P2PE Instruction Manual (PIM)

A Merchant Guide for Deploying and Maintaining the FreedomPay® P2PE Scope-Reduction Solution

Version 3.3

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	*FreedomPay Commerce Platform P2PE*
Solution reference number per PCI SSC website:	2025-00909.016

1.2 Solution Provider Contact Information	
Company name:	*FreedomPay, Inc.*
Company address:	*FMC Tower at Cira Centre South* *2929 Walnut Street · Floor 14* *Philadelphia, PA 19104*
Company URL:	*http://corporate.freedompay.com*
Contact name:	*Matthew J. Donnelly*
Contact phone number:	*+1-888-495-2446*
Contact e-mail address:	*compliance@freedompay.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.

FreedomPay or its certified KIF will email a pre-shipment notification to the merchant identifying the POI device serial numbers, the Trusted Courier name, the tracking number, the Approved Supplier Facility from which the package was shipped, and the Approved Merchant Location to which the package was shipped.

Upon receipt of any POI device shipment, the Merchant must:

i. Inspect the packaging as set forth above.
ii. Verify that the courier identified on the delivery receipt is a Trusted Courier.
iii. Verify that the package was sent from an Approved Supplier Facility listed below:

a. FreedomPay Headquarters
2929 Walnut Street
Floor 14
Philadelphia, PA 19104

b. ScanSource
8650 Commerce Drive, Suite 100
Southaven, MS 38671

c. Ingenico Repair Facility
4020 Steve Reynolds Blvd
Norcross, GA 30093

d. Ingenico Headquarters
3025 Windward Plaza
Suite 600
Alpharetta, GA 30005

e. Brookfield Equinox / Expeditors International of Washington, Inc.
1621 W. Calle Plata Suite B
Nogales, AZ 85621

f. Equinox
9045 E. Pima Center Parkway
Suite 3
Scottsdale, AZ 85258

g. Ingenico Distribution Center
6430 Shiloh Road E, Suite B
Alpharetta, GA 30005

h. Ingenico Warranty and Service Center
6190 Shiloh Crossing, Suite B
Alpharetta, GA, 30005

i. POS Portal
1627 Main Ave.
Sacramento, CA 95838

J. Pos Portal
1920 Watterson Trail Suite A
Louisville, KY 40299

k. Maxwell Paper
435 College Street East
Belleville, ON K8N 5S7
Canada

l. Ingenico UK
17 Ridge Way
Donibristle Industrial Park
Dalgety Bay, Fife KY119JU
United Kingdom

m. First Data Hardware Services
1169 Canton Road
Marietta, GA 30066

n. First Data Hardware Services
205 Export Blvd
Mississauga, ON L5S 1Y4

o. ID Tech US KIF
10721 Walker Street
Cypress, CA 90630

P. ID Tech TW_KIF
32F, 1080 Zhongsheng Road
Taoyuan District, Taoyuan City, Taiwan, R.O.C.

q. Ingenico KIF Italia
Via Giorgio Stephenson 43/A
20157 Milano
Italia

r. CTDI Milton Keynes Ltd
Featherstone Rd,
Wolverton Mill,
Wolverton,
Milton Keynes
MK12 5TH,
United Kingdom

s. CTDI Soemmerda GmbH
Erfurter Höhe 10A
99610 Sömmerda
Germany

t. Zonal Retail Data Systems
Celestra, 1-5 James Way,
Bletchley, Milton Keynes MK1 1SU, United Kingdom
MK1 1SU

u. Zonal Retail Data Systems Ltd
4 Hutton Square
Brucefield Industrial Estate
Livingston EH54 9DJ

v. The Phoenix Group US
6705 Keaton Corporate Pkwy
O'Fallon, MO 63368

w. The Phoenix Group Canada
9-2785 Skymark Ave
Mississauga, ON L4W 4Y3

iv. Verify that the serial numbers on the shipping statement match the serial numbers in the pre-shipment email notification.

v. Update the device record-keeping system to reflect the change in device status and location.

The merchant must immediately return to FreedomPay, as set forth below, any POI device package that appears to have been tampered with, was delivered by anyone other than a Trusted Courier, or was sent from any location other than an Approved Supplier Facility.

Prior to returning a POI device to an Approved Supplier Facility, the merchant must email poidevicereturns@freedompay.com34T to determine where the device should be shipped based on the situation.

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

Upon receiving a FreedomPay POI device, merchants should, at a minimum:

- Verify that the courier identified on the delivery receipt is a Trusted Courier.
- Verify that the package was sent from an Approved Supplier Facility.
- Verify that the serial numbers on the shipping statement match the serial numbers in the pre-shipment email notification.
- Verify the packaging is not damaged to the point of exposing the inside of the package.
- Verify the packaging has not gotten wet to the point that moisture has penetrated the packaging walls.
- Verify that the integrity of the tamper evident packaging is intact.

Example of an untampered package with tamper evident tape:

If the device or packaging fails any of the above inspections, contact your FreedomPay representative and return the device as outlined in Section 5.2.

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.

