

First Data
is now **fiserv.**



Point-to-Point Encryption (P2PE)
Instruction Manual
ID Tech SREDKey 2
Version 1.0



1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	First Data TransArmor P2PE Solution – 3DES
Solution reference number per PCI SSC website:	2018-00541.002

1.2 Solution Provider Contact Information

Company name:	First Data Merchant Services
Company address:	5565 Glenridge Connector, Atlanta, GA 30342
Company URL:	www.fiserv.com
Contact name:	Marco Mabante
Contact phone number:	(912) 484-6660
Contact e-mail address:	TransArmorP2PE@Fiserv.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.

ID TECH terminals used as part of the First Data TransArmor P2PE Solution can only be deployed by First Data Hardware Services or ID TECH.

Do not purchase any ID TECH devices online or from a Key Injection Facility (KIF) that is not a Component of the TransArmor P2PE Solution. You may use PCI Qualified Integrator Resellers to install and activate ID TECH Point of Interaction (POI) devices. To request a Return Merchandise Authorization (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

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

Carefully inspect the shipping carton and its Tamper Evident packaging for damage. If the Tamper Evident packaging is damaged DO NOT put the device into service and immediately contact First Data or ID TECH Customer Support to report.



Inspect the Tamper Evident packaging to ensure no damage or an attempt made to reseal the package with clear tape.

- Photograph and retain pictures of the package (damaged or not).
- Confirm the serial number(s) of the devices against the serial numbers listed on the Advance Ship Notice (ASN) you should have received from First Data Hardware Services (FDHS) or ID TECH prior to receipt of the shipment.

NOTE: If serial numbers do not match do not put device into service and contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com
- Remove the contents from the box. The box contains the following items:
 - a. SREDKey 2 device
 - b. USB Cable
 - c. QuickStart Guide
- We recommend saving the carton and packing material for repackaging or moving the device in the future.

The following is an example of content inside the box:



Cables and power supply can be shipped separately specifically to suit the connectivity requirements of the merchant.

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

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.

First Data does not contract with any third-party personnel to install, troubleshoot, or repair any ID TECH devices.

Merchants may use PCI Qualified Integrator Resellers (QIR) to install their devices using this P2PE Implementation Manual. Below is a link to PCI Certified QIR's:

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.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.

IMPORTANT NOTE: PCI-listed P2PE solutions (and applicable P2PE components) are allowed to revalidate and reassess their existing PCI P2PE approval with expired PTS POI devices for up to, but not exceeding, 5 years past the PTS POI device expiry dates (as listed on the PCI Approved PTS Devices list) for the POI device types used in the solution. In the case of the ID Tech SREDKey 2 the PCI PTS expiry date is April 30, 2026. This means you could use the device until April 30, 2031. Be aware that the hardware manufacturer may end support for the device earlier than April 30, 2031.

All POI device information can be verified by visiting:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See 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):
4-90075	ID Tech	SREDKey 2	80172001(With MSR) 80172002(Without MSR) 80172004(With MSR) 80172005(Without MSR)	SREDKEY2 FW v1.00.xxx.xxxx.S SREDKEY2 FW v1.01.xxx.xxxx.S

<Add additional rows for each PTS POI approval listing with all the POI device types associated with that listing used in this solution, as applicable>

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.

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	ID Tech	SREDKey 2	Hardware # 80172001(With MSR) 80172002(Without MSR)	No	No

3.2 POI Software/Application Details

			<p><i>MSR)</i> <i>80172004(With</i> <i>MSR)</i> <i>80172005(Without</i> <i>MSR)</i></p> <p>Firmware #</p> <p><i>SREDKEY2 FW</i> <i>v1.00.xxx.xxxx.S</i> <i>SREDKey2 FW</i> <i>v1.01.xxx.xxxx.S</i></p>		
--	--	--	---	--	--

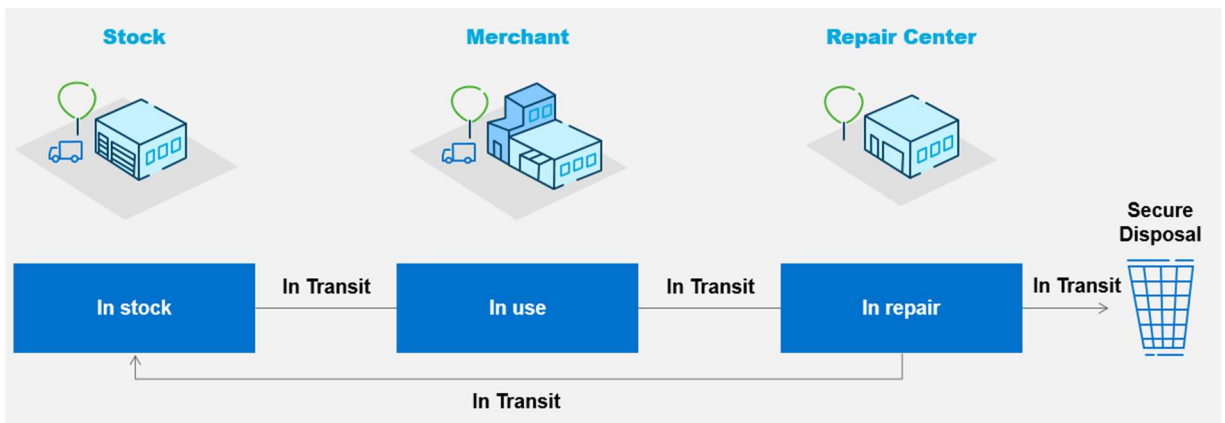
<Add additional rows for each application on a POI device used in this solution, as applicable>

