



P2PE Instructional Manual

Merchant Guide for P2PE Compliance

February 2025

Elavon and Simplify are registered trademarks to U.S. Bank N.A. Safe T, Safe-T Link and "Nothing to Find, Nothing to Steal" are trademarks to U.S. Bank N.A. This document is prepared by Elavon as a service for its customers.

Elavon, Inc. provides this publication as is without warranty of any kind, either expressed or implied. This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes will be incorporated in new editions of the publication. Elavon, Inc. may make improvement and/or changes in the product(s) and/or programs(s) described in this publication at any time.

©2025 Elavon, Inc. All rights reserved. No part of this publication may be reproduced or distributed without the prior consent of Elavon, Inc., Two Concourse Parkway, Suite 800, Atlanta, GA 30328.

Disclaimer: Elavon, Inc. provides this publication as is without warranty of any kind, either expressed or implied. This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes will be incorporated in new editions of the publication. Elavon, Inc. may make improvement and/or changes in the product(s) and/or programs(s) described in this publication at any time.

Table of Contents

1 Introduction to P2PE Requirements	4
2 Elavon's Safe-T Link™ with P2PE Protect Solution Information and Contact Details	5
2.1 P2PE Solution Information	5
2.2 Elavon Contact Information	5
3 Approved POI Devices, Applications/Software, and Merchant Inventory	6
3.1 POI Device Details	6
3.2 POI Software / Application Details	8
3.3 POI Inventory and Monitoring	10
3.3.1 P2PE POI Device Inventory Control Log	10
4 POI Device Installation Instructions	12
4.1 Installation and Connection Instructions	12
4.2 Selecting Appropriate Locations for Deployed Devices	13
4.3 Physically Securing Deployed Devices to Prevent Unauthorized Removal or Substitution	13
5 POI Device Transit	14
5.1 Securing POI Devices for Transit	14
5.2 Ensuring POI Devices Originate from and are Shipped to Trusted Sites and Locations	15
6 POI Device Tamper Monitoring and Skimming Prevention	16
6.1 Inspecting POI Devices, Preventing Skimming, and Reporting Suspicious Activity	16
6.1.1 Additional Ways to Maintain Device Security	16
6.1.2 Educate Employees on how to Identify Modified POI Devices	25
6.2 Responding to Evidence of POI Device Tampering	27
6.3 Confirming Devices and Packaging were not Tampered with and Establishing Confirmed Secure Communications with Elavon	27
6.3.1 Temporary Storage of Devices	30
6.4 Limiting Access to Stored Devices	30
7 Device Encryption Issues	32
7.1 Responding to POI Encryption Failures	32
7.2 Requesting that Elavon Stop the Encryption of Data	32
8 POI Device Troubleshooting	32
8.1 Troubleshooting a POI Device	33
	33

Revisions History

The following table provides a description of the changes made to this document from its origination to the current release.

Revision	Date	Revision Notes
SCR-0001-A	August 2017	Initial Release for review
SCR-0001-B	October 2017	Updated for PCI Release
SCR-0001-C	November 2018	Added newly approved POI devices. Removed “Confidential” stamp. Elavon, Inc. replaced Elavon, Incorporated.
SCR-0001-D	June 2019	Added 6 additional Ingenico devices
SCR-0001-E	November 2021	Added 5 additional Ingenico devices
SCR-0001-F	January 2021	Updated software versioning and devices supported based on final solution re-validation.
SCR-0001-G	July 2022	Updated PCI SSC Listing Number based on final solution revalidation, copyright, and branding (logo)
SCR-001-H	December 2024	Updated Solution parameters, noting optional setup scenarios, Section 6.3 with additional KIF location, Updated Simplify status, Updated POI device list.

Latest PIM Document

The most recent version of the Safe-T Link with P2PE Protect P2PE Instruction Manual will be available at https://www.mypaymentsinsider.com/api/file/c/Safe-T_PIM. To ensure your organization is always operating with the current information, please download before each use.