In most instances, FreedomPay will be able to provide device support remotely without requiring on-site assistance. During complex installations or certain support cases, however, a technician may be dispatched to a merchant location. In the event a FreedomPay technician is needed on-site, ensure the following steps are taken before, during, and after on-site work takes place.

i. A field technician will be assigned to a case and complete a dispatch request.
ii. Once a technician has been assigned, FreedomPay will provide the merchant with details of the request.
iii. When the technician arrives on-site, and before allowing access to the POI device, the merchant should verify the technician's identity as a FreedomPay employee or contractor. All other personnel must be denied access without proper validation of their identity.
iv. Once the technician's identity has been verified, the merchant should assign an escort to monitor the technician's activity at all times.
v. Once the technician has completed the work, the merchant must respond to the dispatch email with the following details:
    i. Form of ID presented for verification
    ii. Time spent at location
    iii. (For support cases only) Serial number(s) of terminal(s) touched by the technician

FreedomPay will never send technicians on-site without coordinating with merchant contacts beforehand and providing information on the technician being dispatched for verification purposes. Anyone claiming to be a repair/support technician without the proper notification or identification should not be provided access to POI devices.

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.

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):
4-20324	Ingenico	*Lane/5000*	LAN51BA (single MSR head), LAN51CA (dual MSR head), LAN51DA (single MSR head and camera), LAN51EA (dual MSR head and camera)	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820555v01.xx (SRED AWL)
4-30257	Ingenico	*Lane/8000*	LAN80AA	820547v01.xx
4-30326	Ingenico	*Link/2500*	LIN25AA (Basic version no CTLS support), LIN25BA (Basic version with CTLS), LIN25CA (Companion version no CTLS support), LIN25DA (Companion version with CTLS), LIN25EA (Touch version no CTLS support), LIN25FA (Touch version with CTLS), LIN25GA (Dual head version no CTLS support), LIN25HA (Dual head version with CTLS), LIN25IA (Companion version with rear connector and no CTLS support), LIN25JA (Companion version with rear connector and with CTLS)	820547v01.xx
4-30237	Ingenico	*Lane/7000*	LAN70AA, LAN70AB	820547v01.xx
4-20316	Ingenico	*Move/5000*	(CTLS + Privacy shield) (CTLS) (Non CTLS + Privacy shield) (Non CTLS) MOV50AB, MOV50BB, MOV50CB, MOV50DB, MOV50JB (CTLS + Privacy shield + Desktop case lid)	820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)

4-30310	Ingenico	*Lane/3000*	LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA	820547v01.xx, 820561v01.xx (base firmware)
4-20317	Ingenico	*DESK/5000*	(CTLS) (Non CTLS + Privacy Shield) (Non CTLS) DES50AB, DES50BB, DES50CB, DES50DB(CTLS + Privacy Shield)	820376v01.xx, 820547v01.xx (Core Firmware), 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)
4-30365	Ingenico	*Moby/5500*	MOB55xBxAx	BOOT: xxxx-F-801-01xx-xxxx-xx, CTRL: xxxx-F-802-01xx-xxxx-xx
4-30263	Ingenico	*Moby/8500*	MOB85AAx (w/o CTLS), MOB85ABx (w/o CTLS), MOB85ACx (w/o CTLS), MOB85BAx (w/ CTLS), MOB85BBx (w/ CTLS), MOB85BCx (w/ CTLS)	Boot: xxxx-F-701-01xx-xxxx-xx, Boot: xxxx-F-701-02xx-xxxx-xx, Boot: xxxx-F-701-03xx-xxxx-xx, Ctrl: xxxx-F-702-01xx-xxxx-xx, Ctrl: xxxx-F-702-02xx-xxxx-xx, Ctrl: xxxx-F-702-03xx-xxxx-xx, Ctrl: xxxx-F-702-04xx-xxxx-xx
4-30481	Ingenico	*Lane/3600*	LAN36AA2-xxxx, LAN36AB2-xxxx, LAN36BA1-xxxx, LAN36BA2-xxxx, LAN36CA1-xxxx, LAN36CA2-xxxx, LAN36CB2-xxxx, LAN36DA1-xxxx, LAN36DA2-xxxx, LAN36DB2-xxxx, LAN36EA2-xxxx, LAN36FA2-xxxx, LAN36AA1-xxxx	820571v01.xx (Core Firmware, 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820570V07.xx (Open Protocols), 820565V01.xx (SRED FF1)
4-30381	Ingenico	*Self/2000*	SEL20AA	820566v01.xx
4-30393	Ingenico	*Self/4000*	SEL40BA	820547v01.xx
4-30384	Ingenico	*Self/5000*	SEL50CA	820566v01.xx

4-30510	Ingenico	*Self/3000*	SEL30BA1-xxxx SEL30BA2-xxxx SEL30AA1-xxxx SEL30AA2-xxxx	820571v01.xx (Base Firmware), 820376v12.xx (Security services), 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820565v01.xx (SRED FF1)
4-30535	Ingenico	*Self/4000 LE*	SEL41AA1-xxxx	820571v01.xx (Core Firmware), 820376v12.xx (Security Services), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)
4-30532	Ingenico	*Self/5000 LE*	SEL51AA1-xxxx	820573v01.xx (Core Firmware), 820376v12.xx (Security Services), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)
4-20359	Ingenico	*Move/5000*	MOV50BR (CTLS)	820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (Core Firmware), 820376v12.xx (Security Services)