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 *First Data* 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.

In order to maintain PCI P2PE compliance it is the Merchant's responsibility to keep track of all devices and regularly manage their inventory at the minimum of once per year. Merchants must track their POI devices for the following states:

- In secure storage awaiting deployment
- Deployed/In Service
- Disabled / Out for repair
- Decommissioned and returned for secure destruction
- In transit



POI's held in storage awaiting deployment or for repair should be stored in a secure area that restricts access to authorized personnel only. In addition to the above states, the Merchant will also need to track the following items to ensure their POI's have not been tampered with:

- Physical connections to POI's
- Hardware and Firmware versions on POI's
- Dates and locations of inspections for each POI
- Name of authorized staff that performed the inspections

Below is the URL that will provide detailed instructions on reviewing Hardware and Firmware versions:

- https://www.pcisecuritystandards.org/ptsdocs/4-90075IDTech_-_PCI-PTS_POI_Security_Policy_-SREDKey2_20200311-1584738052.10652.pdf

Merchants may use an Inventory tracking spreadsheet to keep track of all their devices similar to this sample 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

This section describes how to install the SREDKey 2 device.

Please follow the instructions in the ID TECH Quick Setup Guide:

- [Downloads - Home - Knowledge Base - IDTECH - Confluence \(idtechproducts.com\)](https://idtechproducts.com/knowledge-base/downloads-home)
- Load payment application on host computer
- Connect the SREDKey 2 USB cable to the host computer
- On connection the SREDKey 2 powers on
- The SREDKey 2 is ready for use

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

Checking the Installation Site

1. Ensure that there are NO security cameras focusing on the device.
2. Ensure that there are NO objects close by in which cameras could be hidden.
3. Ensure that the device CANNOT be observed from outside (any window or door) during PIN entry.

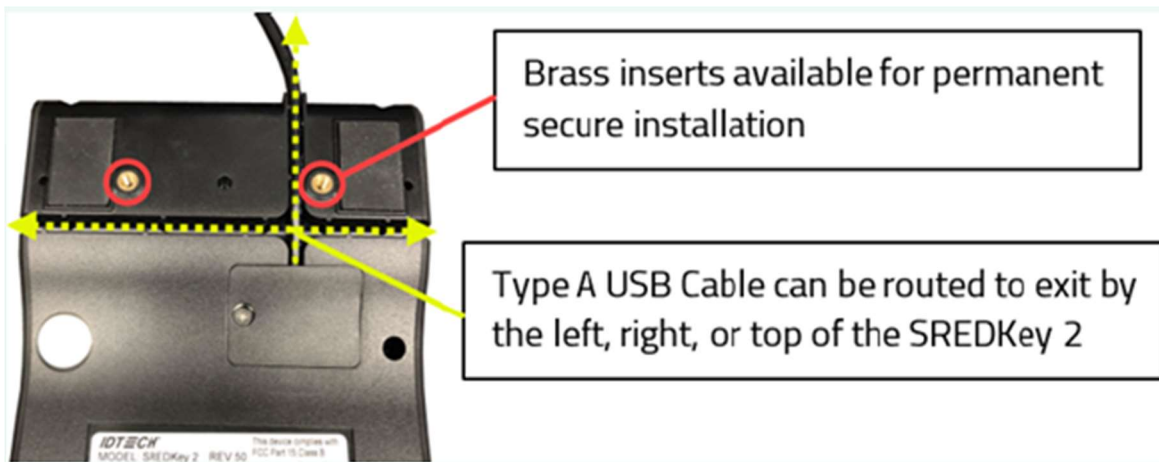
When considering the prevention of theft once the device is installed, it is necessary to strike a balance between securing the asset and damaging usability and therefore, customer service. You should select a location for your POI that is secure, accessible by customers and always visible to staff.

It may be possible to attach the device to your payment station in such a way that prevents it being stolen but this will not necessarily deter the fraudulent engineer or collusive member of staff.

