The Truth about the X-Charge Secure Method

An X-Charge competitor is currently spreading false and misleading information in the market regarding the scope of Payment Application Data Security Standards (PA-DSS). Under the guise of a market bulletin, they are using an email exchange from the PCI Security Standards Council (SSC) to bolster their case; however, the original question in the email from the competitor is misleading and contains false claims and assertions.

X-Charge has invested significant resources researching, developing, and ensuring that our solutions provide the most secure environment for your merchant customers, while protecting your software development efforts from the need to become a "Payment Application," and undergo the requisite burdens and expense of PA-DSS compliance.

Everyone knows that the best way to keep a secret is not to tell anyone! X-Charge uses that same "need to know" policy when designing systems to protect sensitive cardholder data. An environment which contains only one application or module handling cardholder data provides the highest level of security, minimizes compliance burden, and reduces the opportunity for data breaches.

The SSC has published this best practice in the Payment Application Data Security Standards[1] version 1.2:

> *"Note that it is considered a 'best practice' for software vendors to isolate payment functions into a single or small number of baseline modules, reserving other modules for non-payment functions. This best practice…can limit the number of modules subject to PA-DSS"*

This approach has been validated many times by the Security Standards Council, by Qualified Security Assessors, and most recently by the SSC's Technical Working Group on the floor of the SSC North American Community Meeting held in the Fall of 2009.

The PCI Security Standards Council has made it clear to the industry that the only entities authorized to definitively evaluate particular technologies or implementations for compliance with PCI DSS standards are Qualified Security Assessors. Our competitor is not a QSA. They have not reviewed the X-Charge payment application, or our securely integrated partners. However, authorized QSAs have reviewed X-Charge and substantiated our compliance with best practices and PA-DSS requirements.

[1] Page V, Scope of PA-DSS. https://www.pcisecuritystandards.org/pdfs/pci_pa_dss.pdf

Our competitor claims…

"They are stating that their wrapper integration removes compliance…"

The truth is…

X-Charge's XpressLink secure technology does not rely on being a wrapper, a DLL, or any other specific technology that may be here today and gone tomorrow. We have architected X-Charge in accordance with the standards set forth by the PCI SSC to ensure that your application does not handle sensitive cardholder data. This is the very standard used by the PCI SSC to determine whether an application is in scope.

Our competitor claims…

CAM Commerce Solutions' X-Charge product is not listed on the Security Standards Council's list of PA-DSS validated products.

The truth is…

X-Charge is listed on the Security Standards Council's list of PA-DSS validated products. X-Charge has long been compliant with all industry security standards, including the Visa PABP program before PA-DSS even existed! Our current application compliance information can be viewed at: https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html?mn=C

Our competitor claims…

PA-DSS applies to any business application regardless of whether it stores, processes or transmits cardholder data.

The truth is…

The PCI Security Standards Council has published advice on the scope of PA-DSS for all to review, comment and implement. Here is a direct quote from PA-DSS[2] v1.2 itself:

> *"Scope of PA-DSS*
>
> *The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties."*

[2] Page V, Scope of PA-DSS. https://www.pcisecuritystandards.org/pdfs/pci_pa_dss.pdf

Our competitor claims…

Our competitor implies that a modular approach to application security is invalid, and has been refuted by the SSC.

The truth is…

The SSC has specifically clarified their view on modular applications and PA-DSS scope. The following quote from PA-DSS version 1.2:

> *"PA-DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA-QSA). If other modules also perform payment functions, PA-DSS applies to those modules as well. "*

X-Charge's secure modules and integration methods have been reviewed and confirmed by a PA-QSA as being the only part of the overall business system which is performing payment functions.

Our competitor is offering 'select qualifying software developers' …

'Full funding to get {PA-DSS} validated, which could save you thousands!'

The Truth is…

The real costs of the PA-DSS validation go far beyond what you pay the auditor. They include developing process and implementation documents, source code reviews, and listing on the PCC SSC's List of Validated Payment Applications. A single subsidized assessment may offset initial costs, but it will not offset internal development costs or costs for revalidating major software changes in the future. Additionally, a subsidized assessment will require weeks of time, which is completely unnecessary with X-Charge. The X-Charge Secure Method eliminates all validation costs and time required for the assessment, and provides significant protection against compliance liability associated with potential data breaches.

A subsidized assessment may offset part of the costs of PA DSS, but it leaves software developers with costs, risks and time requirements which can and should be eliminated… with the X-Charge Secure Method.

The Truth is X-Charge is a Validated PA-DSS Payment Application That Takes Your Application "Out of Scope."

The X-Charge Secure Method limits the number of moving parts, and restricts access to cardholder data within a single, highly secure, and PA-DSS validated payment application. Achieving true security and compliance is easier for your merchants because they have fewer systems to manage and monitor, and only one trusted system ever has access to sensitive cardholder data.