4-30494	Ingenico	*Lane/7000*	LAN70BD	820547v11.xx (Core Firmware), 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820565V01.xx (SRED FF1), 820548V07.xx (Open Protocols), 820572V01.xx (Tetra JVM Addon), 820376v14.xx (Security Services)
4-30493	Ingenico	*Lane/8000*	LAN80BB	820547v11.xx (Core firmware), 820376v12.xx (Security Services), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820548V07.xx (Open Protocols), 820376v14.xx (Security Services)
4-30498	Ingenico	*AXIUM RX7000*	R70411xxxx	02.03.11.xxxxx (The SRED solution supported by firmware includes SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard FPE, SRED OnGuard SDE, SRED FF1)
4-30444	Ingenico	*AXIUM EX8000*	E801x2	01.09.11.xxxxx (with AP Solution 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)
4-30443	Ingenico	*AXIUM DX8000-2, AXIUM DX8000-5*	D851x3 (with AP Solution 1)	01.09.11.xxxxx (with AP Solution 1 SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)

4-30527	Ingenico	*AXIUM RX5000*	R50411xxxx (no pinshield)	02.03.11.xxxxx(The SRED solution supported by firmware includes: SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)
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
4-30432	Infinite Peripherals, Inc	*QuantumPay Reader 250*	06.00.xx.xx	3.0.xx.xx
4-30433	Infinite Peripherals, Inc	*QuantumPay Reader 300*	05.11.xx.xx	3.1.xx.xx, 3.2.xx.xx
4-30437	Infinite Peripherals, Inc	*QuantumPay PIN 400*	00xxxD1xxxxxx (non CTLS version) CLxxxD1xxxxxx (CTLS version)	3.1.xx.xx, 3.2.xx.xx
4-30438	Infinite Peripherals, Inc	*QuantumPay Connected 150*	PRR05xxx PRR15xxx PXR05xxx PXR15xxx	3.0.xx.xx, 3.1.xx.xx
4-30475	Infinite Peripherals, Inc	*QuantumPay Pro Plus*	21.1x.xx.xxx	SP: 3.0.xx.xx, AP: 1.0.xx.xx
4-80037	Castles Technology Co. Ltd	*Saturn 1000-E*	SATURN1000E-HW-V1.20.xxxx	1.1.1.xxxxxx
4-80033	Castles Technology Co. Ltd	*Saturn 1000*	SATURN1000-HW-V1.03.xxxx SATURN1000-HW-V1.01.xxxx SATURN1000-HW-V1.04.xxxx	1.1.2.xxxxxx 1.1.1.xxxxxx
4-30416	Castles Technology Co. Ltd	*Saturn 1000*	SATURN1000-HW-V2.00.xxxx	1.3.1.xxxxxx 1.4.1.xxxxxx
4-80075	Castles Technology Co. Ltd	*S1E2, S1E2-L, S1E2N*	HW-V1.00, S1E2: HW-V1.00	S1E2 & S1E2-L:
4-80094	Castles Technology Co. Ltd	*S1F4 PRO*	HW-V-1G.00	1.6.1.xxxxxx
4-80082	Castles Technology Co. Ltd	*S1P*	HW-V1.00	1.4.1.xxxxxx
4-80092	Castles Technology Co. Ltd	*S1P2*	HW-V-1D.00	1.6.1.xxxxxx

4-80091	Castles Technology Co. Ltd	*S1Mini2*	HW-V-1E.00	1.6.1.xxxxxx
4-30470	Elo Touch Solutions, Inc	*EMC0600, EMC0600C,* *EMC0600SC'* *EMC0600S*	A01.0EC.x A01.0NC.x A01.S00.x A01.SEC.x A01.SNC.x A01.000.x	5.xxx.xxx.xxxx+ap 5.xxx.xxx.xxxx+p 6.xxx.xxx.xxxx+ap 6.xxx.xxx.xxxx+p
4-90136	Ziosk	*Z600*	6.0.A 6.0.B	6201.29.xxxx.xxx.xxx 6201.30.xx.x.xxx
4-90335	Ziosk	*Z600 Pro*	6.0.A	6201.29.xxxx.xxx.xxx
4-30522	Verifone	*M425* *M450*	H625-0007-0090-1xx-xxx-B0 (with privacy shield), H650-0007-0090-0xx-xxx-B0 (without privacy shield), H650-0007-0090-1xx-xxx-B0 (with privacy shield), H625-0007-0090-0xx-xxx-B0 (without privacy shield),	VOS3: 02.xx.xx, SPBL_01.02.xx.xx, SPFW_01.04.xx.xx, APFW_01.02.xx.xx, Android: 3.01D.xx
4-80062	Verifone	*P630*	H565-0007-xxxx-xxx-xxx-A1	Vault: APFW_01.02.xx.xx, VOS3: 01.xx.xx, Android: 3.01D.xx, Vault: SPFW_01.04.xx.xx
4-110000	Verifone	*V660P*	H660-0007-00D0-0Nx-xxx-B1, H660-0007-00D0-0Nx-xxx-B0	Vault: SPFW_01.06.xx.xx, Vault: APFW_01.03.xx.xx, Vault: SPFW_01.05.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: APFW_01.02.xx.xx, Android: 3.00D.xx, Vault: SPFW-01.04.xx.xx, Android: 3.01D.xx

4-30558	Verifone	*V660p-A*	H660-007-xxxx-xxx-xxx-A0	SPFW_01.05.xx.xx, SPBL_01.02.xx.xx, APFW_01.02.xx.xx, Android (VAOS):4.00F.xx, SPFW_01.06.xx.xx, APFW_01.03.xx.xx
4-80065	Verifone	*UX700*	U605-0007-xxxx-xxx-xxx-A0	Vault: SPBL_01.02.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPFW_01.06.xx.xx, Vault: APFW_01.03.xx.xx, Vault: SPFW_01.05.xx.xx, Android: 3.01D.xx, Vault: SPFW_01.04.xx.xx, VOS3: 02.xx.xx
4-40363	PAX Computer Technology (Shenzhen) Co Ltd	*A6650*	A6650-0xx-0x6-0xxx (NON-CTLS), A6650-0xx-0x6-1xxx (NON-CTLS), A6650-0xx-Rx6-0xxx (CTLS), A6650-0xx-Rx6-1xxx (CTLS),	26.00.01 xxxxx
4-30554	Toast Inc	*TG300, TG310*	REV1.xx	01.xx.xx.-10xxxxx

