



MasterCard
Worldwide

MasterCard PCI & Site Data Protection (SDP) Program Update

The Payment Card Industry Security Standards Council (PCI SSC)



Open, Global Forum
Founded 2006

Responsible for PCI Security Standards

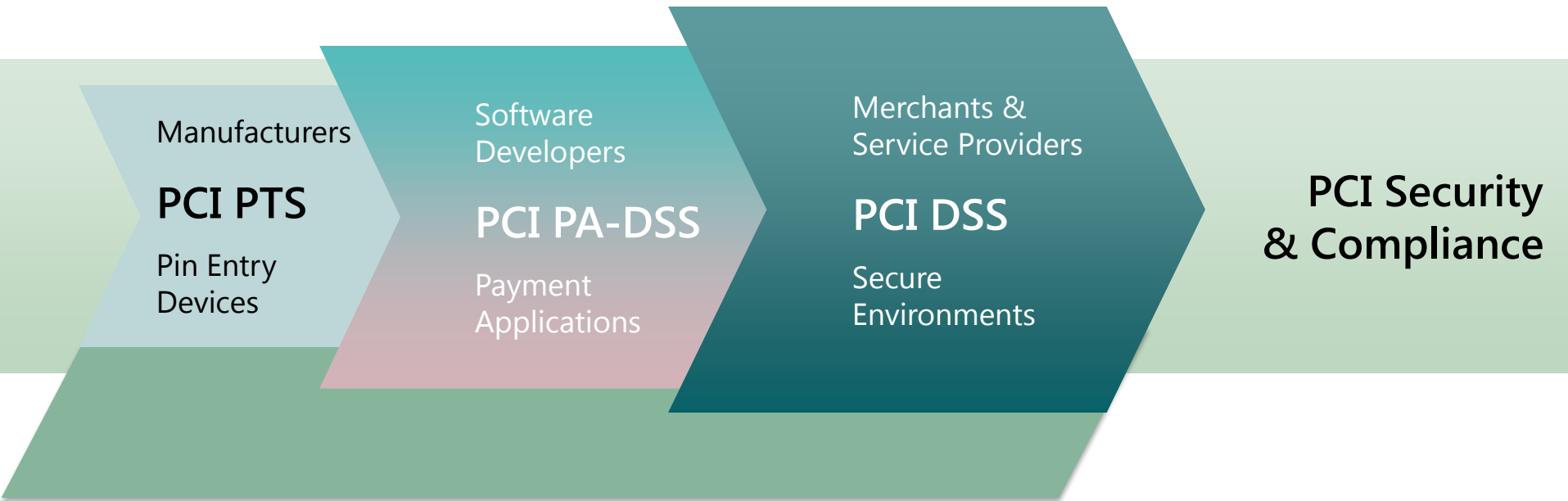
- Development
- Management
- Education
- Awareness



PCI Security Standards



Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

PCI DSS, PCI PA, PCI PTS, PCI P2PE...



Payment Card Industry (PCI)
Data Security Standard



Payment Card Industry (PCI)
PIN Security Requirements



Payment Card Industry (PCI)
Payment Application Data Security Standard



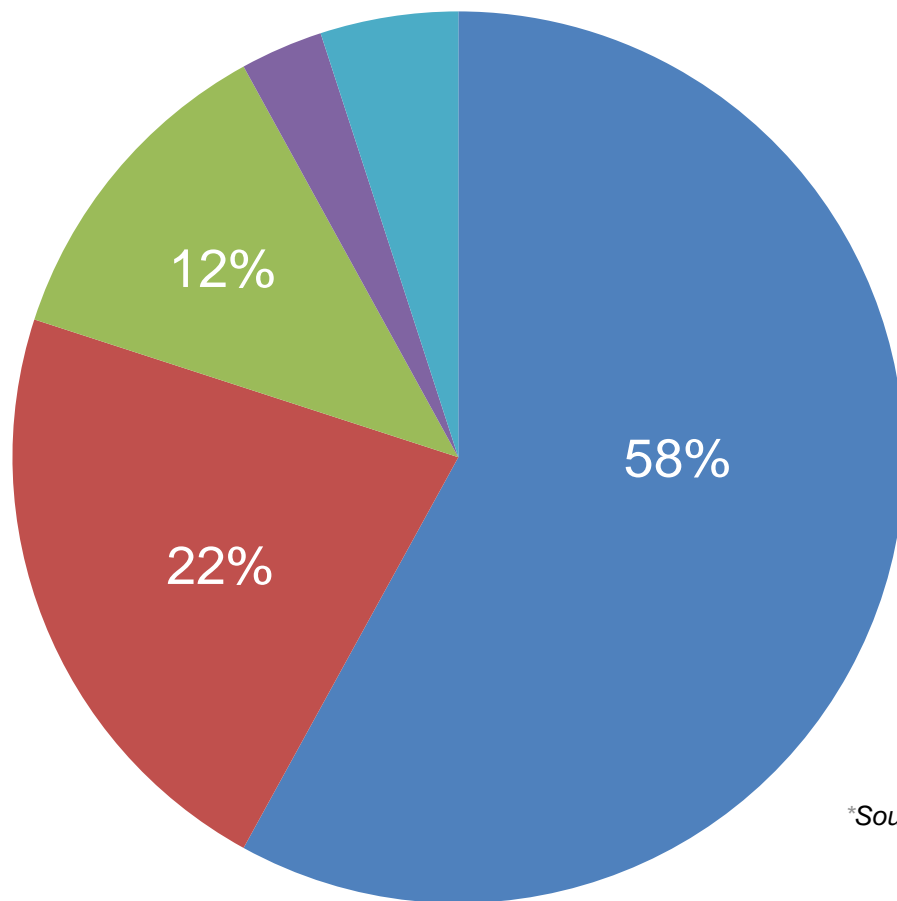
Payment Card Industry (PCI)
Data Security Standard

