Analysis of Elavon Simplify

White Paper

May 2015

What's Inside

Executive Summary

Overview

In August 2014 the US CERT (United States Emergency Computer Readiness Team)[1] and the US Department of Homeland Security[2] reported over 1,000 merchants had been affected by memory scraping malware. These reports were startling and reinforced the need for greater security.

The threat landscape is evolving rapidly and merchants face constant attacks from criminal elements attempting to access systems and steal credit card data, Elavon has developed Simplify, a product designed to reduce the exposure of cyber threats that exploit vulnerabilities in a merchant's Point Of Sale (POS) environment.

SecurityMetrics was contracted by Elavon to objectively review the Simplify solution and provide an opinion regarding their findings. The remaining portion of this report details the summary of findings as well as an analysis of their testing methodology. A P2PE-certified QSA conducted this review.

Elavon has been a leader in processing payments for over twenty years, and consistently ranks among the top 5 global payment providers. Elavon leverages the world's best technologies for their customers, from large worldwide enterprises to locally owned small businesses. With the pace of change accelerating and merchant threats growing in both quantity and complexity, Elavon works tirelessly to provide their customers with resources to guard sensitive credit card data.

SecurityMetrics protects electronic commerce and payments leaders, global acquirers, and their retail customers from security breaches and data theft. The company is a leading provider and innovator in merchant data security, and as an Approved Scanning Vendor and Qualified Security Assessor, has tested over 1 million payment systems for data security and compliance. Founded in October 2000, SecurityMetrics is a privately held company headquartered in Orem, Utah.

Threat Landscape

Attackers work tirelessly to find ways to steal cardholder data for financial gain. Merchants are constantly under attack as they are almost guaranteed to have cardholder data in their environment. Attacks range from skimmers or replaced PTS/PED devices, to attacks on merchant systems and databases containing cardholder data.

Over the last few years, POS malware has been an increasing threat to merchant environments as attackers can compromise merchant systems through a variety of attack methods including email phishing attacks, remote access attacks, insider threats, social engineering, and more.

POS malware and data breaches are a constant concern for merchants, banks and processors. From 2008 to 2011, roughly four versions of POS malware used to steal customer cardholder data were discovered on merchant POS systems. From 2011 to present, more than fourteen additional types of POS malware have been discovered and millions of credit card numbers stolen and sold on the black market. In 2014 development kits were discovered that allowed attackers to customize malware to specific environments and systems.

Elavon will permit the reduction of the scope of PCI in a merchant environment when Simplify is correctly implemented.

Attackers are getting smarter and better at infiltrating systems, hiding malware that steals data and taking data from merchant environments. These breaches cost merchants, banks, and processors millions of dollars to investigate and remediate.

P2PE and E2EE

P2PE (Point-to-Point Encryption)

In an effort to combat the rising trend in threats to merchants, the PCI Security Standards Council (PCI SSC) released a new P2PE assessment standard in 2012. Companies who have implemented the infrastructure for device management and control, key management, encryption and decryption of cardholder data, and validated all P2PE controls, have the ability to provide an end-to-end validated encryption solution for merchants. In the P2PE

1 https://www.us-cert.gov/ncas/alerts/TA14-212A?utm_source=twitterfeed&utm_medium=twitter
2 https://threatpost.com/secret-service-warns-1000-businesses-hit-by-backoff-pos-malware

standard, this provider assumes the role as a solution provider. This allows merchants the option to use a PCI SSC validated P2PE solution provider to help protect data in their environment.

Solution providers distribute validated PTS devices to merchants with pre-injected encryption keys that merchants are unable to obtain or access.

The solution provider monitors transactions from merchant locations. In the event of any alerts or "red flags", the solution provider is notified, at which point they may contact the merchant to investigate the issue.

