PCI-Validated P2PE Solutions

Reduced Scope Requires More From Merchants

Payment Card Industry Data Security Standard (PCI DSS) compliance continues to be a hot topic within American businesses today from a couple of different perspectives:

- As useful guidelines intended to help businesses protect sensitive cardholder data and reduce the likelihood of a data breach
- Demands increasingly more time and effort expended away from core business activities.

There's no doubt, data breaches are on the rise. In its most recent 2015 Data Breach Investigation Report, Verizon saw confirmed data breaches in 2014 rise 55% year over year to 2,122 [1]. And though businesses find point-in-time compliance attainable, continuous compliance remains elusive.

> *"Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place."* [2]

No doubt, businesses are challenged with balancing how much time and effort to devote to core business activities and how much should be devoted to upholding continuous compliance standards. To further complicate matters, although the PCI Security Standards Council (PCI SSC) attempts to keep up with the ever-changing security landscape, Verizon recommends that merchants and financial institutions view PCI DSS as a baseline.

> *"Our viewpoint has always been that the PCI DSS is a baseline, an industry-wide minimum acceptable standard, not a pinnacle of payment security."* [2]

To that point, Verizon dispels the myth that demonstrating PCI compliance and passing a PCI DSS assessment are the only due diligence steps needed to proactively reduce the chances of becoming the next headline. Businesses are in need of newer technologies that both reduce risk and help them reduce time and efforts expended on PCI continuous compliance activities. Can PCI-Validated Point-To-Point-Encryption (P2PE) Solutions help them in this regard?

Elavon

Understand The Part You'll Play in Reducing Scope

"P2PE solutions help reduce merchant PCI DSS scope by eliminating clear-text account data from a merchant's environment, or by isolating the P2PE environment from clear-text account data present in other merchant payment channels." [3]

Though employing a PCI-Validated P2PE Solution is not a requirement to attain PCI DSS Compliance, the allure of reducing PCI scope is real. However, the question remains, will it lead to reduced PCI efforts?

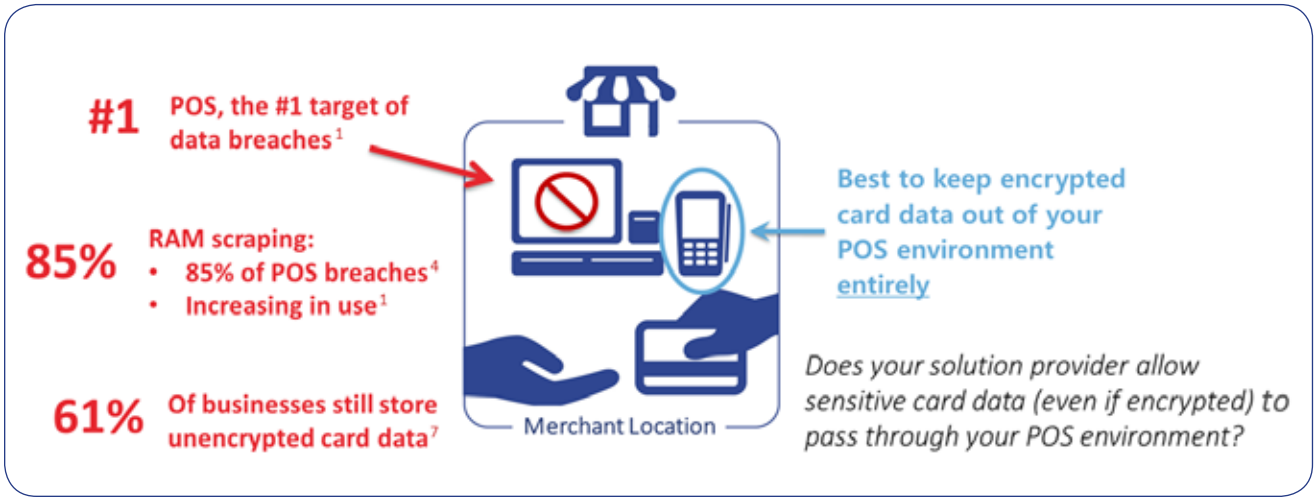
PCI Security Standards Council

Domain 3 Annex: Summary of Contents for the P2PE Instruction Manual (PIM)
This Annex contains a summary of required content for the P2PE Instruction Manual (PIM), as required in Domain 3 (Hardware/Hardware). This Annex contains only those Domain 3 requirements that have related P2PE Instruction Manual (PIM) topics and explains the content for the P2PE Instruction Manual (PIM).

According to Domain 3 of the PCI SSC's P2PE Solution Requirements, the Solution Provider must provide the merchant with an additional set of mandated requirements which consists of 30+ processes the merchant must implement and continuously adhere to in order to support reduced scope[3]. Domain 3 also imposes strict guidelines and policies of payment device inventory management. In other words, reducing PCI scope is not solely reliant upon technology implementation, but upon the merchant committing additional time and effort of their own with no guarantee of reduced scope. Elavon recommends that merchants perform their own due diligence to fully understand the additional time and effort required of them. Reviewing the full set of expectations contained within Domain 3 of the P2PE Solution Requirements would be a good place to start. Additionally, be sure to obtain a copy of the PCI-Validated P2PE Solution Provider's P2PE Instruction Manual (PIM) to fully understand the part you'll play in attaining reduced scope. In this case, you will find that reduced scope requires additional PCI efforts. Are there other ways to reduce scope without the additional mandated effort required with a P2PE validated solution? Ideally, businesses could deploy a solution that reduces PCI scope without the burden of additional PCI efforts.