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)**
Ingenico, RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 3000	Hardware #: LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA Firmware #: 820547v01.xx, 820561v01.xx (base firmware)	Yes. 2024-00470.056 Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes Yes
Ingenico, RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 5000	Hardware #: LAN50AB (non CTLS), LAN50BB (CTLS) Firmware #: 820547v01.xx, 820376v01.xx, 820549V01.xx (SRED), 820555V01.xx (SRED), 820556V01.xx (SRED)	Yes. 2024-00470.056 Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes Yes
Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 7000 v.5	Hardware #: LAN70AA, LAN70BD Firmware #: 820547v01.xx, 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE),	Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes

3.2 POI Software/Application Details					
			820549V01.xx (SRED On-Guard FPE), 820565V01.xx (SRED FF1), 820548V07.xx (Open Protocols), 820572V01.xx (Tetra JVM Addon), 820376v14.xx (Security Services)		
Ingenico, UPP 2.0.x	Ingenico	Lane 7000 v.6	Hardware #: LAN70BD Firmware #: 820376v12.xx (Security Services), 820376v14.xx (Security Services), 820547v11.xx (Core Firmware), 820549V01.xx (SRED On-Guard FPE), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820565V01.xx (SRED FF1)	Yes. 2018-00470.020 Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes Yes
Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 8000 v.5	Hardware #: LAN80AA Firmware #: 820547v01.xx,	Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes
Ingenico, UPP 2.0.x	Ingenico	Lane 8000 v.6	820547v11.xx (Core firmware), 820376v12.xx (Security Services), 820556V01.xx (SRED On-Guard SDE),	Yes. 2018-00470.020 Yes. 2023-00470.045	Yes Yes Yes

3.2 POI Software/Application Details					
			820549V01.xx (SRED On-Guard FPE), 820548V07.xx (Open Protocols), 820376v14.xx (Security Services)	Yes. 2023-00470.051	
RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Move 5000	Hardware #: MOV50AB, (Non CTLS), MOV50BB, (CTLS), MOV50CB, (Non CTLS + Privacy shield), MOV50DB, (CTLS + Privacy shield), MOV50JB (CTLS + Privacy shield + Desktop case lid), MOV50BR Firmware #: 820547v01.xx, 820376v01.xx, 820555v01.xx (SRED), 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL) Hardware #: MOV50AA (Non CTLS); MOV50BA (CTLS), MOV50JA (CTLS), MOV50CA, MOV50DA, MOV50AB, MOV50BB (CTLS), MOV50CB, MOV50DB (CTLS), MOV50JB (CTLS) Firmware #: 820548V06.xx, 820547v01.xx;	Yes. 2024-00470.056 Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes Yes

3.2 POI Software/Application Details					
			820376v01.xx; (SRED) CTLS: 820549V01.xx, 820555v01.xx (SRED), 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820547v01.xx (Core Firmware), 820376v01.xx (Security Services), 820376v02.xx (Security Services), 820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (Core Firmware), 820376v12.xx (Security Services)		
RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Link 2500	Hardware #: LIN25AA (Basic version no CTLS support), LIN25BA (Basic version with CTLS), LIN25CA (Companion version no CTLS support), LIN25DA (Companion version with CTLS), LIN25EA (Touch version no CTLS support), LIN25FA (Touch version with CTLS), LIN25GA (Dual head version no CTLS support),	Yes. 2024-00470.056 Yes. 2023-00470.045 Yes. 2023-00470.051	Yes Yes Yes

3.2 POI Software/Application Details					
			LIN25HA (Dual head version with CTLS), LIN25IA (Companion version with rear connector and no CTLS support), LIN25JA (Companion version with rear connector and with CTLS) Firmware #: 820547v01.xx		
Ingenico, UPP 2.0.x	Ingenico	Self/2000, Self/4000, Self/5000, Self/4000LE, Self/5000LE	Hardware#: SEL20AA Firmware#: 820566v01.xx Hardware#: SEL40BA, SEL41AA1-xxxx Firmware#: 820547v01.xx, 820571v01.xx (Core Firmware), 820376v12.xx (Security Services), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE) Hardware#: SEL50CA, SEL51AA1-xxxx Firmware#: 820566v01.xx, 820573v01.xx (Core Firmware), 820376v12.xx (Security Services), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)	Yes. 2023-00470.051	Yes

3.2 POI Software/Application Details					
Ingenico, UPP 2.0.x	Ingenico	Lane/3600	Hardware #: LAN36AA2-xxxx, LAN36AB2-xxxx, LAN36BA1-xxxx, LAN36BA2-xxxx, LAN36CA1-xxxx, LAN36CA2-xxxx, LAN36CB2-xxxx, LAN36DA1-xxxx, LAN36DA2-xxxx, LAN36DB2-xxxx, LAN36EA2-xxxx, LAN36FA2-xxxx, LAN36AA1-xxxx Firmware #: 820571v01.xx (Core Firmware, 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820570V07.xx (Open Protocols), 820565V01.xx (SRED FF1)820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE),	Yes. 2023-00470.051	Yes
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM RX7000	Hardware #: R70411xxxx Firmware #: 02.03.11.xxxxx (The SRED solution supported by firmware includes SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard FPE, SRED OnGuard SDE, SRED FF1)	Yes. 2024-00470.059	Yes
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM EX8000	Hardware #: E801x2 Firmware #: 01.09.11.xxxxx (with AP Solution 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED	Yes. 2024-00470.059	Yes