Solution providers assume responsibility for the security and integrity of the PTS/PED device from the manufacturing facility, through key injection, to the merchant location where the device is securely stored or installed for use. Solution providers are required to use a unique key per PTS/PED device so in the event one device was compromised, the remaining devices or encryption keys in the merchant environment are not compromised as well. At the end of the lifecycle the PTS/PED device is returned to the solution provider for secure erasure and disposal.

By providing a token to the merchant, Elavon is eliminating the need for merchants to store cardholder data for any future transactions.

A validated Point-to-Point encryption solution allows a merchant to claim scope reduction with their acquirer if they follow the Point-to-Point implementation manual (PIM) provided by the solution provider. The PIM includes 8 requirements/sub requirements of the PCI standard as well as over 25 additional requirements outlined in the PIM for correct implementation. The merchant still is responsible for PCI DSS compliance of any environments outside of their POS/PMS system including MOTO, ecommerce, etc.

SRED and TRSM

PTS validated devices are devices that have been validated as being tamper-resistant and secure. If tampering occurs, the device will erase all secure memory and conduct and auto-reset process. These types of devices are known as Tamper Resistant Security Modules, or TRSM.

Many TRSM devices encompass an additional level of security where secure processing and encryption of sensitive data is handled. In the PTS validation process some manufacturers choose to have this secure processing area undergo an additional validation to ensure it is also secure. This additional functionality is validated and listed as Secure Read and Encrypt of Data (SRED).

E2EE (End-to-End Encryption)

Prior to the P2PE standard being released by the PCI SSC, service providers offering off the shelf "P2PE offerings or "E2EE offerings" had no framework or minimum set of security requirements on which they could base their offering. Because most advertised solutions did not have a minimum set of requirements to adhere to, a merchant or business looking for a secure solution was not able to differentiate between an offering that was secure versus a well marketed offering that provided little to no security.

Some companies offer a non-validated "Point-to-Point Encryption" solution also referred to as "End-to-End Encryption". This can be confusing and makes it difficult to distinguish between a P2PE SSC validated P2PE solution and other similar products that have not been validated according to the PCI SSC P2PE standard. In most non-validated P2PE or E2EE offerings, the services provided cover part of the PCI SSC P2PE set of requirements but not necessarily all components. These alternate products are intended to help reduce the threat landscape in the merchant environment. But since they have not been reviewed or assessed by a P2PE QSA against the P2PE standard, the protection they provide to merchants can vary from very little additional protection to a great deal of protection.

Elavon's Simplify Solution

Elavon's Simplify product responds to concerns and requests of banks, credit card companies, and merchants. Elavon's Simplify helps avoid cardholder data theft from merchant environments by restricting the number of places clear text cardholder data resides in those environments. Simplify is an Elavon product that encrypts cardholder data on approved PTS/PED validated devices. Simplify does not change the basic customer experience.

A customer presents their credit card for payment at a PCI PTS validated approved card acceptance terminal. Once the credit card is presented for payment, the terminal encrypts the cardholder data within that terminal.

All transactions processed through Simplify are performed on PTS/PED validated devices or TRSM devices. Whenever possible the SRED module is also used for transaction processing. In addition, Elavon only maintains the data decryption keys in a Hardware Security Module (HSM), which is also a TRSM, managed within their PCI DSS validated environment. Keys injected on the PTS devices are stored and injected at an Elavon-approved key-injection facility in TRSM devices.

Any applications on the PTS/PED device, such as Simplify, are also required to undergo code review and penetration testing to ensure they are secure and developed according to best practices in secure coding as well as the device manufacturer's recommendations for secure coding and handling of data.

POS Isolation

Only encrypted PAN (the Primary Account Number or the 15-16 digit number on the front of the credit card) and SAD (Sensitive Account Data including the PAN, CVV, PIN, and contents of the magnetic stripe or chip data found on the card), data leaves the terminal when the card is presented for payment. One of the unique benefits of Elavon's Simplify solution is the ability for the PCI PTS/PED device to send encrypted data directly to Elavon for payment processing, bypassing any other system or POS in the merchant environment. By never allowing cardholder data (encrypted or unencrypted) to enter a merchant POS system[3] or database the risk of cardholder data compromise is significantly reduced.

