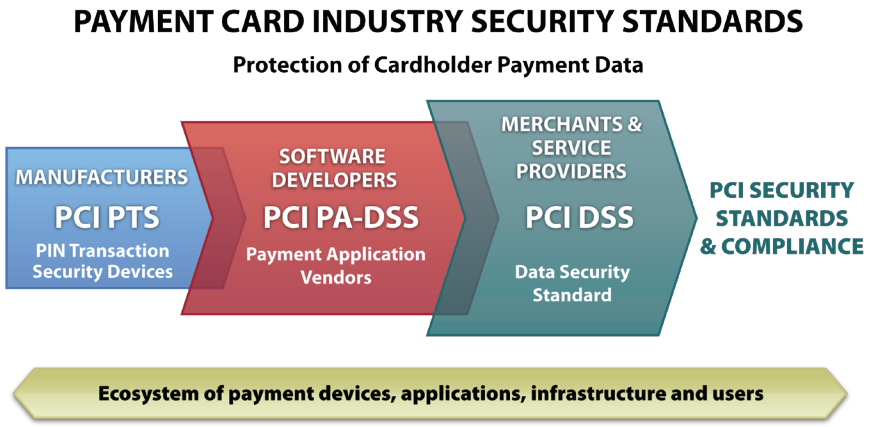
Payment Card Industry Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.



PCI Standards Include:

PCI Data Security Standard: The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

PIN Transaction Security Requirements: The PCI PTS applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions.

Payment Application Data Security Standard: The PA-DSS is for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement. It governs these applications that are sold, distributed or licensed to third parties.

PCI SSC Founders

American Express
Discover
JCB
MasterCard Worldwide
VISA

Participating Organizations

Merchants, banks, processors, developers and point-of-sale vendors

PCI Data Security Standard for Merchants & Processors

The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

COMPLIANCE PROGRAM

Assessing

Test and verify controls in place to protect cardholder data during storage, processing and transmission. Systems and data must be available for analysis.

Reporting

Validate compliance and present evidence that data protection controls are in place.

Monitoring & Alerting

Implement systems that provide auto-alerting to constantly monitor access and usage of data.

Extend system controls to include collection and storage of log data.

How to Comply with PCI DSS

The PCI Security Standards Council sets the standards for PCI security but each payment card brand has its own program for compliance. Specific questions about compliance should be directed to your acquiring financial institution. Links to payment card brand compliance program include:

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp (U.S.)

Qualified Assessors. The Council provides programs for two kinds of certifications: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are companies that assist organizations in reviewing the security of its payments transaction systems and have trained personnel and processes to assess and validate compliance with PCI DSS and PA-DSS. ASVs provide commercial software tools and analysis services to perform certified vulnerability scans for your systems. The PCI SSC also provides educational resources to further security awareness for merchants and service providers, including training for Internal Security Assessors (ISAs). Additional details can be found on our Web site at: www.pcisecuritystandards.org.

Self-Assessment Questionnaire (SAQ). The SAQ is a validation tool for eligible merchants and service providers who self-assess their PCI DSS compliance. Different SAQs are available for various business environments; more details can be found on our web site at: www.pcisecuritystandards.org, or contact the acquiring financial institution or payment brand to determine if you should complete an SAQ.

Payment Application Data Security Standard for Developers

The PA-DSS minimizes vulnerabilities in payment applications. The goal is to prevent the compromise of full magnetic stripe data located on the back of a payment card or equivalent data from a chip. PA-DSS covers commercial payment applications, integrators and service providers. Merchants and service providers should use certified payment applications and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.

Payment Application DSS Requirements – Validated by PA-QSA Assessment	
1. Do not retain full magnetic stripe, card verification 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 access to payment application
4. Log payment application activity	11. Encrypt sensitive traffic over public networks
5. Develop secure payment applications	12. Encrypt all non-console administrative access
6. Protect wireless transmissions	13. Maintain instructional documentation and training programs for customers, resellers, and integrators
7. Test payment applications to address vulnerabilities	14. Maintain instructional documentation and training programs for customers, resellers and integrators

PIN Transaction Security (PTS) Requirements for Manufacturers

This standard, referred to as PTS, applies to companies which make devices that accept personal identification number (PIN) entry for all PIN-based transactions. Merchants and service providers should use PTS approved devices and should check with their acquiring financial institution to understand requirements and associated timeframes for compliance.

PTS Evaluation Module Groupings	
Evaluation Module	Requirements Set
1. Core Requirements	Physical and logical security
2. POS Terminal Integration	POS terminal integration
3. Open Protocols	Open protocols
4. Secure Reading and Exchange of Data	Requirements in support of cardholder account data encryption
5. Device Management	Device management (manufacturing and initial key loading)