3.2 POI Software/Application Details					
			OnGuard FPE, SRED FF1)		
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM DX8000-2, AXIUM DX8000-5	Hardware #: D851x3 (with AP Solution 1) Firmware #: 01.09.11.xxxxx (with AP Solution 1 SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)	Yes. 2024-00470.059	Yes
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM RX5000	Hardware #: R50411xxxx (no pinshield) Firmware #: 02.03.11.xxxxx(The SRED solution supported by firmware includes: SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)	Yes. 2024-00470.059	Yes
FreedomPay, FreeWay Standalone Application (FSA) v3.0	Ingenico	Move 5000	Hardware #: MOV50AB (Non CTLS), MOV50BB (CTLS), MOV50CB (Non CTLS + Privacy shield), MOV50DB (CTLS + Privacy shield), MOV50JB (CTLS + Privacy shield + Desktop case lid) Firmware #: 820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE),	Yes. 2025-00909.015	Yes

3.2 POI Software/Application Details					
			820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)		
FreedomPay, FreeWay Standalone Application (FSA) v3.0	Ingenico	Desk 5000	Hardware #: (CTLS) (Non CTLS + Privacy Shield) (Non CTLS) DES50AB DES50BB DES50CB DES50DB(CTLS + Privacy Shield) Firmware #: 820376v01.xx 820547v01.xx 820549v01.xx (SRED OnGuard FPE) 820555v01.xx (SRED) 820556v01.xx (SRED OnGuard SDE) 820559v01.xx (SRED ANL) 820565v01.xx (SRED FF1) 820548V02.xx (Open Protocol), 820548V03.xx (Open Protocol),820548 V05.xx (Open Protocol)	Yes. 2025-00909.015	Yes

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 *FreedomPay, Inc* 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.

The merchant must implement and maintain a POI device-tracking system that will identify each POI device according to its current state. Examples of potential states include:

- Deployed
- Awaiting Deployment
- Out of Service and/or Out for Repair
- In Transit
- Removed and returned

FreedomPay offers a basic record keeping system through its Enterprise Reporting Portal called the Device Management Portal, which can be configured during implementation. Alternatively, merchants may implement their own system if preferred. Electronic POI device inventories should be securely stored, with access limited to authorized personnel only.

The merchant must also establish a "state system of accounting and control" to keep track of all POI Devices (quantity and type), note changes in material inventories (incoming/outgoing), and monitor all aspects of the POI device lifecycle while the device is in the possession and control of the merchant. Record all inventory discrepancies within your inventory control system, and report missing or lost devices to FreedomPay once identified to compliance@freedompay.com, or to the designated FreedomPay partner/reseller who provided the devices.

If your organization is multi-store, regional, or a national operator it is important to employ inventory management and tracking systems at the local, regional and national levels to ensure that the knowledge and capability for managing, tracking and reporting of inventories is met at all levels.

It is recommended that device inventory contain, at a minimum, information similar to that in the Sample Inventory Table below. All device specific identification information required for inventory tracking can be found on a sticker on the back panel, the battery compartment of each POI device (pictures of serial number location for a sample of devices included in **Appendix C in Section 9, Additional Guidance** and/or through the logical interface on the POI device.)

The merchant must develop and maintain written protocols for device relocation among merchant locations. The merchant must monitor and document compliance with such protocols. The merchant's POI device relocation protocols must be at least as secure as the protocols identified in this PIM for shipment of POI devices to and from Approved Supplier Facilities. For additional information on maintaining chain of custody for device relocation or device storage, please contact compliance@freedompay.com or the FreedomPay partner/reseller who provided the devices.

The merchant may be asked to submit their annual POI inventory to their merchant acquirer as part of their annual PCI DSS compliance. A failure to follow the controls listed within the PIM may result in "Merchant Opt-Out; that is, suspension of the FreedomPay Commerce Platform P2PE Scope Reduction Program.

If a merchant no longer wishes to utilize the FreedomPay-provided POI devices as part of a PCI P2PE Scope Reduction Program due to Merchant Op-Out, contract termination, close of business or other

reason, the merchant is required to securely destroy all FreedomPay-provided POI devices. Secure destruction must take place using FreedomPay's secure destruction service by submitting a request to fprecycleservices@freedompay.com including the number of devices and serial numbers for each device. Once received, FreedomPay's Professional Services team will respond with further details. For more information on possible destruction services, please contact your FreedomPay representative.

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

Each POI device installation is recommended to be secured using one of the following methods or an alternative approved by your Qualified Security Assessor (QSA):

i. The device is physically mounted or tethered to prevent unauthorized removal, tampering or substitution. Acceptable methods include:

   a. Mounting the device to an approved PIN security stand

   b. Securing the device using a tether lock attached to the security slot on the POI device and permanently secured to the counter or other secure, physically affixed hardware at the opposite end of the tether. A wide variety of tether locks are available at most computer retailers, available online, or from FreedomPay. Please contact your FreedomPay Representative if you need assistance finding a suitable tether lock.

ii. The device should be located so that it can be readily observed/monitored by authorized personnel and in an environment that deters compromise attempts.