1 Introduction to P2PE Requirements

The purpose of this document is to provide procedures and guidance to merchants who are using Elavon's Point- to-Point Encryption (P2PE) Payment Card Industry (PCI) validated Safe-T Link™ with P2PE Protect solution. The P2PE standard emphasizes reducing PCI scope by not solely relying upon technology as in the past, but by also relying on merchants to control and manage POI device security, and in the process, protect the highly-sensitive cardholder data.

P2PE dictates that merchants no longer store, process, or transmit cardholder data on any system or electronic media (computers, portable disks, audio recordings, etc.) outside of the payment device used as part of Elavon's Safe-T Link™ with P2PE Protect solution. Additionally, no legacy storage of cardholder data from other payment devices or systems is permitted.

The following merchant requirements are explained in detail within this document.

- Maintaining a Chain-of-Custody for approved POI devices
- Receiving and activating approved POI devices
- Storing approved POI devices (location, inventory, periodic inspection)
- Deploying approved POI devices
- Device transit between merchant sites
- Inspection of approved POI devices
- Actions to take in the event of tampering or other security-related incidents

To maintain compliance with PCI P2PE requirements, merchants must agree to the following compliance requirements and adhere to directions set forth in this document, including:

- Use of Elavon's Safe-T Link™ with P2PE Protect solution after coordinating which solutions and devices to implement.
- Adherence to this P2PE Instructional Manual (PIM) provided by Elavon.
- Ensure that if any other non-P2PE payment channels are used, the P2PE environment is adequately segmented (isolated) from the non-P2PE payment channels.
- Removal of any legacy cardholder data or systems from the P2PE environment.
- Ensure that payment environments are validated against applicable PCI DSS requirements in accordance with applicable payment card brand requirements.

Please note that regardless of the financial obligations of the P2PE equipment (i.e., whether it is purchased, leased, etc.), the Merchant has full responsibility to ensure their payment environments maintain P2PE scope reduction by following the instructions set forth in this document, including maintaining the Inventory Control Log and Chain-of-Custody Form, by storing the device in a secured location when not in use, and by properly monitoring the equipment to prevent tampering.

2 Elavon's Safe-T Link™ with P2PE Protect Solution

Information and Contact Details

2.1 P2PE Solution Information

Solution name:	Safe-T Link™ with P2PE Protect
Solution reference number per PCI SSC website:	2024-00679.007

2.2 Elavon Contact Information

Company name:	Elavon, Inc.
Company address:	Two Concourse Parkway, Suite 800, Atlanta, GA 30328
Company URL:	https://www.elavon.com/
Contact name:	Elavon Gateway Support Inbox
Contact phone number:	1-866-265-6225 Option 3
Contact e-mail address:	gatewaysupport@elavon.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.

3 PCI-Approved P2PE PTS Devices Utilized in Elavon's Solution

3.1 POI Device Details

The following PCI-approved PTS devices are covered within the scope of this document.

Telium – Application Name: Simplify Version: V-OG-2.03.xxyy CHD Access: Yes				
PTS Approval #	Device Name	Hardware #	Firmware #	PCI Version
4-30132	iSC Touch 250	iSC2xx-31Txxxxx	M1: 820518v12.xx M3: 820073v01.xx M4: 820528v02.xx	V4
4-30125	iSC Touch 480	ISC4xx-11Txxxxx	M1: 820518v12.xx M3: 820073v01.xx M4: 820528v02.xx	V4
4-30176	iPP320, iPP350	IPP3xx-31Txxxxx	M1: 820305v11.xx M3: 820073v01xx M4: 820528v02.xx	V4
4-30220	iSMP4	IMP6xx-11Txxxxx	M1: 820305v11.xx M3: 820073v02.xx M4: 820528v02.xx	V4
Tetra – Application Name: Simplify Version: V-OG-2.03.xxyy CHD Access: Yes				
PTS Approval #	Device Name	Hardware #	Firmware #	PCI Version
4-30414	Lane3000	LAN30AA	M1: 820547v11.xx 820376v12.xx M3: 820548v06.xx M4: 820549v01.xx	V6
4-20324	Lane5000	LAN51DA	M1: 820547v01.xx 820376v02.xx M3: 820548v02.xx M4: 820549v01.xx	V5
4-30237	Lane7000	LAN70AA	M1: 820547v01.xx 820376v02.xx M3: 820548v02.xx M4: 820549v01.xx	V5
4-30494	Lane7000	LAN70AB	M1: 820547v11.xx 820376v12.xx M3: 820548v07.xx M4: 820549v01.xx	V6