Coupled with the Elavon tokenization service, the merchant receives a token from Elavon during the transaction. This token is used for any future transactions with the same credit card, including recurring payments, returns, voids, etc. By providing a token to the merchant, Elavon is eliminating the need for merchants to store cardholder data for any future transactions.

With POS bypass, PAN and SAD cardholder data is encrypted on the terminal and never sent to the POS system. This protects the merchant from theft of sensitive authentication data in the event their system is infected with POS malware designed to steal cardholder data. The malware would never access data that can be used to commit cardholder data fraud.

Data is only encrypted in the PTS/PED validated terminal and only decrypted in the Elavon PCI validated environment. Cardholder data passing through merchant networks is encrypted with no corresponding keys to decrypt it. By restricting storage of encryption keys to the secure card acceptance terminal and the Elavon environment, no information passing through merchant systems can be decrypted and no encryption keys are passed with the information, making it impossible for attackers to intercept keys to decrypt data.

Elavon has coded the following PCI PTS PED approved devices for the Simplify solution:

- Ingenico iPP320
- Ingenico iPP350
- Ingenico iSC250
- Ingenico iSC480
- Verifone Mx915
- Verifone Mx925

Evaluation of Simplify

Simplify is a solution that follows many of the P2PE controls but has not been validated to the P2PE standard. The purpose of this whitepaper is to provide an independent analysis of the Simplify solution and the amount of protection and risk reduction it may provide. This analysis provides information to merchants who are looking to implement Simplify or who have already implemented Simplify to demonstrate where clear-text data resides in a Simplify environment as well as where data is encrypted so they can make good design decisions as they architect the security infrastructure of their environments. This paper will also help ISAs (Internal Security Assessors)

3 Some merchants have the option to process offline or store and forward transactions in which case they may receive encrypted cardholder data from the PTS/PED device to send for processing, but no unencrypted cardholder data ever leaves the PTS/PED device. Merchants who have chosen the option for offline will only receive transactions if the device goes offline. Once back online transactions are automatically sent for authorization.

and QSAs (Qualified Security Assessors) by providing information to assist them in validating the scope of a PCI environment and assist them in performing assessment activities.

Scope of activities

The scope of the assessment activities was limited to how the Elavon PTS/PED validated devices with Simplify function in a merchant environment for protecting cardholder data. Analysis was conducted on the functionality of the devices used including: configuration, access merchants had to change settings, and how Simplify handled cardholder data. Analysis was also conducted on traffic leaving the PTS/PED device to ensure that all forms of external communication (USB, Serial, Ethernet) contained encrypted cardholder data.

Data was analyzed entering the PCI validated decryption environment to ensure it was encrypted as it entered and prior to being sent for authorization.

The assessor reviewed the data returning from the decryption environment to the merchant environment to ensure that the merchant was only receiving a token and no cardholder data was being returned to the merchant environment.

An overview of keys and key storage was also reviewed to ensure Elavon was using strong encryption keys in their environment for encrypting cardholder data. Interviews were conducted with personnel at Elavon and vendors to validate that keys were injected securely and that no VAR, Integrator, or Merchant had access to encryption keys or clear-text account data through any Elavon system.

All types of supported transactions were performed on the PTS/PED validated device with Simplify, including:

- Sales
- Sale Inquiries
- Returns
- Voids
- Return Inquiries
- Return Voids

The following supported acceptance mechanisms were included:

- Online credit and debit card transactions
- Offline credit and debit card transactions
- Manual or keyed card transactions
- Contactless transactions
- Chip cards, also known as EMV (Europe MasterCard Visa), Chip and PIN, or Chip and signature

Each transaction type and mechanism was sampled for each device listed to ensure that data leaving the device was encrypted.

