PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL (PCI SSC)

An Open Global Forum

Founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc., the PCI SSC is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.

PCI SSC Mission

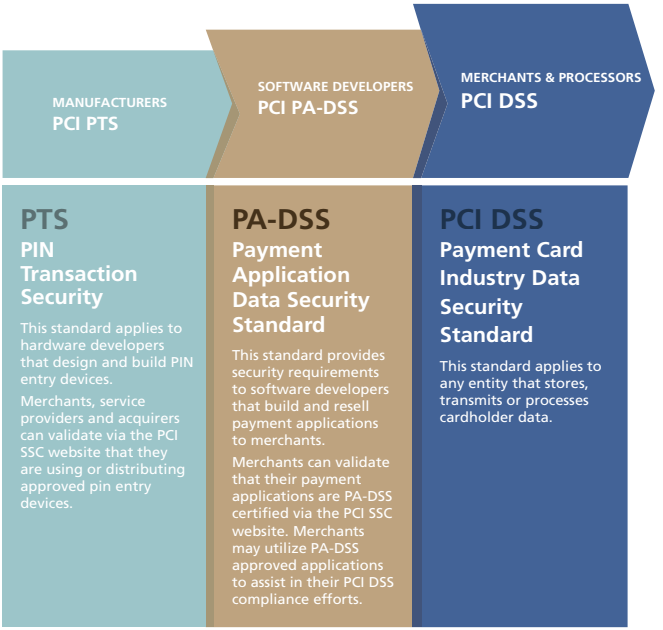
The mission of the PCI SSC is to enhance payment account data security by driving education and awareness of the PCI Security Standards (including the Data Security Standard [DSS], Payment Application Data Security Standard [PA-DSS], and PIN Transaction Security [PTS] Requirements) globally.

Participating Organizations

The PCI SSC encourages merchants, processors, Point-of-Sale (POS) vendors, and financial institutions to actively participate in the standards lifecycle and revisions process, vote for the Board of Advisors, and attend the annual community meetings.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



PCI Security Standards and Compliance

Landscape of payment devices, applications, infrastructure, and users

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

Prevent, Detect, and React

A successful business makes security its top priority, thereby giving assurance to its customers that their transactions are protected. That's why MasterCard and the other payment brands developed the PCI DSS.

The PCI DSS comprises technical and operational requirements established by the PCI SSC to protect cardholder data and to prevent, detect, and react to potential account data compromise. The PCI DSS applies to any entity that stores, processes, or transmits cardholder data. With over 250 sub-requirements, the PCI DSS can be sorted at a high level into six best practices and 12 main requirements.

Six Goals, 12 Requirements

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 cardholder data 4: Encrypt transmissions of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5: Use and regularly update anti-virus software 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 additional resources, please visit www.pcisecuritystandards.org

MasterCard
Worldwide

MASTERCARD SITE DATA PROTECTION PROGRAM (SDP)

Compliance Provides Security and Confidence

The SDP Program, with the PCI DSS as its foundation, details the data security requirements and compliance validation requirements to protect stored and transmitted MasterCard payment account data.

The SDP Program is designed to identify vulnerabilities in security processes, procedures, and Web site configurations. PCI DSS compliance and subsequent compliance with the SDP Program mandate, helps merchants, Service Providers, and customers protect themselves against security breaches, enhance consumer confidence, and protect the integrity of the overall payment system.

PCI Compliance

PCI Self Assessment
PCI Onsite Assessment
PCI Quarterly Network Scanning
PCI Compliant Payment Application

A merchant or Service Provider that has successfully completed the above relevant validation tools and achieved compliance with the PA-DSS as applicable, is compliant with the PCI DSS

SDP Compliance

Acquirer validation of the merchants' applicable compliance validation tools

Acquirer reporting of merchant or service provider with MasterCard

A merchant or service provider that has successfully completed the above steps is compliant with the PCI DSS AND compliant with the MasterCard SDP Program requirements

New PCI Payment Application (PA-DSS) Compliance Mandate effective 1 July 2012

MasterCard has adopted a new PCI PA-DSS mandate. All merchants and service providers that use third party-provided payment applications must only use payment applications that are compliant with the PCI PA-DSS, as applicable.