Tetra – Application Name: Simplify Version: V-OG-2.03.xxxx CHD Access: Yes

PTS Approval #	Device Name	Hardware #	Firmware #	PCI Version
4-30493	Lane8000	LAN80AA	M1: 820547v11.xx 820376v12.xx M3: 820548v07.xx M4: 820549v01.xx	V6
4-30481	Lane3600	LAN36BA1	M1: 820571v01.xx 820376v12.xx 820549v01.xx M3: 820570v07.xx	V6
4-30326	Link2500	LIN25BA	M1: 820547v01.xx 820376v02.xx M3: 820548v07.xx M4: 820549v01.xx	V5
4-20316	Move5000	MOV50BB	M1: 820547v01.xx 820376v02.xx M3: 820548v02.xx M4: 820549v01.xx	V5
4-20359	Move5000	MOV50BR	M1: 820547v11.xx 820376v12.xx 820549v01.xx M3: 820548v06.xx	V6
4-30510	Self3000	SEL30AA1	M1: 820571v01.xx 820376v12.xx 820549v01.xx M3: 820570v07.xx	V6
4-30393	Self4000	SEL40BA	M1: 820547v01.xx 820376v02.xx M3: 820548v04.xx M4: 820549v01.xx	V5
4-30447	Self7000	SEL70JA	M1: 820547v11.xx 820376v12.xx 820549v01.xx M3: 820548v06.xx	V6
4-30445	Self8000	SEL80IA	M1: 820568v01.xx	V6

3.2 POI Software/Application Details

Below are the details of the software and applications (both P2PE applications and P2PE non-payment software) on the Ingenico Point-of-Interaction (POI) devices covered within the scope of this document.

Note: 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	Device Model	Hardware Version	Firmware Version	Device Version	PCI Listed?	Clear Text Account Data?
Simplify Version V-OG- 2.03. AAAAA	iPP320/ iPP350	IPP3xx- 11Txxxxx	820305V11.xx 820528V02.xx, 820073v01.xx	4	Yes	Display, ICCR, MSR, CTLS, PIN Entry, OP, SRED
Simplify Version V-OG- 2.03. AAAAA	iSC Touch 250	iSC2xx- 31Txxxxx	820518 V12.xx, 820528V02.xx, 820073V01.xx	4	Yes	Display, ICCR, MSR, CTLS, PIN Entry, OP, SRED
Simplify Version V-OG- 2.03. AAAAA	iSC Touch 480	ISC4xx- 11Txxxxx	820518 V12.xx, 820528V02.xx, 820073V01.xx	4	Yes	Display, ICCR, MSR, CTLS, PIN Entry, OP, SRED
Simplify Version V-OG- 2.03. AAAAA	iSMP4	IMP6xx- 11Txxxxx	820305v11.xx 820528V02.xx, 820073V01.xx	4	Yes	Display, ICCR, MSR, CTLS, PIN Entry, OP, SRED
Simplify Version V-OG- 2.03. AAAAA	Link/2500	LIN25BA	820547v01.xx 820376v02.xx 820548v07.xx 820549v01.xx	5.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Move/5000	MOV50BB	820547v01.xx, 820548v02.xx, 820549v01.xx	5.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Move/5000	MOV50BR	820547v01.xx, 820548v02.xx, 820549v01.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Lane3000	LAN30AA	820547v01.xx, 820548v02.xx, 820549v01.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED

Application	Device Model	Hardware Version	Firmware Version	Device Version	PCI Listed?	Clear Text Account Data?
Simplify Version V-OG- 2.03. AAAAA	Lane5000	LAN51DA	820547v01.xx, 820548v02.xx, 820549v01.xx	5.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Lane7000	LAN70AA	820547v01.xx, 820548v02.xx, 820549v01.xx	5.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Lane7000	LAN70AB	820547v01.xx, 820548v02.xx, 820549v01.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Lane8000	LAN80AA	820547v01.xx, 820548v02.xx, 820549v01.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Lane3600	LAN36BA1	820547v01.xx, 820548v02.xx, 820549v01.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Link2500	LIN25BA	820547v01.xx 820376v02.xx 820548v07.xx 820549v01.xx	5.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Self3000	SEL30AA1	820571v01.xx 820376v12.xx 820549v01.xx 820570v07.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Self4000	SEL40BA	820547v01.xx 820376v02.xx 820548v04.xx 820549v01.xx	5.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Self7000	SEL70JA	820547v11.xx 820376v12.xx 820549v01.xx 820548v06.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED
Simplify Version V-OG- 2.03. AAAAA	Self8000	SEL80IA	820568v01.xx	6.x	Yes	Display,ICCR,MS-R,CTLS, PIN Entry,OP,SRED

3.3 POI Inventory and Monitoring

Elavon's Safe-T Link™ with P2PE Protect solution is comprised of a combination of secure POI devices, applications, and processes that encrypt cardholder data as it travels from a POI device to our secure decryption environment. The encryption key contained in each POI device is a highly sensitive piece of information. Therefore, it is essential that all measures be taken to protect POI devices and their encryption keys from tampering. Elavon's Safe-T Link™ with P2PE Protect solution requires that a Chain-of-Custody Form and a Device Inventory Log be maintained and that devices are physically secured or monitored at all times.

3.3.1 P2PE POI Device Inventory Control Log

A P2PE POI Device Inventory Log must be maintained for each POI device a merchant has in their possession. Devices must be inventoried upon initial receipt and quarterly thereafter throughout all phases of device usage. Additionally the devices must be inventoried whenever the location of a device changes. Maintaining this inventory log provides a means to track and monitor the following important information for each device.

- Device Number
- Device Vendor
- Device Make/Model
- Device Serial Number
- Device Location (address and any other defining information)
- General Description (security seals, labels, hidden markings, etc.)
- Photograph that clearly shows device type and model to assist with ID of different devices.
- Device Status (Sealed/Deployed/Stored/In Repair/No Longer in Use/Returned)
- Number of Physical Connections
- Type of Physical Connections
- Firmware Version
- Hardware Version
- Application(s) and Version(s)
- Inventory Date
- Name of Inspector

If there is already an inventory control system in place that tracks all required data stated above, that system may be utilized instead of the one included within Elavon's Safe-T Link™ with P2PE Protect solution.

Any variances in inventory, including missing or substituted POI devices, must be reported to Elavon **Gateway Support** at 1-866-265-6225 Option 3 or by e-mail at GatewaySupport@Elavon.com immediately.



Maintain log for all elevator-installed P201E-approved equipment. Review log quarterly, and submit to Elevon annually.

[illegible]

This form must be secured using the guidelines below.

Must have password controlled access with regular password changes and strong password requirements.

Regular checks of user access lists must be conducted.

Arrest should be on a "need-to-know" basis.

All changes must be traceable to individual users, and the activity must be fully documented.

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.
- Only P2PE approved capture mechanisms as designated on PCI's list of Validated P2PE Solutions and in the PIM can be used.

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

Elavon's Safe-T Link™ with P2PE Protect solution is comprised of a combination of secure POI devices that are shipped pre-programmed and ready to use. Simply, perform the following actions upon receiving a device.

1. Verify shipping details for the device(s) to confirm it originated from a trusted source. Please see the acceptable shipping addresses within the P2PE POI Device Reception Inspection List found in Section 6.3 of this document.
2. Inspect the integrity of the tamper-resistant packaging as explained in Section 6.3 before installing a device.
3. Unpack the device from the box.
4. Connect any USB, Ethernet, or serial cable as needed before powering up device.
5. The device will now go through boot cycle to power up.

Once the device completes booting up, press 0 to confirm that the version listed on the pin pad is the P2PE solution. If the device displays another message, or if you are unable to process a transaction, contact the Elavon Gateway Support at 1-866-265-6225 Option 3 or by email at GatewaySupport@Elavon.com for installation support.

After initial installation, it is considered best practice to disconnect and securely store your devices when unattended.

