



Control Essentials

PCI: Understanding Your Requirements and Your Role

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements aimed at providing “secure transactions” by enhancing the security of payment account data. The standard was developed by the founding payment brands of the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.

In addition to the PCI DSS, the payment brands recently created the Payment Application Data Security Standard (PA-DSS) based on Visa’s Payment Application Best Practices (PABP). The objective of the PA-DSS is to help payment application vendors develop secure payment applications that support compliance with the PCI DSS.

As PCI DSS compliance continues to evolve and grow in complexity, it is essential that organizations clearly understand where they fall in the PCI compliance world: their role in the play, and what they need to do. Organizations that fail to comply with the PCI standards will be severely fined with consequences to their financial stability, customer trust and reputation.

The Game and the Players

The PCI and the new PA DSS affect all the entities involved in transactions and/or cardholder information flow including the processing, storage, and transmission of such data. However, as a rule of thumb, we can distinguish the following roles:

Cardholders: A cardholder is the owner of a credit card.

Merchants: Merchants are businesses that accept credit cards as a payment method.

Acquirers: Acquirers are entities that acquire transactions and are issued a merchant ID to enable the merchant to accept payments with credit cards. Typically, the acquirer is the merchant bank.

Payment Brands: The payment brands are the 5 credit card brands: American Express, Discover, JCB, MasterCard and Visa.

Issuers: The issuer is the cardholder bank that issues the credit card and receives the cardholder's payment at the end of the billing period.

Service Providers: Service providers are companies that provide services to merchants, acquirers, and/or other service providers. In order to be “in scope” for PCI compliance, the service provider must directly impact the security of cardholder data. Service providers include, but are not limited to the following:



In This Issue...

PCI: Understanding Your Requirements and Your Role

Give Us Your Feedback!

ERM At a Glance

Transaction Processors: Participate in the transaction authorization and/or settlement between merchants, issuers and/or acquirers.

Payment Gateways: Enable transactions between merchants and processors.

Other Service Providers: Credit Reporting Services, Customer Service Functions, Managed firewall and IDS providers, Plastic Card Embossing, etc.

Payment Application Vendors: Payment application vendors are software vendors that develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators).

ASVs, and PCI and PA DSS QSAs: Approved Scanning Vendors (ASVs) are companies that are authorized to perform PCI scanning tests. [Qualified Security Assessors](#) (QSAs) are companies that are qualified to perform PCI and PA DSS reviews. These companies are responsible for proving an opinion regarding whether the PCI and/or PA DSS requirements are being met and documenting the results of the review. It is the QSA's ultimate responsibility to state whether or not compliance has been achieved.

The Rules of the Game

Now that we know who is in the play, let's understand the role of each player and what PCI requires from every one of them.

The Payment Brands

Each Payment Brand defines its own PCI-DSS compliance validation requirements. Payment brands such as American Express, JCB, MasterCard and Visa classify merchants and service providers into levels based on transaction volume.

The Payment Brands also develop and enforce programs related to PA-DSS compliance, including, but not limited to, the following:

- Requirements, mandates, or dates for use of PA-DSS compliant applications
- Fines or penalties related to use of non-compliant payment applications

Acquirers

Acquirers are ultimately responsible for the compliance of all their merchant population. Acquirers must ensure that merchants understand the PCI DSS, keep track of their compliance efforts and provide merchant compliance status to payment brands. In addition, acquirers determine the merchant transaction volume and thus the merchant's level. Sometimes acquirers may also determine the level of service providers.

Merchants & Service Providers

Depending on the level assigned by the acquirer, merchants and service providers will be required to undergo at least one of the following:

1. A network scan performed quarterly by an Approved Scanning Vendor (ASV).
2. An annual onsite review by a Qualified Security Assessor (or internal auditor if signed by an officer of the merchant company).
The onsite assessment requirements entail the following 12 domains:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

3. An Annual Self-Assessment Questionnaire. The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

In relation to the PA-DSS, merchants and service providers that buy or receive a third-party payment application to store, process, or transmit cardholder data as part of authorizing or settling of payment transactions, are responsible for:

- Implementing a PA-DSS compliant payment application into a PCI DSS compliant environment.
- Configuring the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor.
- Configuring the application in a PCI DSS compliant manner.
- Maintaining the PCI DSS compliant status for both the environment and the application configuration.

Payment Application Vendors

A given payment application requires being PA-DSS compliant if it meets the following requirements:

- The payment application is sold and installed “off the shelf” without much customization by software vendors.
- The payment application is provided in modules, which typically includes a “baseline” module and other modules specific to customer types or functions, or customized per customer request. In this case, PA-DSS applies to all the modules that perform payment functions.

PA-DSS does **NOT** apply to:

- Payment applications developed for and sold to only **one** customer. An example of this scenario would be an application designed and developed according to the specifications provided by a single customer.
- Payment applications developed by merchants and service providers if used only in house (not sold, distributed, or licensed to a third party).

However, if PA-DSS compliance is required, vendors are responsible for:

- Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers’ PCI DSS compliance (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement).
- Following PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting).
- Creating a *PA-DSS Implementation Guide*, specific to each application, according to the requirements in the *Payment Application Data Security Standard*.
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS compliant manner.
- Ensuring payment application meet PA-DSS requirements by successfully passing a PA-DSS review.
- Vendors submit their payment applications and supporting documentation to the PA-QSA for review.

Continued on next page...

If resellers and integrators are involved in the sale, installation, and/or service of payment applications on behalf of software vendors, they are responsible for:

- Implementing only PA-DSS compliant payment applications into a PCI DSS compliant environment (or instructing the merchant to do so).
- Configuring such payment applications (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor.
- Configuring such payment applications (or instructing the merchant to do so) in a PCI DSS compliant manner servicing such payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) according to the *PA-DSS Implementation Guide* and PCI DSS.
- Resellers and integrators do not submit payment applications for assessment. Products can only be submitted by the vendor.

Conclusion

The PCI standards have had a great impact on the payment card industry and all the parties involved. The latest PCI DSS (v1.1) with the introduction of the PA-DSS, further enhanced the overall security of credit card transactions to prevent fraud and identity theft crimes. On the other hand, the clock is ticking for all the old and new businesses that need to comply with the PCI standards. PCI compliance projects can be time consuming and very demanding in terms of resources. Requirements such as the network segmentation and encryption of payment account data flow can cause some serious headaches to organizations that have not yet properly implemented their credit card processing environment. Therefore, organizations should chart out their compliance plan ahead of time in order to avoid bumping into delays that could compromise the compliance process and objective as a whole.

Enterprise Risk Management: *At a Glance*

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions. Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

Services

IT Security
Regulatory Compliance
IT Audit
Computer Forensics
Risk Management
Attestation

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Qualified Security Assessor (QSA)
Approved Scanning Vendor (ASV)

Some of our Clients

ABN-AMRO Private Banking
Bacardi-Martini, Inc.
Bancafe International
Banco Industrial de Venezuela
Banco ITAU
Bank United
Carnival Cruise Lines, LLC
CitiBank
Coconut Grove Bank
Commerce Bank
E-data Financial
Florida International University
Florida Power & Light Company
Heico Aerospace
Helm Bank
Knight Ridder
Nova Southeastern University
Rinker Materials
Rudy, Exelrod & Zieff, LLP
TecniCard, Inc.
The International Bank of Miami
TransAtlantic Bank