The assessment utilized forensic tools and methods to visually inspection all device output. Validation that no unencrypted cardholder data left any device for any transaction or payment mechanism type was confirmed. No data entering merchant POS systems contained unencrypted cardholder data.

No analysis was conducted on the logistics and handling of POI devices from manufacturer to the point of installation. The parties who inject keys onto devices had been assessed to the ANSI TR-39 assessment procedures. These reports were reviewed and interviews conducted with key personnel as part of this assessment.

No code review or penetration activities were conducted on the Simplify application resident on the PTS/PED validated devices. PTS/PED destruction and retirement procedures were also not assessed.

The Elavon decryption environment is assessed by an independent QSA company as being compliant to the PCI DSS 2.0 standards.

Findings

The assessor reviewed the configuration of PTS/PED validated devices to ensure that merchants were not able to modify the configuration of the approved devices in a manner that would allow them to bypass encryption or export, view or retrieve clear text cardholder data. Merchants were found to have no access to the encryption process or the ability to decrypt data.

The assessor reviewed the configuration of PTS/PED validated devices to ensure that merchants were not able to access, modify, retrieve, or change encryption keys resident on the device. No function gave merchants access to encryption/decryption keys or the process or ability to decrypt data.

No evidence of unencrypted cardholder data storage on PTS/PED validated devices was observed.

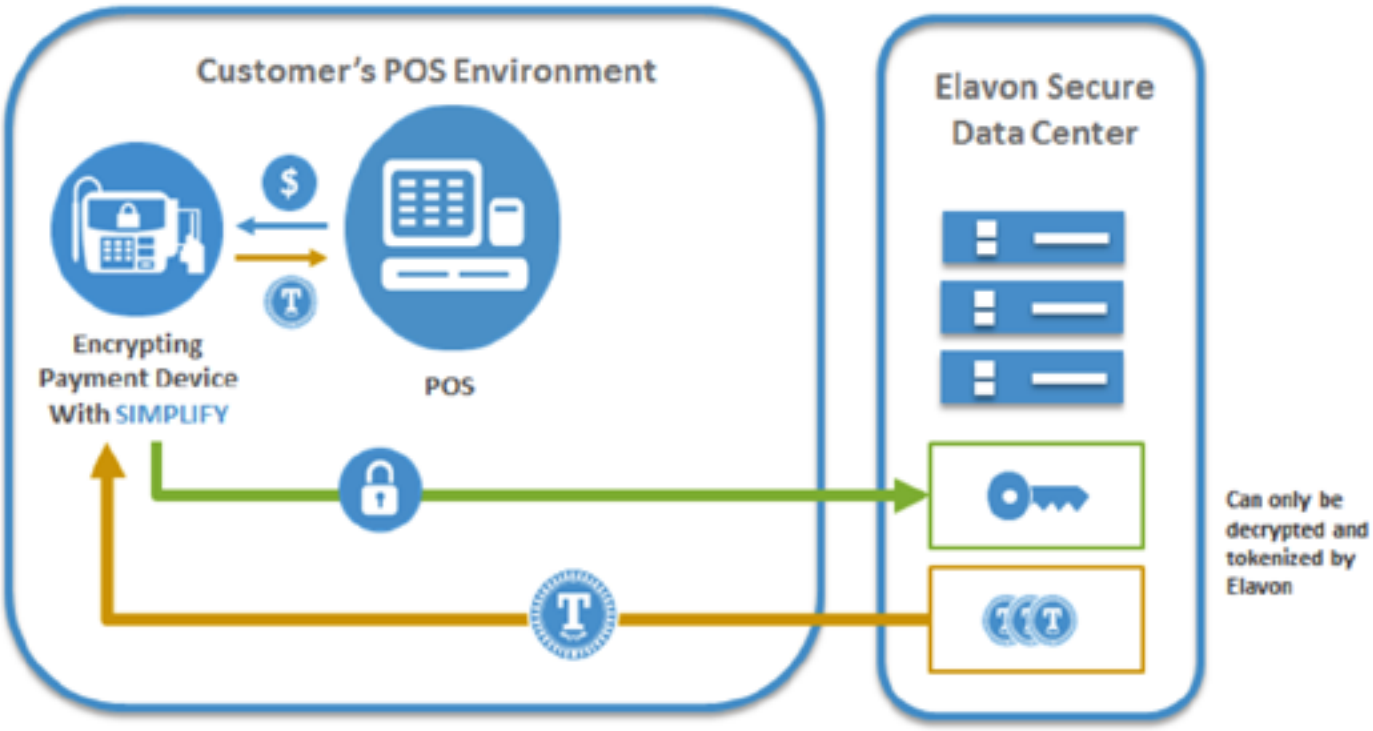
The assessor also reviewed traffic leaving the devices via USB, Serial, and Ethernet to ensure that cardholder data leaving the device was encrypted. Forensics tools were used to search data leaving devices using test transactions with known card numbers. No unencrypted cardholder data was found in any data stream. Transaction information was also analyzed as it returned from the Elavon environment to ensure that clear-text cardholder data was not returned to the merchant location. Only tokens were returned.