Please refer to the Troubleshooting guides that are shipped with each Ingenico iPP320/iPP350, iSC250, iSC480, and iWL2xx/iWL25x device for instructions on installation, including setup for Bluetooth connectivity for the iWL25x series devices. Alternatively, <http://www.ingenico.com> may also contain installation instructions, or you can contact Elavon Gateway Support at 1-866-265-6225 Option 3 or by email at GatewaySupport@Elavon.com for installation support.

Note: *Elavon's Safe-T Link™ with P2PE Protect solution is provided for specific PCI-approved POI devices, which are listed in Section 3.1 of this document. Only these devices can be used to capture cardholder data under this P2PE- certification program.*

Physically secure POI devices in your possession, including devices:

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

4.2 Selecting Appropriate Locations for Deployed Devices

The following guidelines should be considered when placing and deploying each POI device covered within the scope of this document.

- Position the device in a location where it can be easily and continuously observed and monitored by authorized personnel.
- Physically secure all device components so that cables cannot be unplugged by turning the device over. Consider installing locking stands, cable trays, or other securing mechanisms to prevent unauthorized removal.
- Limit access to parts of the device that are NOT required for payment processing (e.g., PIN pad and card reader).
- Position in-store cameras and devices so that the PIN entry keypad is not visible to cameras.
- Place the devices at least 6 feet away from anti-theft doorway units.
- Take photos of new equipment and periodically cross-check the entire POS system with the photo to confirm there are no changes.

4.3 Physically Securing Deployed Devices to Prevent Unauthorized Removal or Substitution

The following guidelines should be considered when placing and deploying each POI device covered within the scope of this document.

- Physically secure all terminals to the structure of the payment location when possible (e.g., mount and secure the terminal and cables with locking stands, cable trays, and other securing mechanisms.)
- Place terminals in a location where all equipment is easily observed and can be monitored at all times.
- Limit access to parts of the device that are NOT required for payment processing (e.g., PIN pad and card reader).
- Terminals should be at least 6 feet away from anti-theft doorway units and at least 18 inches from surface mounted deactivation pads.

5 POI Device Transit

If a P2PE-approved, Elavon-issued POI device must be transferred between merchant sites or if the device is being returned to Elavon, the following procedure must be used to ensure the security of the device is not compromised.

5.1 Securing POI Devices for Transit

If returning the device to Elavon, first contact Elavon to request a Call Tag, then follow the packing instructions below. Elavon will provide additional shipping instructions with the Call Tag. **It is important to store the device in a physically secure location until it is returned.**

1. Place the device in a bar-coded, tamper-resistant bag, if using. The image below shows an example of such a bag that has a tamper seal designed to indicate attempts at opening the bag. A clear “VOID” will appear within the green adhesive strip if tampering occurs.



Proper Placement of Device in Tamper-Resistant Bag

2. If using a bar-coded, high-risk grade tamper-resistant bag, print the tamper-resistant bag serial number next to the device's serial number on a Packing Slip to link them for tracking purposes, as well as on the Device Inventory Log under the General Description column. If not using a bar-coded, high-risk grade tamper resistant bag, be sure to list the device serial number on the packing slip.
3. Verify the address where the device will be sent with the recipient and inform them of the impending delivery.
4. It is required that the device be shipped using ONLY a secured carrier, such as UPS, so that it is tracked at all times during transit.
5. Once shipped, update the Device Inventory Log with all necessary information for tracking the device until it reaches its destination. At that point, update your log to note that status.

5.2 Ensuring POI Devices Originate from and are Shipped to Trusted Sites and Locations

As stated in the previous section, Elavon requires that the address where a POI device is being sent is verified prior to shipment by contacting the recipient. The recipient must also be informed about the impending delivery and given the estimated date and time of that delivery.

Please contact Elavon Gateway Support at 1-866-265-6225 Option 3 or by email at GatewaySupport@Elavon.com if you suspect that a device has been tampered with or has originated from an untrusted or unknown source.

6 POI Device Tamper Monitoring and Skimming Prevention

6.1 Inspecting POI Devices, Preventing Skimming, and Reporting Suspicious Activity

As noted previously, each POI device must be examined upon receipt and initial deployment, as well as on regular basis thereafter. Any abnormalities, such as missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other material that could be used to mask damage from device tampering must be noted at each inspection. Merchants must, at a minimum, inspect as follows.

