SPBL_01.01.xx.xx: 31 Dec 2024,Vault: SPFW_01.01.xx.xx: 31 Dec 2024,Vault: APFW_01.01.xx.xx: 31 Dec 2024,Vault: SPBL_01.02.xx.xx: 31 Dec 2024,Vault: SPFW_01.02.xx.xx: 31 Dec 2024,Vault: APFW_01.02.xx.xx: 31 Dec 2024*	Y	Y

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 according to PCI guidelines.

However, best practices we recommend at least monthly and more frequently depending on device setup and transaction volume.

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 according to PCI guidelines.
- However, as part of best practices, we recommend at least monthly and more frequently depending on device setup and transaction volume.
- Any variances in inventory, including missing or substituted POI devices, must be reported to Global Payments 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 using the Global Payments P2PE solution must maintain a current device inventory document, following the instructions below:

1. Prior to implementation, identify or establish a document or electronic system suitable to maintain the present state of all information found in the sample below for all merchant P2PE devices.

    - Some merchants may choose to create a spreadsheet, word processing document, or other electronic file to keep track of this information. Other merchants may wish to use an existing inventory management system to keep track of their devices, but this is not required. As long as the system can be relied upon to keep an accurate status of each POI device in your environment and can be updated to reflect the current values shown in the sample below, it is acceptable for use to meet this requirement.

    - While the inventory must contain device vendor, device model name and number, location, status, and serial number or other unique identifier for each device, merchant may optionally choose to maintain additional information about the device, such as inspection results (see Section 6.1), store number, device condition, firmware version, hardware version, any physical connectors and their condition, and individuals/job functions authorized to access to the device ("authorized personnel").

    - The "serial number or other unique identifier" value may be either the serial number imprinted on the label affixed to the bottom of the device or another unique ID. Any alternate unique ID must be reliable to positively identify the device, and not easily counterfeited, such as a tamper-evident asset tag or RFID value. For most merchants, tracking using the manufacturer's serial number is the best choice.

2. Prior to implementation, upon device status or location change, and at least annually thereafter, reconcile all devices against the inventory spreadsheet, making note of any discrepancies.

    - This process may be combined with the inspection process outlined in Section 6.1, or performed separately.

    - If an inventory discrepancy is detected (such as a missing or substituted device), the merchant must immediately contact the Customer Care team using the contact information found in Section 1.2.

    - It is recommended, although not required, to employ the inventory document for reference when performing inspection (see Section 6.1) to help aid in detection of unauthorized removal or substitution of devices.

3. Save a copy of your inventory each year to reflect the state of your devices at that time, which may also be provided as evidence for your annual assessment.

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 2.1 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 or attempting to change device configurations or settings will invalidate the PCI-approved P2PE solution in its entirety.

Examples include, but are not limited to:

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

4.1 Installation and connection instructions

For any questions on installation or connection for your devices please go to https://help.globalpay.com/en-ca for installation instructions for your device or contact your POS provider. *Please note that the URL above will change depending on where documents are stored.*

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

The following guidance may assist merchants in selecting the appropriate installation or storage locations for POI devices in order to ensure proper protection of the device:

- When choosing an installation position, consider that the device should be positioned such that the public has easy access to the screen, PIN pad, and card interfaces in order to complete a transaction. Where possible, it is recommended to reduce public access to the bottom or rear of the device.
- Devices should be located where it can be easily and frequently observed by authorized personnel. This will also aid in performing periodic inspections (see Section 6.1).
- Devices should be located with ample lighting to improve operation and deter theft or unauthorized manipulation.
- Device PIN pad should be positioned in such a way that any video monitoring or third-party visual observation is restricted. Use of approved PIN guards is recommended to ensure only the consumer can observe the entry of sensitive data.
- Personnel access to and use of the device should be restricted to individuals based on job function.

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

Methods used to prevent unauthorized removal or substitutions depend upon whether the device will be securely mounted or maintained under operator supervision. Attended devices may be either mounted or unmounted as described below. However, devices intended for unattended use must be securely mounted.

- If mounted, the POI device should be installed in accordance with the terminal manufacturer's approved installation instructions.
    - For mounted devices for which the manufacturer has not provided approved installation instructions, merchants should select and install mounting hardware that provides customers access to the card, display, and PIN entry interfaces without modifying the case of the POI device, placing stress on device seams, or removing any screws.
    - The device should be secured such that it may not be easily or quickly removed and/or substituted by unauthorized individuals.
- If the merchant chooses not to mount the device (e.g., for mobile or attended countertop operation), or chooses to use a non-permanent mount (e.g., Velcro, dock, quick-release tension mount), the POI should be maintained under operator supervision, ensuring additional care is taken to prevent removal or substitution. These precautions must include:
    - Limiting access to the device to authorized personnel only. Note: This requirement does not prevent the merchant from passing the device to the customer for card insertion, card swipe, or PIN entry, however the authorized personnel should observe the operation of the device to prevent removal or substitution.
    - When not in use, the device should be securely mounted (see above) or stored in a secure location accessible only to authorized personnel.