One of the unique benefits of Elavon's Simplify solution is the ability for the PCI PTS/PED device to send encrypted data directly to Elavon for payment processing, bypassing any other system or POS in the merchant environment.

The assessor reviewed the traffic entering the Elavon decryption environment at to ensure that encrypted traffic entering Elavon was only entering to a PCI DSS validated environment.

The assessor interviewed a sample of integrators, developers, and project managers at Elavon and validated that no unauthorized individual or merchants had access to decryption keys.

The following diagram shows a flow of cardholder data utilizing the Simplify application on the PTS/PED validated device:



Encryption keys

The Ingenico devices utilize Voltage for encryption of cardholder data. Verifone devices use VeriFone's VeriShield Protect encryption methodology. Verifone utilizes secure key store and pre-injected AES keys for data encryption. Both devices utilized different TDEA DUKPT keys for PIN block encryption and unique keys for each encrypted PIN block based on industry standards for PIN block encryption. Both devices encrypt data in the TRSM. VeriFone adds the additional control of also utilizing the SRED module for data encryption. Both Voltage and VeriShield Protect are well-documented encryption methodologies and used in many PTS/PED implementations throughout the world.

Communication to the Elavon back-end environment is through an IP link directly from the PTS[4] device to the Elavon decryption environment using a secure connection. The decryption environment accepts TLS for incoming connections.

No encryption of cardholder data ever occurs outside the approved PTS devices with Simplify.

Access to encryption keys is restricted to a few key custodians at Elavon who have assumed the responsibility for secure key management. No parties outside the Elavon key custodians and the POS portal key injection facility have access to cardholder decryption keys.

PCI Scope Analysis

For Merchants and QSAs

A merchant implementing a P2PE or E2EE solution still has responsibility for PCI DSS. PCI controls are required in environments or network segments any time cardholder data is stored, processed or transmitted. PCI DSS requires all machines or environments that capture, store, or transmit cardholder data to be evaluated against the PCI DSS requirements.

In the past merchants have been able to reduce the number of network segments and systems required to adhere to the PCI DSS requirements and controls through network segmentation. Network segmentation allows a company to reduce the scope of their assessment by isolating machines and network segments that store, process, or transmit cardholder data from other non-cardholder systems. In a validated P2PE solution, this segmentation is reduced further to the PCI approved and validated PTS card data capture devices used. During a P2PE assessment these devices are validated to be secure and hardened. As such a merchant implementing a validated PCI P2PE solution has the scope of their assessment reduced further to only include the cardholder data capture mechanisms providing they are sufficiently isolated in the merchant environment.