- ☐ Is the POI device in its designated location?
- ☐ Is the manufacturer's name correct? ☐ Is the model number correct?
- ☐ Is the serial number printed on the label and displayed on the screen correct?
- ☐ Is the color and general condition of the POI device as described, with no additional marks or scratches (especially around the seams)?
- ☐ Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
- ☐ Are the manufacturer's security markings and reference numbers as described?
- ☐ Are any expected ultra-violet lights present and as described?
- ☐ Are all connections to the POI device as described, using the same type and color of cables and with no loose wires or broken connectors?
- ☐ Are all cables screwed in or connected all the way?
- ☐ Is the number of connections entering the POI device correct?
- ☐ Is the total number of POI devices in use the same as the number of POI devices officially installed?
- ☐ Are you getting a high number of mag-stripe read failures or debit card declines?
- ☐ Are customers having difficulty inserting a chip and PIN card into the EMV slot?

6.1.1 Additional Ways to Maintain Device Security

- ☐ Apply all security updates and patches when necessary and always use a network firewall.
- ☐ Be aware of overlays, which form to the device covering the keyboard area and possibly concealing damage resulting from tampering.
- ☐ Check the device wire connections for signs of tampering, such as a larger wire being used that contains additional data-stealing wires.
- ☐ Note the serial number on the back of all POI devices and check this against the electronically displayed serial number on the POI device.
- ☐ Take photos of new equipment and periodically cross-check the entire POS system with the photo to confirm there are no changes.
- ☐ Keep all areas around POI devices clear and free of smartphones and other unnecessary electronic equipment.
- ☐ Train personnel to be aware of suspicious behavior of customers and to report tampering or substitution of devices.
- ☐ Periodically rotate the individuals performing the device-checking to ensure nothing gets missed and to eliminate collusion.
- ☐ Be cautious of unannounced service visits. All service visits must be verified prior to the appointment and all service personnel must be identified and their activity involving the POI device logged on the Inventory Control Log.

The following images (provided by Ingenico) show how each of the POI devices listed in Elavon's Solution should appear when in an unaltered state. Use the images to compare your devices to ensure tampering has not occurred.

iPP320



iPP350



iPP3xx



ISC250



ISC480



iWL250



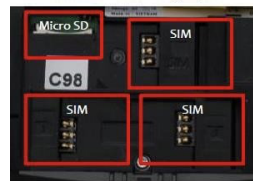
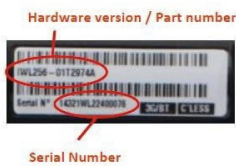
iWL2xx



Rear View casing closed



Rear View casing open



Lane 3000



Lane 5000



Lane 7000/8000



iUC150



iUP250



iUR250



6.1.2 Educate Employees on how to Identify Modified POI Devices

The following images (taken from <http://krebsonsecurity.com> and Ingenico) are examples of how devices may be altered to compromise security. Please use these as examples to train your staff on how to spot altered devices.

The image on the right is the device as it appears from the manufacturer. Notice the image on the left is larger. This is because it has a skimming overlay that must be larger than the original device in order for it to fit on top of it.



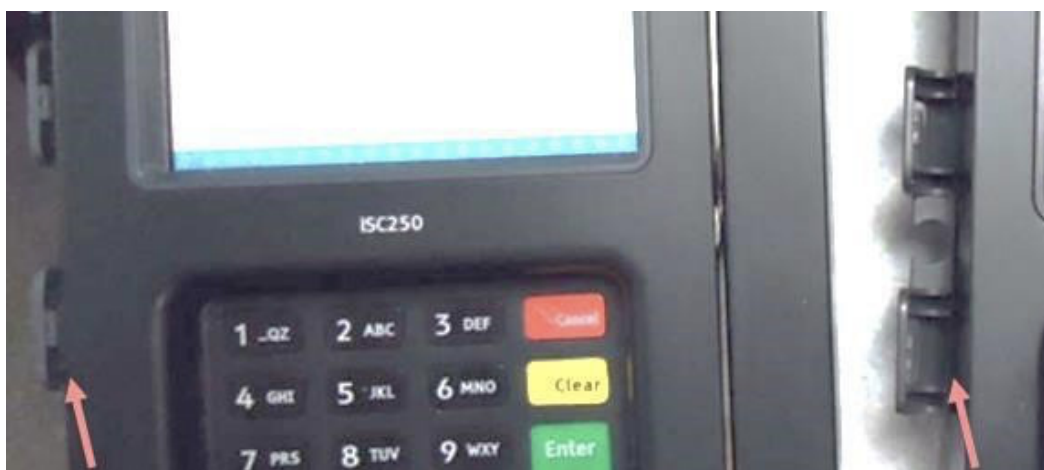
Another way skimming devices can be detected is by looking at the backlight. The image on the right is untampered. Notice the brightness of the keypad, as opposed to the keypad on the left that is darkened.



