MERCURY®

Help Protect Your Business from a Card Data Breach

What is PCI-DSS?

The Payment Card Industry Data Security Standards (PCI-DSS) are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to help protect cardholder data. The council is responsible for managing the security standards, while compliance with the PCI Security Standards is enforced by the payment card brands. Compliance with the PCI-DSS helps to alleviate data theft and merchant breaches.

What is your responsibility?

Merchant based vulnerabilities may exist almost anywhere in the card-processing environment and data theft is a serious problem. To protect cardholder data and reduce the amount of data breaches, merchants are required to be compliant with the PCI-DSS by the payment card brands and through their card processing agreements with Mercury.

Maintaining compliance is not a single event, but should be a "business as usual" process which includes, (i) selecting an Approved Scanning Vendor (ASV) to perform external network and system scans if applicable, (ii) completing the Self-Assessment Questionnaire also referred to as the SAQ annually, (iii) Using the SAQ to identify and remediate any gaps in compliance with the requirements.

What is PA-DSS?

The Payment Application Data Security Standard (PA-DSS) is the global security standard created by the PCI SSC and was implemented to provide a standard for software vendors developing payment applications that store process, or transmit cardholder data as part of authorization or settlement. The standard was created to prevent payment applications from storing sensitive card data.

If a payment application does not process, store, or transmit cardholder data as part of the payment functions in the application, the developer may be removed from the scope of PA-DSS and therefore PA-DSS is non-applicable to the application.

Is your payment application compliant?

If your payment application developer has integrated with Mercury to provide payment processing and is utilizing point-to-point encryption (P2PE) and tokenization solutions, the payment application may not be transmitting, processing or storing sensitive cardholder data and it may not applicable for the payment application to meet PA-DSS requirements.

What is point-to-point encryption (P2PE)?

Point-to-point encryption (P2PE) solutions are provided by a third party solution provider, and are a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe) until the data reaches the solution provider's secure decryption environment.

Encrypting cardholder data at the time of swipe and throughout the transaction renders the data useless to thieves. Since cardholder data is never exposed or available in the clear past the point of swipe, P2PE significantly reduces the risk of a card data compromise by reducing the opportunity an attacker has to steal clear-text data from their environment.

The foregoing is provided for information purposes only, and is not legal advice. The information provided does not relieve InTouchPOS or it's merchants of its obligations to comply with PCI-DSS. A Payment Application Qualified Security Assessor will need to review the application to make the statement that InTouchPOS is fully removed from the scope of PA-DSS when utilizing Mercury's E2E™. You should review your compliance obligations with your own legal or other advisors.

InTouchPOS

InTouchPOS is now available and incorporates Mercury's P2PE technologies.

- When properly utilized, Mercury's E2E™ encryption (P2PE) helps merchants achieve compliance and maintain a more secure payment processing environment.
- When InTouchPOS is used with E2E, it may be removed from the scope of PA-DSS since cardholder data is not being processed, transmitted or stored in the application.
- While merchants are never fully removed from the scope of PCI- DSS, efforts can be simplified if card data is not stored electronically on the point of sale system.
- Merchants using InTouchPOS exclusively for all transactions, may fill out SAQ-C rather than the lengthy SAQ-D since electronic cardholder data is not stored on the POS.

What is PCI 3.0?

In order to stay current with evolving security threats, the PCI SSC makes updates to the standard on a three-year cycle.

The 3.0 standards will take effect on January 1, 2014, but the 2.0 versions will remain active until the end of 2014 to allow time for organizations to transition their compliance programs.

Resources

For more information on Mercury's integration solutions including E2E™ call 800.846.4472 or visit:

http://www.mercurypay.com/developer-solutions/integration-solutions/security/

Payment Card Industry Data Security Standards:
https://www.pcisecuritystandards.org/

Card Brand Compliance Programs:
http://usa.visa.com
http://www.mastercard.com
http://www.discovernetwork.com