For Simplify, all data leaves the PCI PTS approved capture devices encrypted. As it was validated that no data leaves the device without being encrypted, when implemented correctly Elavon will permit the reduction of the scope of PCI in a merchant environment based on an FAQ issued by the PCI SSC (Payment Card Industry Data Security Standards) titled "Is encrypted cardholder data in scope for PCI DSS?). With appropriate isolation of capture mechanisms and following the PCI DSS 3.0 Requirement 9.9 for periodic inspection of these devices, a merchant may be able to reduce the scope of their PCI DSS, thereby reducing the amount of work necessary to comply with the PCI DSS. Merchants working with a QSA will be able to validate the scope of their PCI DSS utilizing Simplify in their environments.

PCI Council FAQ: "Is encrypted cardholder data in scope for PCI DSS?"

Merchants are required to perform an annual exercise to define the scope of their PCI DSS environment. QSAs are required to validate the scope of the assessment. Merchants using Simplify may be able to reduce the scope of their PCI DSS assessment, as only encrypted data leaves the validated PTS/PED devices. The following PCI SSD FAQ should help merchants and QSAs in defining and validating their PCI DSS scope.

Article URL: https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Is-encrypted-cardholder-data-in-scope-for-PCI-DSS

August, 2012: This FAQ has been updated to eliminate inconsistencies in how the scope of PCI DSS is determined with respect to the presence of encrypted data. This FAQ is intended to clarify that storage of encrypted data

4 With the exception of offline or store and forward transactions

without access to the decryption keys does not automatically result in the data, or the merchant, being out of scope.

October, 2012: This FAQ has been updated to add further clarification based on feedback received from the PCI community.

The scoping guidance in this FAQ is additional to the underlying scoping principles defined in PCI DSS. PCI DSS applies to all system components included in or connected to the cardholder data environment.

Encryption of cardholder data with strong cryptography is an acceptable method of rendering the data unreadable in order to meet PCI DSS Requirement 3.4. Because encrypted data can be decrypted with the right cryptographic key, encrypted cardholder data remains in scope for PCI DSS. Generally, the encrypted data is the responsibility of the entity (that is, the corporation, organization or business being reviewed) that controls and/or has access to the encrypted data and the decryption keys. It is possible that encrypted data may potentially be out of scope for a particular entity if, and only if, it is validated (for example, by a QSA or ISA) that the entity in possession of the encrypted data does not have access to the cleartext cardholder data or the encryption process, nor do they have the ability to decrypt the encrypted data. This means the entity does not have cryptographic keys anywhere in their environment, and that none of the entity's systems, processes or personnel have access to the environment where cryptographic keys are located, nor do they have the ability to retrieve them.

If an entity outsources encryption or key management operations to a third party, the entity is responsible, as part of their due diligence processes, for ensuring that all applicable PCI requirements (for example PTS, PIN, PCI DSS, PA-DSS, and P2PE) for protection of the account data are being met, including the security of any cryptographic operations used to protect the data.

Systems performing encryption and/or decryption of cardholder data, and any systems performing key management functions, are always in scope for PCI DSS. Scope reduction for encrypted data may only be considered when that data is isolated from these processes.

Impact to Merchant Scope

The PCI Data Security Standard PCI DSS version 3.1 was published April 2015. PCI DSS comprises a set of security standards and requirements for protecting account data. The primary account number is the defining factor for cardholder data and the applicability of PCI DSS controls.

In and environment with Simplify, the primary account number is only present when the customer presents the card for payment. Once the PTS/PED device receives the card number it is encrypted and not accessible again until it is processed in the Elavon decryption environment.

The following table from the PCI DSS standard provides a high level overview of the twelve 12 PCI DSS requirements as well where the scope of PCI DSS for merchants may be reduced.

Build and Maintain a Secure Network and Systems	
PCI DSS Requirement 1	How Simplify Helps
Install and maintain a firewall configuration to protect cardholder data	Firewalls are used to protect networks and information passing through them. Simplify never transmits unencrypted cardholder data over networks. Cardholder data is present when a customer presents their card for payment at the PTS/PED device, is encrypted and not accessible again until it enters the Elavon decryption environment.