The green LED light, shown below, that displays on the device when a customer uses a contactless payment method such as Apple Pay.



Check the stylus tray to ensure it is visible and useful. Notice in the image on the left the stylus tray is covered by the skimming device.



Performing routine checks like these can help to lessen the chances of a criminal gaining access to customer card data. This list is not inclusive of all hacking methods, but should serve as a general guide to stress upon your employees the importance of being vigilant in monitoring and inspecting your POI devices on a regular basis.

See also the PCI SSC's Skimming Prevention Taskforce's document titled, "*Skimming Prevention: Best Practices for Merchants*," available at www.pcisecuritystandards.org.

6.2 Responding to Evidence of POI Device Tampering Do NOT use the device.

Immediately remove the device from the network, if applicable, but DO NOT power it down. Preserve all evidence. Contact your company's bank, corporate security team, or local law enforcement. Then, contact Elavon Gateway Support at 1-866-265-6225 Option 3 or by e-mail at GatewaySupport@Elavon.com.

Use pre-established, documented, and distributed security incident response and escalation procedures to timely and effectively handle device tampering situations.

6.3 Confirming Devices and Packaging were not Tampered with and Establishing Confirmed Secure

Communications with Elavon

Packages containing the POI devices are shipped via UPS 3-day ground, UPS Ground, or UPS Next Day Air (by 5:30 p.m. arrival). Elavon does not deliver UPS Next Day Early a.m. arrival.

They will arrive in a sealed cardboard package with OEM branding (inside the outer box). Thoroughly inspect the packaging upon receipt by comparing it to the images below to ensure no tampering has occurred during transit.



The POI device (and power supply, if included) will be nested inside a protective cardboard casing inside the package.



The device will be wrapped in a tamper-resistant bag.

The front of the tamper-resistant bag is barcoded and serialized prior to shipping and are scanned together to associate the device to the tamper-resistant bag. The tamper-resistant bag serial number is printed next to the device's serial number on the Packing Slip. Confirm these numbers match upon receipt.

IMPORTANT! Do NOT remove the device from the tamper resistant packaging until such time that it is being deployed. Store the device in a physically secured area. Once the device is in your possession, you are responsible for safeguarding it throughout the lifecycle of use.

Record all information regarding the device on the POI Device Inventory Log provided in Section 3.3.1, then either store or deploy the device.

The Device Reception Inspection checklist, shown below, may be used during the process just described.

P2PE POI Device Reception Inspection List	
Address	
<p>Your package(s) will be sent from one or more of secure POI deployment facilities. If the Senders address differs, call Elavon immediately, and do NOT open the package(s).</p>	<p>POS Portal 1627 Main Ave Sacramento, CA 95838 OR 1920 Watterson Trail # A, Louisville, KY 40299</p> <p>Ingenico 6195 Shiloh DR, Alpharetta, GA 30004</p> <p>Ingram Micro Canada Inc. Dock SPS - TPG (The Phoenix Group) 88 Foster Crescent Mississauga, ON L5R 4A2</p>
Packing Slip	
<p>Every order contains a packing slip with the P2PE device's serial number and its associated Tamper Evident Bag Serial Number.</p>	<p>Compare the two serial numbers. If they differ, do NOT use the device. Call Elavon immediately.</p>
Tamper Bag	
<p>P2PE Devices are always shipped with a security bag. Is the bag missing? The bag will have a green adhesive seal at the top of a barcoded clear bag.</p> <p>Do you see the words "VOID" on the green seal?</p> <p>Has the bag been cut? Has it been replaced?</p> <p>Verify the serial number on the device matches the serial number on the pack slip.</p>	<p>NOTE: POS Portal, Ingenico, and The Phoenix Group have the functionality to have both a P2PE and a Non- P2PE device on a single order. Verify the device arrived in the tamper-resistant bag.</p> <p>If the device has been tampered with, the word "VOID" will appear in white behind the green security seal.</p> <p>Check to make certain the bag has not been cut and that new clear tape has not been placed over the existing security seal.</p> <p>Each Device that is P2PE intended will have a tamper bag serial number next to the device's Serial Number. Both are visible through the Tamper Evident Bag.</p>
Cardboard Box	
<p>The box must NOT be torn or cut.</p> <p>The box must have the Manufactures Sticker (OEM) on the front.</p>	<p>An outer box for shipment may be used.</p>