MYTH: PCI-VALIDATED P2PE SOLUTIONS ARE THE ONLY ENCRYPTION SOLUTIONS THAT REDUCE PCI SCOPE

It is possible to reduce PCI scope without the Solution Provider also adding to your PCI efforts. Today, Qualified Security Accessors (QSAs) are signing off on encryption solutions that offer significant risk reduction without imposing additional PCI efforts upon the merchant. Recall that the definition of P2PE solutions calls for eliminating clear text account data from the merchant's environment[3]. Some vendors address this by encrypting the account data without removing it from the merchant point-of-sales (POS) environment. Even better would be to protect card data by isolating encrypted card data outside the merchant's POS environment entirely, and better yet returning only a token back to the merchant. Elavon encourages you to ask PCI-Validated P2PE solutions providers whether they allow the encrypted card data to pass through the merchant POS environment and if they also tokenize card data.



DUE DILIGENCE CALLED FOR

The decision to employ a PCI-Validated P2PE Solution Provider is not as cut and dry as one might think. At first glance, PCI scope reduction holds promise. But at what cost to your business? As part of the implementation, merchants are called upon to shoulder considerably more cost and effort. Some additional merchant requirements to consider[3]:

- Merchant never stores, processes, or transmits clear-text account data within their P2PE environment outside of a PCI-approved Point of Interaction (POI) device.
- Physical environment controls for POI terminals, third-party agreements, and relevant merchant policies and procedures are in place.
- Merchant has followed the P2PE Instruction Manual (PIM), provided to the merchant by the P2PE Solution Provider.
- Merchant has adequately segmented (isolated) the P2PE environment from any non-P2PE payment channels or confirmed that no other channels exist.
- Merchant has removed or isolated any legacy cardholder data, or systems that stored, processed, or transmitted cardholder data, from the P2PE environment.

Moreover, not all QSAs are qualified to conduct a P2PE assessment. Will there be additional cost associated with utilizing a P2PE QSA?

BUSINESS-LED BEST PRACTICES VS SOLUTION-PROVIDER MANDATED PRACTICES

Elavon fully endorses the intent and spirit of the additional requirements contained within the P2PE Instruction Manual (PIM) and agrees that they are best practices. However, we don't believe that an all-or-nothing set of onerous P2PE Solution requirements is realistic for American businesses to shoulder. Rather, breaking down the full gamut of P2PE Solution requirements into far more attainable components is both more practical and realistic. Each business is different and it's their choice whether to take on the additional overhead associated with PCI-Validated P2PE solutions. It may very well be the right solution for them. At Elavon, we're reluctant to impose additional overhead with uncertain benefits to our customers.

ELAVON'S SOLUTION - REDUCES PCI BURDEN WITHOUT IMPOSING ADDITIONAL OVERHEAD

Elavon's approach to encryption has been strategically designed to completely bypass the existing POS environment, ensuring that at no time does the encrypted cardholder data reside within or pass through the merchant's existing POS environment. Then, once the transaction is authorized, the Elavon solution returns a token in place of card data for subsequent business transactions. In other words, not only does the Elavon solution eliminate clear-text payment card data from a merchant's environment through encryption, it takes it a step further by keeping it out of the merchant's POS environment entirely.

[1] Verizon 2015 Data Breach Investigation Report
[2] Verizon 2015 PCI Compliance Report
[3] "Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware)," PCI Security Standards Council, v 1.1.1, July 2013
[4] Verizon 2014 Data Breach Investigation Report

About Simplify™

Simplify™ is a secure software application that resides on a payment device. Simplify™ securely encrypts card data (manually entered, swipe, tap or insert) at the Point of Interaction and sends the encrypted transaction data to Elavon's payment gateway where a token for the payment card data is created and returned to the POS. Through the Simplify™ application programming interface (API), one can easily isolate sensitive cardholder data from the POS/PMS payment system and reduce card data related compliance headaches.

OTHER FACTORS TO CONSIDER

Criteria	Elavon, Inc. a direct subsidiary of U.S. Bank, National Association	PCI-Validated P2PE Solution Provider
Systems Stability (transaction volume)	$300 billion volume #1 airline processor #2 hospitality processor #4 acquirer[6]	?
Financial Stability	publicly held, 5th largest bank $75 Billion market cap $18 Billion revenues	?
Ethical Stability	US Bank - 2015 Most Ethical Company[5]	?
Customer Attested To Reduced Scope	White Castle	?
QSA Attested To Reduced Scope	Security Metrics	?
Customers	1.3 million customers	?
Employees	3,600 (Elavon)	?
Call Centers	Open 24 x 7 600+ dedicated to customer support	?
Approach to Security	Security first via layered approach with PCI as a security baseline, not the pinnacle.	?

[5] Ethisphere Institute
[6] based on bank card volume
[7] Security Metrics, The Dangers of Storing Card Data

Elavon