5- POI Device Transit

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

From time to time a merchant may need to ship POI devices. Examples of such shipments may include transferring devices between merchant locations or return of devices to the authorized repair location. Merchants are responsible to secure devices during transit by using the following protections:

- Shipping must use reputable courier service, such as a private courier, US postal service, or public shipping company (e.g., FedEx, UPS, DHL).
- Courier must provide merchant with unique tracking details and shipment status.
- Recipients must be provided with notification of shipment including tracking details.

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

Devices should only be shipped to or received from Global Payments authorized distributors and trusted repair centers. Global Payments uses the following trusted deployment facilities to distribute devices and provide repair services.

- When preparing to ship, the merchant should verify that POI devices are shipped to the following trusted locations:
- Upon receipt, the merchant should verify that POI devices originated only from the following trusted locations.

Refer to section 2.1 for the list of trusted deployment centers.

If a device is received from a location not listed above, merchants should contact Customer Care (see Section 1.2 for contact information) to verify the device's authorization and authenticity, and arrange for replacement of the device, if applicable. The device should not be used unless it has been verified to be an authentic device from an authorized source.

Devices should be inspected upon receipt following the instructions found in Section 6.1.

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 terminals can be found in the document entitled Skimming Prevention: Best Practices for Merchants, available at www.pcisecuritystandards.org.

- Purpose: It is important to inspect Inspection should include identification of unauthorized removal, tampering, substitution of devices or suspicious activity. The inspection should be a validation of the inventory identifiers to the physical device and include inspection to ensure that the condition of the device can detect tampering. Potential indicators of tampering could include security seals removed or damaged, damage of the actual device or additional connections than expected. If a discrepancy occurs within the inspection of the inventory (such as a missing or substituted device) or there is identification of suspicious activity (such as device tampering), follow guidance in Section 6.2 immediately.
- Frequency: PCI dictates that physical POI inspections are conducted periodically (at least annually). To limit risk, Global Payments strongly recommends inspecting monthly, at a minimum. Depending on the transaction volume for the merchant and placement of the devices, inspections should be done more frequently (weekly or daily).
- Physical Inspection Guidance: The PCI guidance on monitoring, Skimming Prevention: Best Practices for Merchants may be found in the Document Library on the pcisecuritystandards.org website and provides a full list of best practices for visual inspection. The following guidance is provided by Global Payments to aid in basic inspection of the P2PE POI devices for use of the Global Payments P2PE solution:
    - **Tamper Evident Security Seals:**
        - Review the reference photographs found in Appendix A to aid in identifying the placement of seals based on device model and recognizing the appearance of tampered seals.
        - During physical inspection, check for the existence and integrity of all tamper seals.

- Placement of seals may vary by device and manufacturer and are typically found over a seam or screw. These seals are intended to help prevent incidental access to sensitive areas of the device, and easily identify potential tampering if they are removed, broken, or modified.

- **Screws and Seams:**
  - Review the reference photographs found in Appendix A to aid in identifying the location and appearance of screws and seams based on device model, and in recognizing the appearance of removed screws or modified seams.
  - Validate that all visible screws are in place and that the area near the screws show no signs of attempted entry (e.g., scraping, plastic shavings).
  - Observe the seams and ensure that there is no lifting of the seam that may allow a user access to the internal components of the device, or the presence of markings to indicate prying along the seams. All seals on the seams should be in place without tearing or breaking.
- **Visual Examination of the Device:**
  - Review the reference photographs found in Appendix A to aid in becoming familiar with the normal appearance of the card swipe and chip reader slots, keypad, and case/housing for the specific device model, and recognizing alterations such as insert skimmers, PIN pad overlays, modifications to the housing, or device substitution.
  - Visually inspect the card swipe and chip reader slots for evidence of tamper, including extraneous wiring, holes, or foreign material inserted into the slots.
  - Visually inspect the pin pad for evidence of tamper, including extraneous wiring, holes, or overlay covering the screen or keypad.
  - Visually inspect the external case/housing to evaluate for signs of damage, scraping, holes, or other alteration which may signify prying, modification, application of overlay, or insertion of skimming device. Inspect for any signs that the equipment itself does not match the factory design (e.g., change in color, shape, size).
- **Connections:**
  - During physical inspection, ensure there are no additional cables, wires or cords attached to the terminal, which may indicate the presence of a skimming device.
- **Mount**
  - Reference Section 4.3 for guidance on securing deployed devices.
  - If the device is permanently mounted, inspect mounting hardware to ensure the device is securely fastened, and cannot be easily removed.
  - If the device is unmounted, confirm that device is stored in a secure location when not in use, with access limited to authorized personnel only.