Additional implementation steps include:

i. Upon device initiation, the merchant must perform the following steps:
   a. Verify that the displayed serial number matches the serial number on the underside of the device.

i. For assistance locating the serial numbers on POI devices, please view the **Appendix C in Section 9, Additional Guidance** section.

b. Update the device record keeping system to reflect the change in device status and location.

ii. The device must utilize one of the following communication/connection types:

a. USB
b. Serial
c. Ethernet
d. WiFi
e. Bluetooth
f. Cellular

Other: For POI communication types not listed above, the merchant must contact compliance@freedompay.com to receive official FreedomPay compliance approval for use of such device from FreedomPay's compliance team. The merchant must receive, in writing, an official attestation from FreedomPay stating that the POI communication type, which is not listed in the above list, is an accepted communication/connection method for the FreedomPay Commerce Platform P2PE solution.

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 is recommended by FreedomPay, and reinforced by the PCI DSS, that all deployed devices be securely mounted and easily visible by staff to prevent unauthorized removal or tampering. The device should be located so that it can be readily observed/monitored by authorized personnel and in an environment that deters compromise attempts. In the event an implementation is designated for unattended use, procedures should be in place to mitigate the risk associated with the implementation. This may involve security cameras, more frequent inspections, tamper prevention controls, or other methods approved by your QSA.

Devices not in-service must be stored in accordance with the methodology outlined in Section 3.3.

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

Merchants are encouraged to mount in-service devices to an approved PIN security stand or secure the device using a tether lock attached to the security slot on the POI device and permanently secured at the opposite end of the tether. A wide variety of tether locks are available at most computer retailers or available online. Please contact your FreedomPay Representative or QSA if you need assistance finding a suitable tether lock. For implementations not conducive to mounted devices (i.e. standalone devices or mobile scenarios), procedures should be implemented to mitigate the risk of device tampering or compromise. This may include device assignment to location personnel, more frequent inspections, or other, QSA approved procedures.

The merchant must establish a “secure storage” area for POI devices not in service. This storage will be used when POI devices are received from FreedomPay prior to installation, transferred in from other Approved Merchant Locations, or removed from active use. Secure storage is defined by PCI as a designated space or location that has controlled physical access, whereby personnel must be authorized to gain access and mechanisms/policies are in place for documenting all physical access to the “secure storage” area including:

- Identifying personnel authorized to access devices
- Restricting access to authorized personnel
- Maintaining a log of all access including personnel name, company, reason for access, time in and out

The merchant must implement a “secure storage” access policy before implementing FreedomPay’s PCI Validated P2PE solution. This policy must include a description of what and where the secure storage area is as well as the procedures established to comply with requirements set forth in this section.

5. POI Device Transit

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

In order to ensure security delivery of devices, a trusted courier that allows for parcel tracking and delivery confirmation is recommended. FreedomPay leverages and recommends the following couriers, but other secure methods are permitted:

- FedEx
- UPS
- USPS (in certain scenarios)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

All devices shipped by and to the merchant (including merchant location to merchant location shipment) must be packaged with tamper resistant packaging.

Examples of tamper-proof packaging include envelopes or bags with serialized labels that irreversibly show evidence of any attempt to open the package. Tamper-proof packaging may be purchased from office supply providers and will be labelled specifically as "Tamper-Proof" or

"Tamper-Resistant." Packages may also be secured with tamper evident security tape around all openings.

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

All devices shipped to the merchant by FreedomPay will utilize a FreedomPay Trusted Courier. FreedomPay's Trusted Couriers are listed below and could be used by merchants for location-to-location shipments as well:

- FedEx
- UPS
- USPS (in certain scenarios)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

These couriers will be used to deliver devices to businesses addresses provided by merchant personnel during onboarding. In the case of shipment between merchant locations, devices should only be delivered to trusted business addresses. All devices shipped by and to the merchant (including merchant location to merchant location shipment) must be packaged with tamper resistant packaging.

Examples of tamper-proof packaging include envelopes or bags with serialized labels that irreversibly show evidence of any attempt to open the package. Tamper-proof packaging may be purchased from office supply providers and will be labelled specifically as "Tamper-Proof" or "Tamper-Resistant." Packages may also be secured with tamper evident security tape around all openings.

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.

Merchants must inspect the following, at a minimum, in an appropriate time frame based on their risk profile (typically quarterly):

- Has the USB/ethernet cable been damaged or altered in any way?
- Does the serial number on the device match the serial number provided by FreedomPay? (Refer to Appendix C for serial number location)
- Are active POI devices secured appropriately according to the PIM?
- Are inactive POI devices securely stored according to the PIM?
- Has the POI device been damaged in any way?
- Is the "Secured by FreedomPay" screen present?
- Are any additional tamper detection measures added by the merchant and noted in the inventory intact, such as security seals, labels, or hidden markings?