Therefore the physical location of the device and security of components should be considered. Can it be removed easily; are components hard wired together or physically protected to prevent easy tampering or theft?

Devices should always be placed in a location that allows the customer to use them in a manner that obscures their PIN entry from other customers and where practical should include PIN shielding. Secure mounts should be used to minimize opportunities for theft but care must be taken to balance security needs with the requirements of the Americans with Disabilities Act (ADA).

SREDKey 2 can be securely mounted by using the brass inserts shown below



Where the needs of the ADA can be met with the device in a mounting bracket, consideration should be given to modifying the bracket from a 'support only' mechanism to one that physically restrains the device reducing the potential for a 'smash and grab' type theft.

Where locking the device into the mounting bracket would contravene the ADA, consideration should be given to connecting a security wire cable to the device and the mounting bracket so giving a degree of movement but maintaining security against theft.

You should ensure that you treat your SREDKey 2 as you do your cash till and make sure that it is safe and secure. It is the merchants' responsibility to ensure the devices are secure at all times.

- Do not place the SREDKey 2 device on a PC monitor, adjacent to an electronically active security tag deactivation system, or near other sources of magnetic fields. The SREDKey 2 device must be at least 12 inches away from an electronically active type of security tag deactivation pad. This is specifically defined as:
 - An electronically active system that sends out a powerful and potentially disruptive signal to deactivate the security tag. If the SREDKey 2 device is placed too close to the system's pad or placed too close above the pad, malfunction may occur.
- ***When selecting the device location, keep in mind that you must perform daily tasks to ensure the security and compliance of your device. Refer to section 6 POI Device Tamper Monitoring and Skimming Prevention for more information.***

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

Devices should be examined daily to check for suspicious attachments and any signs that they have been altered or interfered with. It is the merchants' responsibility to check the devices for any interference, unsecure devices, or scanning devices.

For POI devices located in areas away from merchant personnel, mechanism should be in place to ensure that suspicious attachments or alterations are found and investigated. It is the merchants' responsibility to ensure the devices are checked regularly for the following items:

- Physical connections to POI's
- Hardware and Firmware versions on POI's
- Dates and locations of inspections for each POI
- Name of authorized staff that performed the inspections

You should also perform the following for devices that cannot be secured:

- Secure devices in a locked room, drawer or cabinet when not in use.
- Assign responsibility to specific individuals when device is in use.
- Observe devices at all times.
- Sign devices in/out, etc.

For lost or stolen devices:

How do I report a stolen device?

You can report a device as stolen to one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

5. POI Device Transit

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

Each party involved in organizing the shipping should follow these security requirements:

- Ensure that devices are sealed with tamper-proof tape prior to shipment and during shipping process. This can be obtained at an office supply store
- Wherever the device is stored, it should be secured in an access-controlled area with sealed tamper-proof packaging
- Shipments are transported using Customs-Trade Partnership Against Terrorism (C-TPAT) approved common carriers such as FedEx, UPS or DHL
- Advance Ship Notice (ASN) including device serial numbers shall be provided

to the receiving company at time of physical shipment via electronic method

- Receiving company should always verify physical receipt (part number, serial numbers, qty, etc.) with separately provided ASN information to ensure no en-route tampering
- Tracking number must be provided to track shipment status including locations at any given time
- Inspection should be conducted upon receiving the device (see Section 2.2 for instructions). If the device is tampered, it must be returned

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

ID TECH terminals used as part of the First Data TransArmor P2PE Solution can only be deployed by First Data Hardware Services or ID TECH.

Do not purchase any ID TECH devices online or from an unauthorized P2PE Solution Provider KIF. Only use PCI Qualified Integrator Resellers to install and activate ID TECH POI devices. To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

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

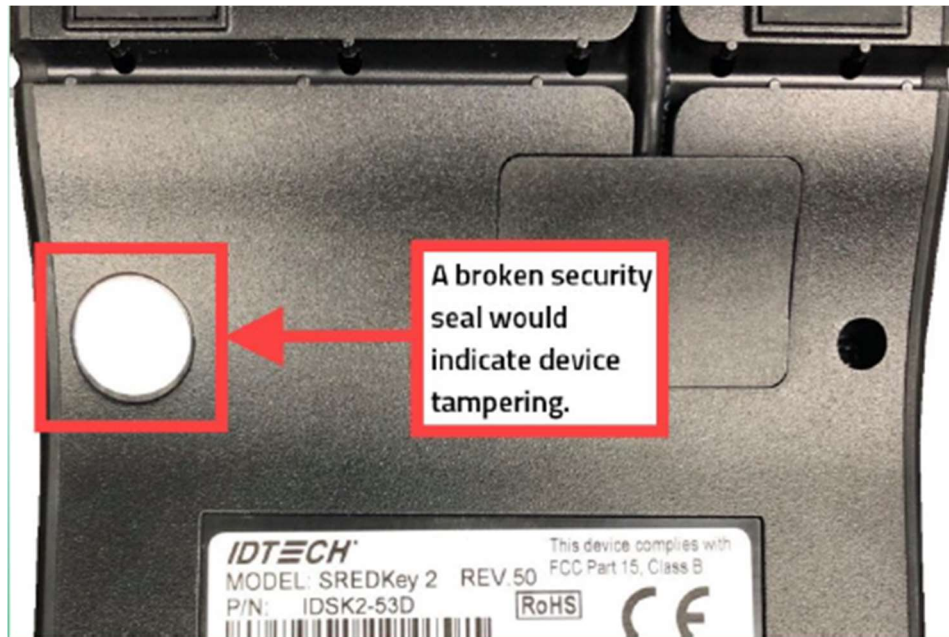
Additional guidance for inspecting POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants*, available at www.pcisecuritystandards.org.

