



This white paper is one of many articles prepared by Skipjack to help merchants and developers get the most out of payment processing. To view others, please visit www.skipjack.com.

The Payment Card Industry Data Security Standard

An Introductory Overview



THE PAYMENT SOLUTIONS *EXPERTS*

In an effort to provide a uniform and effective standard for improving the security of cardholder information, the various credit card associations have joined together to launch three important security standards: PCI-DSS, PA-DSS and PED. Understanding these three standards, their requirements and their implications, is critical for merchants and their customers. The consequences of non-compliance can range from hefty fines to loss of credit card acceptance privileges. With this in mind, the following summary has been prepared to provide a high-level overview of the standards and their impacts on the various stakeholders.

What is PCI-DSS?

PCI-DSS stands for **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard. The primary objective of PCI-DSS is to establish a set of requirements to protect cardholder information. *Any merchant or service provider that stores, processes, or transmits cardholder payment data is required to be PCI compliant.* In addition, there are requirements for software developers (PA-DSS) and certain hardware device manufacturers (PED Standard) that participate in the transaction process. PCI-DSS compliance is mandatory for the respective parties involved. PCI-DSS encompasses 6 key areas with a total of 12 requirements (see table “PCI-DSS 12 Requirements”).

Merchants and service provider PCI-DSS compliance requirements are categorized according to the number of card transactions they process over a 12-month period. Their category will determine whether an onsite data security assessment is required or whether a self-assessment is possible, and how frequently the network must be scanned for vulnerabilities. *It is important that you understand which category applies to your business and what your specific requirements are.*

PCI-DSS Twelve Requirements	
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 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

What is PA-DSS?

PA-DSS stands for **P**ayment **A**pplication **D**ata **S**ecurity **S**tandard. PA-DSS applies to all applications used to store, process, or transmit cardholder data as part of the authorization or settlement cycles. The objective of PA-DSS is to reduce the risk of compromise of prohibited card data (e.g. full card magnetic stripe data or other data contained on the back of the card). Commercial payment applications, integrators and service providers are governed under PA-DSS. PA-DSS highlights 14 requirements which address the requirements in PCI-DSS that are specific to payment applications, or could be impacted by a payment application. Merchants are mandated by the various card brands to use certified payment applications. Merchants are directed to check with their acquiring financial institution to verify if an application is considered compliant.

PA-DSS Requirements	
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data.	8. Facilitate secure network implementation.
2. Protect stored cardholder data.	9. Cardholder data must never be stored on a server connected to the Internet.
3. Provide secure authentication features.	10. Facilitate secure remote software updates.
4. Log payment application activity.	11. Facilitate secure remote access to payment application.
5. Develop secure payment applications.	12. Encrypt sensitive traffic over public networks.
6. Protect wireless transmissions.	13. Encrypt all non-console administrative access.
7. Test payment applications to address vulnerabilities.	14. Maintain instructional documentation and training programs for customers, resellers, and integrators.

What is the PIN Entry Device (PED) Security Requirement?

This requirement, commonly referred to as PED, is applicable to devices that are used in the process of entering a PIN code during the transaction process. The PED Security Requirements focus on Device Characteristics and Device Management. Device Characteristics can be classified as either Physical Security Characteristics (ones that prevent the device from being stolen from the installed location) or Logical Security Characteristics (functional capabilities). Device Management focuses on the management of the device during manufacturing, logistics involved with encrypting the device, and with the delivery and storage of the device. The Device Management requirement is designed to prevent unauthorized modifications to the physical or logical security characters of the device. Merchants and service providers are required to use devices that are certified as PED compliant.

Skipjack's Role

Skipjack is classified as a Service Provider, and is therefore required to maintain PCI-DSS compliance. Using a PCI-DSS compliant service provider, such as Skipjack, provides the merchant with the ability to supply proof of the service provider's PCI-DSS compliance in order to meet certain aspects of the merchant's PCI-DSS requirements. It does not, however, remove a merchant from the requirement to comply with other aspects of PCI-DSS.

Integration of Skipjack into a payment application, such as a Shopping Cart or Point-of-Sale system, does not guarantee PA-DSS certification. *Creators of applications that handle credit card information must still go through the PA-DSS process and pass certification.* Once certified, these applications are subject to review on an annual basis.

Summary

Merchants, Service Providers, and Hardware and Software developers are encouraged to review the PCI-DSS / PA-DSS / PED standards and determine the impact these standards have on their solutions. Skipjack provides the tools and knowledge to simplify the process of compliance for all stakeholders.

A summary of how the three payment compliance standards impact the various participants involved in the payments process follows:

Participant	PCI-DSS	PA-DSS	PED
Merchant	Must adhere to PCI-DSS guidelines based on their transaction volume	Must use PA-DSS compliant application software or have compensating controls in place	Must utilize PED Compliant devices
Payment Gateway	Must adhere to PCI-DSS guidelines regardless of transaction volume	Ensures that applications connected to the payment gateway are PA-DSS certified	Ensures that PED Compliant devices are used in conjunction with their service or third party applications connected to the payment gateway
Application Developer	See PA-DSS	Must meet PA-DSS requirements. Applications installed in a PCI-DSS environment can not cause the environment to be non-compliant with PCI-DSS requirements	Ensures that PED Compliant devices are used in conjunction with their applications
PIN Entry Hardware Manufacturer	See PED	See PED	Must Maintain PED compliance

Please note that this document should not be construed as the definitive guide to PCI-related requirements. Its intention is merely to provide summary information. Many resources exist that provide comprehensive and up-to-date information. We strongly suggest that you refer to these resources, as the requirements are subject to change. A starting point for additional information includes:

1. PCI Council: <https://www.pcisecuritystandards.org/>
2. Visa: www.visa.com/cisp
3. MasterCard: www.mastercard.com/us/sdp/index.html
4. Amex: www10.americanexpress.com/sif/cda/page/0.1641.17457.00.asp
5. Discover: www.discovernetwork.com/fraudsecurity/disc.html
6. JCB: www.jcb-global.com/english/pci/index.html