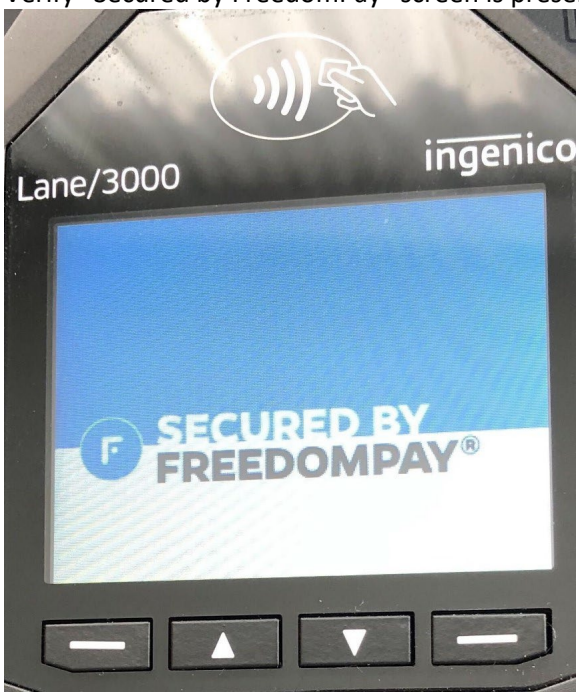
Examples of Inspection Areas:

Check connection point for additional wires/connections or hardware.

Verify exterior screws have not been removed.

Check points of interaction for overlays or inserted tools.

Verify “Secured by FreedomPay” screen is present.



If a merchant deploys a FreedomPay POI device in an area not physically monitored by an approved merchant employee, there must be appropriate procedures in place to reduce the possibility of device tampering and, in worst case scenarios, the time between compromise and detection. Please consult your independent Quality Security Assessor (QSA) for additional information on POI inspection and monitoring.

Any instance of device tampering must be reported to FreedomPay, and any device that has been or is suspected of being tampered with must be removed from the POS environment immediately and returned to FreedomPay per the instructions outlined in Section 5.2.

6.2 Instructions for responding to evidence of POI device tampering

The merchant must immediately return to FreedomPay, as set forth below, any POI device, or package containing a POI device, that appears to have been tampered with, was delivered by anyone other than a Trusted Courier, or was sent from any location other than an Approved Supplier Facility.

POI Device Shipment:

i. POI devices may be transported only by a Trusted Courier to an Approved Supplier Facility listed in section 4.2.
ii. Serial numbers of device(s) being returned, along with the reason for returning the device(s) must be communicated to RMA@freedompay.com who will generate a shipping label for the return.

iii. All POI device serial number(s) must be printed on the packaging statement or shipping label.

The merchant must update its device record-keeping system to reflect the change in device status and location.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

In the event of an encryption failure indicated by the presence of a 266 Error Code or a "P2PE Encryption Error" message, it is recommended that the merchant:

i. Review all Point of Sale (POS) system logs and batching functions for credit authorization and any sign of clear text cardholder data.
ii. Review all POS settlement reports to ensure that no unencrypted cardholder data is present.

In the event that clear text cardholder data is found, or there is a failure of a device security control or proven or suspected unauthorized use of sensitive administrative functions, the merchant must contact FreedomPay technical support immediately and follow the troubleshooting instructions found in Section 7 of this document. Until proper encryption functionality on the device has been restored and the device has been reauthorized by FreedomPay, the faulty device may not be used to process transactions unless the merchant formally requests a suspension of P2PE encryption as outlined in Section 6.2.

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

If a POI device is damaged, destroyed, appears to be malfunctioning or otherwise requires servicing, the merchant must follow the following process when interacting with FreedomPay personnel:

i. Contact FreedomPay tech-support at 888-495-2446 or by email techsupport@freedompay.com.
ii. If the FreedomPay support technician determines that a field technician should be dispatched, the technician will complete a dispatch request.
iii. Once a technician has been assigned, FreedomPay will provide the merchant with details on the deployment request.
iv. When the technician arrives on-site, and before allowing access to the POI device, the merchant should verify the technician's identity as a FreedomPay employee or contractor. All other personnel must be denied access unless without proper validation of their identity.
v. Once the technician's identity has been verified, the merchant should assign an escort to monitor the technician's activity at all times.
vi. Once the technician has completed the work, the merchant must respond to the dispatch email with the following details:
    i. Form of ID presented for verification
    ii. Time spent at location
    iii. Serial number(s) of terminal(s) touched by the technician

If a merchant no longer wishes to utilize the FreedomPay-provided POI devices as part of a PCI P2PE Scope Reduction Program due to Merchant Op-Out, contract termination, close of business or other reason, the merchant is required to securely destroy all FreedomPay-provided POI devices. Secure destruction of devices is required and must utilize industry-accepted standards. Proof of destruction must be provided through a destruction certificate and must be submitted to FreedomPay following the secure destruction process. For more information on FreedomPay POI destruction services, please contact your FreedomPay representative for more information.

9. Additional Guidance

Notice and Acknowledgements

This P2PE Instruction Manual is provided pursuant to the requirements of the PCI DSS. Implementation of the controls set forth in this PIM is a requirement for the PCI DSS SAQ-P2PE and Attestation of Compliance. The use of any POI device not approved by FreedomPay and/or any failure to comply with the requirements set forth in this manual is at the merchant's sole risk and may result in non-compliance with PCI DSS SAQ-P2PE, loss of qualification for PCI DSS scope reduction and/or compromised data security.