Perform the following tasks daily to ensure the security and compliance of your device:

Ensure that no attempts have been made to tamper with the device, using the following method:

1. Check that there is NO external damage to the device, particularly around the keypad, display, and reader areas.
2. Check that the keypad is firmly in place.
3. Ensure that there are NO additional cables protruding from the device or associated equipment.

4. Check that there are NO holes drilled into the device's housing.
5. No changes to the resistance when swiping a card through the magnetic stripe reader.



Ensure that this warranty label has not been removed

Inspect the MSR slot for obstructions and alterations



Inspect for case modifications, new stickers covering holes or signs of case separation




6.2 Instructions for responding to evidence of POI device tampering

The SREDKey 2 device detects any “tampered state”. In this state the PIN pad will repeatedly flash the message **“Tampered”**, beep and further use of the PIN pad will not be possible.



SREDKey 2 also has a LED's that changes color to show the following states:

SREDKey 2 units have an LED below the LCD screen that indicates device status.

Device State	
Active/Ready	
Tampered	 flashing
Missing Transaction Key	



Check with your device integrator if the LED is red or amber.

If you observe the **"Tampered"** message, you should contact one of the following immediately:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

What does it mean if my device has been tampered?

This can happen for a number of reasons, such as a credit card skimmer is applied to the device or someone has attempted to break the device open. This can also happen if the device is dropped hard enough during shipment or by the merchant or a customer.

What should I do if my device has been tampered?

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

If First Data has contacted the Merchant to inform them of encryption errors, OR the merchant experiences a **"Tampered"** alert the POI must be taken out of service immediately and replaced.

To request a swap (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

This section covers basic troubleshooting.

To request a return (RMA) for a POI that has been tampered with or defective, please contact 1 of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

Magnetic Card Reader Does Not Work Properly

1. Slide the card through the magnetic stripe reader
2. Swipe the card at a faster or slower steady speed.
3. Swipe the card in a different direction.
4. Inspect the magnetic stripe on the card to make sure it is not scratched or badly worn.
5. To determine if the problem is with the card:
 - a. If your host device has a magnetic stripe reader, try swiping the card there.
 - b. If you have another working SREDKey 2 device, try swiping the card there.
6. If there is still a problem, contact your internal Help Desk.

No Information is Visible on Screen

7. Make sure the SREDKey 2 cable is fully inserted and secured into the device.
8. Restart the device.
9. If you have another working SREDKey 2 device, swap the devices to determine if the problem is with the device, cable, POS, or power supply.

10. Replace the cable.
11. Reset the host by turning it off and back on again.

Checking the Device's Integrity

Ensure that no attempts have been made to tamper with the device, using the following method:

12. Check that there is NO external damage to the device, particularly around the keypad, display, and reader areas.
13. Check that the keypad is firmly in place.
14. Ensure that there are NO additional cables protruding from the device or associated equipment.
15. Check that there are NO holes drilled into the device's housing.

PED Tampered

The SREDKey 2 device detects any "tampered state". In this state the PIN pad will repeatedly flash the message "**Tampered**" and further use of the PIN pad will not be possible. If you observe the "**Tampered**" message, you should contact one of the following immediately:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

9. Additional Guidance

9.1 Additional Solution Provider Information

What should I do if I do not find the answer to my question or want to leave feedback?

Please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@Fiserv.com
- ID TECH Technical Support: (714) 761-6368 or support@idtechproducts.com

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

Below is the URL that will provide detailed instructions on reviewing Hardware and Firmware versions:

- [https://www.pcisecuritystandards.org/ptsdocs/4-90075IDTech - PCI-PTS POI Security Policy -SREDKey2_20200311-1584738052.10652.pdf](https://www.pcisecuritystandards.org/ptsdocs/4-90075IDTech_-_PCI-PTS_POI_Security_Policy_-SREDKey2_20200311-1584738052.10652.pdf)