- **Monitoring:**
    - Attended devices should be monitored by personnel, as described in Section 4.3.
    - Unattended devices must be securely mounted and monitored to prevent tampering or substitution. Acceptable controls to monitor devices include video surveillance, or active tamper alerting system which provides electronic notification to personnel if an attempt is made to remove the device. During physical inspection, device monitoring control(s) should also be inspected for proper function and calibration.

- **Inventory Updates:** In the event of device status change identified during inspection, the POI inventory must be updated. See Section 3.3 for instructions on maintaining POI inventory.
- **Training:** Personnel performing the inspection function should be familiar with the guidance above. This PIM should be made available to all staff performing this function as official guidance for performing inspections. However, it is also acceptable to provide merchant-specific instructions or procedures that meet the guidance above (e.g., as part of existing training materials), to ensure full integration of P2PE POI inspection procedures with existing merchant processes.

6.2 Instructions for responding to evidence of POI device tampering

If at any time it has been identified that a device has been tampered, through the inspection process during inventory, or during normal operation or storage, the merchant must notify the Customer Care team and discontinue deployment and/or use of the device. When contacting Customer Care, be prepared to confirm the device manufacturer, model, and serial number. See Section 1.2 for Customer Care contact information.

Any device that has been identified to have been tampered must not be deployed or remain connected for running transactions. If currently in use, the merchant must remove it from service immediately.

Inventory checklist should be updated by the merchant to reflect the device being returned after physical inspection failure.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures
Any device failure involving encryption, keys, or other cryptographic function must be addressed immediately. Under no circumstances should a merchant continue processing transactions if they suspect a device encryption failure has occurred. **Follow these steps to resolve the issue:** 1. Discontinue use of the device immediately and write down the error message or details that help to demonstrate that an encryption failure has occurred. 2. Contact Customer Care using the contact information found in Section 1.2. 3. Customer Care will troubleshoot the issue. 4. If the issue can be resolved such that normal encrypting device functions are fully restored, Customer Care may provide authorization to continue use of the device. 5. If the issue must be resolved through device repair, Customer Care will generate a return tag, which will be sent to the merchant to facilitate the return. 6. If the issue is not fully resolved, the merchant may not re-enable the device. Merchants who do not wish to continue use of the P2PE solution may choose to opt-out following the opt-out instructions in Section 9.1

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device
1. If a device is unable to authenticate or unable to transact, communicating an error code, please contact the Customer Care team using contact information found in Section 1.2. 2. If the Customer Care team is unable to resolve the issue, it may be resolved by requesting a replacement device. This will be completed by the Customer Care team by generating a return tag to be distributed to the merchant to return the device to the approved deployment facility via a trusted courier. Likewise, the Customer Care team will request a new device be sent to the merchant; then, the merchant should follow the normalized intake process as described previously with appropriate inventory controls.

9. Additional Guidance

9.1 Additional pertinent guidance for merchants regarding the P2PE solution
Instructions for formally requesting of the P2PE solution provider that P2PE encryption of account data be stopped
Understanding the PCI DSS implications, should a merchant determine they no longer desire to participate in the PCI P2PE program (e.g., due to device encryption failure or other business constraint), they will need to contact the Customer Care team. The merchant will be required to complete an opt-out form provided by Global Payments, indicating that they understand the security and compliance implications incurred by opting out, including additional PCI DSS controls, ineligibility for the SAQ P2PE, necessary notification to acquiring banks, and impact to PCI DSS compliance validation. The merchant has the responsibility to address all applicable requirements and must communicate this written form to Customer Care (options for delivering this form will be discussed upon contact with the Customer Care team). Global Payments will work with the merchant to perform the demotion of the terminal from P2PE, or the generation of a return tag to replace the device using a trusted courier to an approved deployment facility.

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices
As the instructions for confirming hardware, firmware, and application versions of POI devices vary by device, please refer to your POI device manufacturer or reseller for instructions on confirming this information.

Appendix A – POI Reference Photographs

The following illustrations should be used during physical inspection to confirm physical appearance of the POI device(s). See Section 5.1.

<table>
<tr><th colspan="2">T650C</th></tr>
<tr><td> 

Front</td><td> 
Back</td></tr>
<tr><td> 
Left Side</td><td> 
Right Side</td></tr>
</table>

T650P	
 Front	 Back
 Left Side	 Right Side

globalpayments

P630	
 Front	 Back
 Left Side	 Right Side

globalpayments