



Shift4[®]

Secure Payment Processing

Position Paper on:

PCI Data Security Standards and Visa Payment Application Security Mandates

Authored by Stephen Ames, CISSP

Director, Security and Compliance

September 2009

Disclaimer: The information provided in this position paper is the sole opinion of Shift4 Corporation. This paper is not intended to provide compliance advice or to diminish the efforts of the PCI Security Standards Council or the spirit and intent of the PCI Data Security Standard

Statement

Merchants that correctly implement Shift4® pre-authorization and post-authorization Tokenizationsm technology will dramatically reduce their requisite, internal security control requirements relative to all PCI Data Security Standards and the Visa payment applications security mandates.

Background

The PCI Security Standards Council (SSC) developed the Data Security Standards (DSS) to encourage and enhance Cardholder Data (CHD) security and to facilitate the broad, global adoption of consistent data security measures. The DSS includes 12 security best practices that, when properly implemented, will ensure that CHD is securely processed, stored, and transmitted. The DSS applies to post-authorization CHD.

The PCI Payment Application Data Security Standard (PA-DSS) was also developed by the PCI SSC. The PA-DSS applies to payment application vendors that sell their systems off-the-shelf with minimal customization to more than one merchant. It includes 14 security requirements that must be validated in-place on payment applications before implementation by merchants. The PA-DSS is based on the DSS and includes application development and security best practices.

Visa recently issued a five-phased, payment application security mandate for VisaNet Processors (VNPs), third party agents, and acquiring banks. Phase IV is rapidly approaching and requires VNPs and agents to decertify all vulnerable payment applications within 12 months of identification (effective on October 1, 2009). The final phase is effective on July 1, 2010, and requires acquiring banks to ensure their merchants, VNPs, and agents use only PA-DSS compliant applications.

Discussion

Shift4 technologies include PA-DSS validated applications and operating system level drivers that are not considered payment applications, but rather provide a secure conduit for pre-authorization CHD from the card swipe device to the Shift4 DOLLARS ON THE NETsm data centers. This Shift4 secure conduit, or virtual private network (VPN), is routed around the merchant's payment application, never through it. The emphasis here is pre-authorization CHD, because,

again, the DSS applies only to post-authorization CHD. From the moment a payment card is swiped, that card data is immediately encrypted and securely transported through the Shift4 VPN to the DOLLARS ON THE NET payment service where a Token is generated and sent back to the merchant's payment system. At the end of each transaction the payment system will process for settlement, transmit, and store DOLLARS ON THE NET issued Tokens that consists of the last four digits of the real card number plus 12 randomly generated alpha-numeric characters.

This, in essence, removes any payment application from scope of the DSS, the PA-DSS, and Visa's payment application security mandates because Shift4 PA-DSS validated technologies are doing all the pre/post-authorization CHD heavy lifting and the merchant has no post-authorization CHD anywhere in their payment systems.

What now? Simplify PCIsm compliance for merchants. As an ambassador of the PCI Security Standards Council and a security company itself, Shift4 views the Data Security Standards as a good thing for the Payment Card Industry. The Standards are a set of minimum security best practices that merchants must comply with if they process, store, or transmit post-authorization CHD. But the pragmatic approach for any business entity, and not just merchants, is to be a good citizen on the Internet. Good citizenship on the Internet includes having in place those security best practices described in the Data Security Standards and more. However, if a merchant is not processing, storing, or transmitting post-authorization CHD, just what is in scope for the DSS?

Recommendations

Write language into the Data Security Standards to include breach mitigation technology and processes such as card information replacement technology and Tokenization to reduce CHD hot spots and to eliminate CHD from merchants' payment systems. Create a new self-assessment questionnaire (SAQ) for merchants with payment systems connected to the Internet, but do not process, store, or transmit post-authorization CHD. The new SAQ should include a self-attestation form that defines the merchant's payment system configuration, the type of card information replacement technology in use, and a certification of compliance from a QSA firm.



For more information:

Contact us at
Email: sales@shift4.com
Phone: (800) 265-5795

www.Shift4.com
www.SimplifyPCI.com

1491 Center Crossing Road
Las Vegas, NV 89144-7047
Office: (702) 597-2480

1453 South Dixie Dr., Ste 250
St. George, UT 84770-5854

Support: (866) 980-4446
Sales: (800) 265-5795
Fax: (702) 597-2499