SDP Merchant Levels

Category	Criteria	Requirements	Compliance Date
Level 1	• Any merchant that has suffered a hack or an attack that resulted in an account data compromise • Any merchant having more than six million total combined MasterCard and Maestro transactions annually • Any merchant meeting the Level 1 criteria of Visa • Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	• Annual Onsite Assessment[1] • Quarterly Network Scan conducted by an ASV[2]	• 30 June 2011[3]
Level 2	• Any merchant with more than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually • Any merchant meeting the Level 2 criteria of Visa	• Annual Self-Assessment[4] • Onsite Assessment at Merchant Discretion[4] • Quarterly Network Scan conducted by an ASV[2]	• 30 June 2011
Level 3	• Any merchant with more than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually • Any merchant meeting the Level 3 criteria of Visa	• Annual Self-Assessment • Quarterly Network Scan conducted by an ASV[2]	• 30 June 2005
Level 4	• All other merchants[5]	• Annual Self-Assessment • Quarterly Network Scan conducted by an ASV[2]	• Consult Acquirer

[1]Effective 30 June 2011, Level 1 merchants that choose to conduct an annual onsite assessment using an internal auditor must ensure that primary internal auditor staff engaged in validating PCI DSS compliance attend PCI SSC-offered merchant training programs and pass any PCI SSC associated accreditation program annually in order to continue to use internal auditors.

[2]Quarterly network scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV).

[3]Initial compliance date for Level 1 merchants has passed. 30 June 2011 affects merchants that choose to conduct an annual onsite assessment using an internal auditor.

[4]Effective 30 June 2011, Level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC-offered merchant training programs and pass any associated PCI SSC accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA) rather than complete an annual self-assessment questionnaire.

[5]Level 4 merchants are required to comply with the PCI DSS. Level 4 merchants should consult their acquirer to determine if compliance validation is also required.

SDP Service Provider Levels

Category	Criteria	Requirements
Level 1	• All Third Party Processors (TPPs) • All Data Storage Entities (DSEs) with more than 300,000 total combined MasterCard and Maestro transactions annually	• Annual Onsite Assessment conducted by a QSA[1] • Quarterly Network Scan conducted by an ASV[2]
Level 2	• All DSEs with 300,000 or less total combined MasterCard and Maestro annual transactions annually	• Annual Self-Assessment • Quarterly Network Scan conducted by an ASV[2]

[1]All Level 1 Service Providers must complete an annual onsite assessment conducted by a PCI SSC certified QSA

[2]Quarterly network scans must be conducted by a PCI SSC ASV.

For additional resources, please visit www.mastercard.com/sdp

To contact us, please send an e-mail to sdp@mastercard.com

MASTERCARD PCI 360 EDUCATION PROGRAM (PCI 360)

Helping You Help Your Customers

In an effort to increase awareness and promote adoption of the PCI DSS, MasterCard offers complimentary PCI education opportunities for acquirers as well as their merchants and service providers.

PCI 360 is designed to familiarize participants with the PCI DSS and better enable acquirers, merchants, and service providers to collaborate in implementing and managing effective PCI compliance programs.

PCI 360 Benefits

- The ability to provide merchants with a holistic view of the PCI DSS to increase their knowledge of the requirements and potential benefits
- Complimentary webinar series to provide merchants and service providers with the information that will help them on their journey toward becoming PCI compliant at **www.mastercard.com/pci360**
- Customized programs available face-to-face or on the Web to fit your client's needs
- Tools to help increase compliance rates and reduce the risk of account data compromise
- Access to industry security experts
- Networking opportunities with merchants and service providers

PCI 360 ON DEMAND WEBINAR SERIES

On Demand at Your Convenience

- The Cost of Account Data Compromise
- Merchant Mayhem: Wireless Encryption and Wireless Threat Identification
- SDP Compliance and the Prioritized Approach (Spanish)
- The PCI Security Standards Council
- A Merchant's Journey Toward Compliance
- Understanding Account Data Compromise
- Preparing for a Successful PCI Assessment, Lessons from the Field
- Reducing Your Risk: A Look into PCI Vulnerability Scanning
- A Look at the New Self-Assessment Questionnaire
- Network Segmentation
- Maximize Internal Preparations for PCI DSS
- Data Encryption: Understanding Encryption and PCI DSS
- The PCI Requirements
- Data Storage
- PCI Perspectives: Service Provider
- PCI Perspectives: PA-DSS Vendor

Coming in 2010:

- MasterCard and the Payment Card Industry
- Implementing Requirements as Part of Your Policies and Procedures
- Building Secure Applications
- Application Security – Protecting Your Custom Applications from Attack

To view the series, please visit www.mastercard.com/pci360

To contact us, please send an e-mail to pci_education@mastercard.com