Build and Maintain a Secure Network and Systems	
PCI DSS Requirement 2 Do not use vendor-supplied defaults for system passwords and other security parameters	How Simplify Helps Elavon installs simplify PCI approved PTS devices that have been hardened and tested with secure configurations. Simplify removes any vendor supplied defaults from the PTS/PED device thereby prohibiting merchants from gaining access to any sensitive information.

Protect Cardholder Data	
PCI DSS Requirement 3 Protect stored cardholder data	How Simplify Helps Simplify does not allow any storage or transmission of cardholder data. Data is encrypted in the PTS/PED device. No merchants have access to decryption keys and data is only decrypted in the Elavon decryption environment. Elavon provides tokens to merchants in the event they need to store data for transactions.
PCI DSS Requirement 4 Encrypt transmission of cardholder data across open, public networks	How Simplify Helps Simplify uses the validated communication protocol of the PTS/PED device to securely transmit traffic from the PED/PTS device to the Elavon decryption environment.

Maintain a Vulnerability Management Program	
PCI DSS Requirement 5 Protect all systems against malware and regularly update anti-virus or programs	How Simplify Helps PTS/PED device manufacturers are require to update devices and firmware when vulnerabilities are found. Simplify program developers monitor threats and update the application as vulnerabilities are found. Simplify uses the latest released version of PTS firmware and the Simplify application to ensure merchants using Simplify are protected against known malware and threats.
PCI DSS Requirement 6 Develop and maintain secure systems and applications	How Simplify Helps Simplify develops applications based on industry best practices for code review and ensures these applications are developed according to PTS/PED vendor security guidelines for application development within the PTS/PED device.

Implement Strong Access Control Measures	
PCI DSS Requirement 7 Restrict access to cardholder data by business need to know	How Simplify Helps Simplify does not allow any access to cardholder data. Cardholder data enters the PTS/PED device, is encrypted, and never revealed again until it enters the Elavon decryption environment.
PCI DSS Requirement 8 Identify and authenticate access to system components	How Simplify Helps The only system where cardholder data resides is on the PTS/PED devices. No merchant or third party has access to those systems.
PCI DSS Requirement 9 Restrict physical access to cardholder data	How Simplify Helps Cardholder data is only ever located in the approved PTS/PED devices. Merchants are still required to maintain the security of their PTS devices.

Regularly Monitor and Test Networks	
PCI DSS Requirement 10 Track and monitor all access to network resources and cardholder data	How Simplify Helps Cardholder data is only ever located in the approved PTS/PED devices. Elavon monitors transactions entering their environment and monitors for anomalies.
PCI DSS Requirement 11 Regularly test security systems and processes	How Simplify Helps PTS/PED manufacturers are required to regularly test security systems and processes. Elavon also tests the security of their application installed on the PTS/PED device.

Maintain an Information Security Policy	
PCI DSS Requirement 12 Maintain a policy that addresses information security for all personnel	How Simplify Helps Merchants should continue to maintain a security policy, risk assessment program, and incident response program.

Conclusion

Simplify isolates unencrypted cardholder data to the PTS/PED validated device in the merchant environment. Cardholder data only enters the approved PTS/PED device, is encrypted, and sent directly to the Elavon decryption environment bypassing[5] all POS systems or other systems in a merchant environment. By allowing only encrypted cardholder data to leave the PTS/PED device, merchants isolate where cardholder data resides in their environment as which reduces their scope of PCI DSS to the PTS devices and environments they reside in. QSAs would be able to validate the scope of the PCI DSS assessment to the merchant environments that contain only PTS/PED devices and POS systems.

5 With the exception of offline or store and forward transactions, which are still encrypted prior to leaving the PTS/PED device.