6.3.1 Temporary Storage of Devices

Physically secure POI devices in your possession. This includes devices that are:

- awaiting deployment,
- undergoing repair or otherwise not in use, and
- awaiting transport between sites.

6.4 Limiting Access to Stored Devices

Limit access to stored devices only those employees who need it to perform job functions (e.g., managers). Confirm each business need and identify all third-party personnel claiming to be present for support or equipment repair PRIOR to granting them access to POI devices.

An Access Control Form, such as the one provided below, should be used to maintain a list of preauthorized personnel who have access to all stored devices. Update the list each time ANY stored device is accessed. Include on the form the following information.

- The name of the authorized personnel accessing the device.
- The name and company of an escorted non-authorized person (if any).
- The date, and time in and time out of access.
- The reason for access.

Elavon P2PE-Approved POI Device Access Control Form

[illegible]

7 Device Encryption Issues

7.1 Responding to POI Encryption Failures

Although it is unlikely, there may be occasions where a device encryption failure occurs. In such an event, an Elavon Customer Service member will alert your primary point of contact regarding the failure and work with your representative to troubleshoot the specific device(s) based on the criteria outlined within the “Troubleshooting” section of this guide. If troubleshooting fails to resolve the encryption failure, you will be required to remove the device from service, and either send it to Elavon for repair or replacement. Elavon’s solution does not permit opting out of using P2PE with any device within your payment environment.

7.2 Requesting that Elavon Stop the Encryption of Data

Elavon’s solution does not permit opting out of P2PE with any device. If a merchant chooses to stop processing using our P2PE solution and opt out of the Safe-T Link™ with P2PE Protect solution, this must be done in compliance with any signed agreement. At that point, the merchant accepts responsibility for the following impacts.

- The security impact to the merchant’s account data and potential risks associated with processing transactions without P2PE protection.
- Implementing alternative controls to protect account data in lieu of Elavon’s Safe-T Link™ with P2PE Protect solution.
- The merchant is no longer eligible to complete the Self-Assessment Questionnaire (SAQ) P2PE associated with use of the PCI-approved devices.
- Processing transactions without P2PE protection may impact the PCI DSS compliance validation.

8 POI Device Troubleshooting

8.1 Troubleshooting a POI Device

If assistance is needed for troubleshooting your POI device(s), Elavon will work remotely with the point of contact to troubleshoot the issue.

Visit Ingenico's website at <http://www.ingenico.com> to find the most current device documentation, or contact Elavon Gateway Support at 1-866-265-6225 Option 3 or by e-mail at GatewaySupport@Elavon.com for help.



Elavon and Simplify are registered trademarks to U.S. Bank N.A. Safe T, Safe-T Link and "Nothing to Find, Nothing to Steal" are trademarks to U.S. Bank N.A. This document is prepared by Elavon as a service for its customers.

Elavon, Inc. provides this publication as is without warranty of any kind, either expressed or implied. This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes will be incorporated in new editions of the publication. Elavon, Inc. may make improvement and/or changes in the product(s) and/or programs(s) described in this publication at any time.

©2025 Elavon, Inc. All rights reserved. No part of this publication may be reproduced or distributed without the prior consent of Elavon, Inc., Two Concourse Parkway, Suite 800, Atlanta, GA 30328.