By using the FreedomPay P2PE Scope Reduction Solution, Merchant agrees that it will not modify or attempt to modify any FreedomPay supplied POI device configurations, including, without limitation:

- Attempting to enable any device interfaces or data capture mechanisms that have been disabled on a Freedom Pay supplied device
- Attempting to alter security configurations or authentication controls
- Physically opening any device
- Attempting to install applications onto any device

In order to maintain the scope reduction offered by the FreedomPay solution, Merchant acknowledges that all credit card transactions are to be entered/swiped through an approved POI device to remain with the P2PE Scope Reduction Program. Transactions entered through any other means are not subject to FreedomPay's PCI SSC approved Validated P2PE Program. FreedomPay has implemented a mechanism on its payment gateway (Freeway) to reject transactions that are sent, unencrypted, from a non-FreedomPay approved device with a "P2PE Device Error" response, also known as a 266 error. These unencrypted transactions are not stored in FreedomPay's environment but may be stored in logs generated by the merchant's Point-of-Sale, putting the merchant at risk of losing PCI scope reduction. If a merchant accepts payment through any other method outside of the FreedomPay PCI P2PE solution or is unable to resolve regular occurrences of 266 errors within 30 days of generation, they must opt out of the PCI P2PE Scope Reduction Program using the Merchant Opt Out Request form (Appendix A).

Country/Region Restrictions

In the event a country or region places restrictions on which make and model of device can be used within its borders, the below table will be updated:

Country/Region	Device Make	Device Model
Australia	Ingenico	Lane 5000, Move 5000
Australia	IDTech	SREDKey v2

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

Hardware versions can be found on the back of all devices on the manufacturers sticker that contains the serial number. Examples of placement of this sticker can be found in Appendix C.

Ingenico Devices:

To find the firmware version, follow the below steps:

1. Unplug the device from the POS system or other front-end system
2. Power the device by utilizing the power cable, or plugging it into a PC using the USB cable
3. During device boot-up, press the following key sequence on the Ingenico device: 2634, [Green button], F
4. If your device does not have an 'F' key, the key sequence would be 2634, [Green button], +
5. Select the following menu: *Control Panel/Terminal Information/Firmware PCI PTS/Display*
6. Record the firmware information associated with M1

The version of the application loaded onto Ingenico devices can be seen on the splash screen during device bootup. The "PCI Version" value should match version number template shown on the PCI SSC website.

ID Tech Devices:

Firmware versions for these devices can only be seen using an application provided by ID Tech. For a download of this application, please reach out to compliance@freedompay.com for assistance.

Castles/Elo Devices:

Open the CX Application menu from the main screen, then click "About". At the bottom of this screen, you will see the firmware version.

Ziosk Devices:

Firmware version can be seen in the device menu by going to Settings > About device > Firmware version.

Infinite Peripheral Devices:

Firmware versions for these devices can only be seen using an application provided by Infinite Peripherals. For a download of this application, please reach out to compliance@freedompay.com for assistance.

PAX Devices

From the home screen select Settings > About and record the firmware displayed.

Toast Devices

From the home screen select Settings > About and record the firmware displayed.

Verifone Devices

From the home screen select Settings > About and record the firmware displayed.

Appendix A: Merchant Opt Out Request

This Opt-Out request must be signed by an authorized merchant representative as reflected in FreedomPay's records. Prior to submitting a Merchant Opt-Out Request, please contact FreedomPay Technical Support for Opt-Out instructions. Technical Support will verify the authorized merchant representative and provide an Incident Number.

Incident Number (if applicable): _____
Opt-Out Request Date: _____

The undersigned Merchant hereby elects to opt out of the FreedomPay P2PE Solution. By signing this request, Merchant acknowledges that:

1. Transactions processed while an Opt-Out is in effect are not subject to P2PE scope reduction.
2. Merchant is solely responsible for implementing alternative controls to protect account data in lieu of the FreedomPay P2PE Solution.
3. Merchant is obligated to advise its acquirer or payment brand that Merchant has opted out of the FreedomPay P2PE Solution.
4. FREEDOMPAY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES REGARDING THE FREEDOMAY P2PE SOLUTION AS TO EACH TRANSACTION PROCESSED WHILE OPT-OUT IS IN EFFECT.
5. FREEDOMPAY DISLAIMS ALL LIABILITY INCLUDING, BUT NOT LIMITED TO, A DATA BREACH RESULTING FROM THE MERCHANT PROCESSING PAYMENTS OTHER THAN THROUGH THE USE OF FREEDOMPAY'S VALIDATED P2PE SOLUTION AND THE FREEDOMPAY COMMERCE PLATFORM.
6. Merchant has 60 days from the time of opt-out ("opt-out window") to resolve the conditions which prompted the opt-out and re-enroll in the solution, unless a different opt-out window is mutually agreed upon in writing between FreedomPay and the merchant. Following the opt-out window, the merchant may be restricted from processing transactions on the FreedomPay Commerce Platform indefinitely.

Note: Following Opt-Out, a merchant may elect to re-enroll in the FreedomPay P2PE Scope Reduction Solution subject to security protocol established by FreedomPay, including, a merchant attestation that all remnants of clear-text cardholder data have been deleted from the merchant's systems using secure data deletion processes.

Merchant: _____

Signature: _____
(Authorized Merchant Personnel Name - Printed)
Name: _____
Title: _____
(Authorized Merchant Personnel Name – Signature)

Please email this form to: compliance@freedompay.com

Appendix C: POI Device Serial Number Identification Examples

The below images depict some examples of POI devices from various manufacturers and the physical location of serial numbers applied by Key Injection Facilities for purposes of POI inspection, verification, or RMA (who can further assist with serial number location or mapping). For additional questions regarding POI device serial numbers, please contact compliance@freedompay.com.

Ingenico Lane 3000

Quantum Pay Reader 250

Ziosk