PCI DSS Applicability in an EMV Environment
A Guidance Document
Version 1
Release Date: 5 October 2010



Payment Card Industry (PCI)
Point-to-Point Encryption

Top Cyber attack and Data Breach Worries

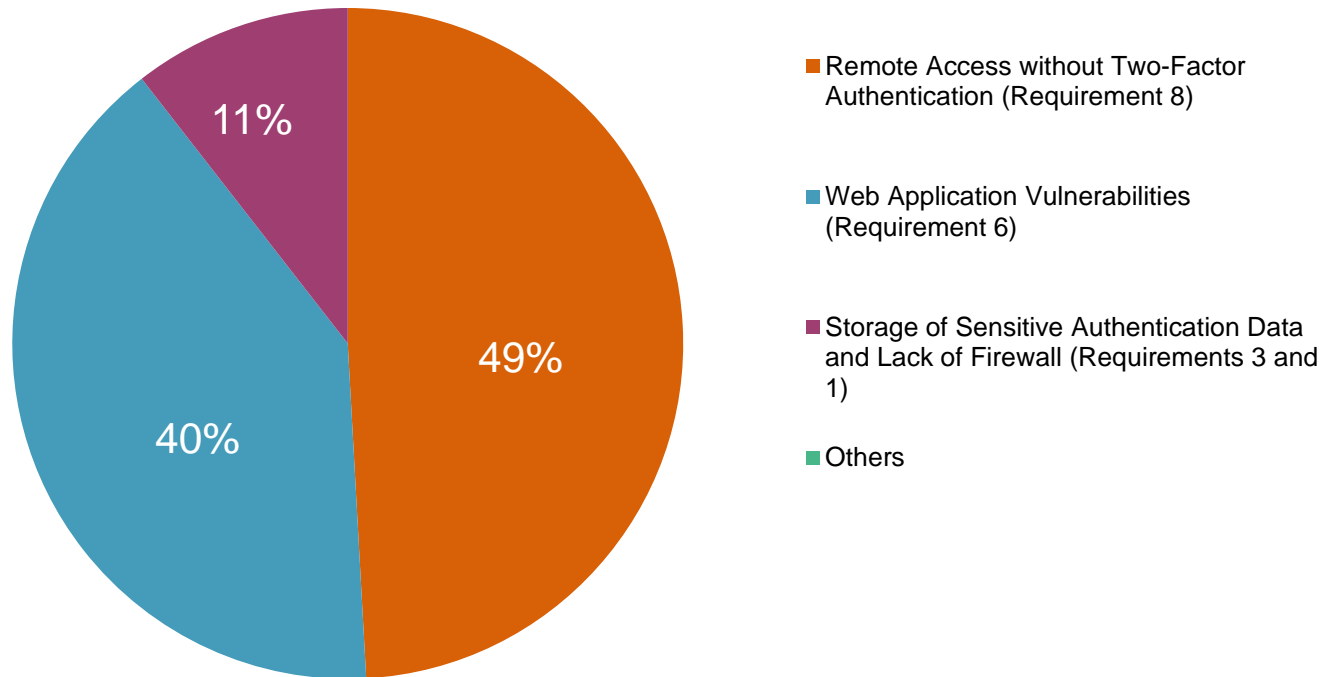


Data loss worries IT pros more than reputation damage, fines and legal action, but 3 out of 4 think their organization is safe.*

- Customer Data Theft 58%
- Intellectual Property Theft 22%
- Reputation Damage 12%
- Fines or Legal Action 3%
- Won't Fall Victim 5%

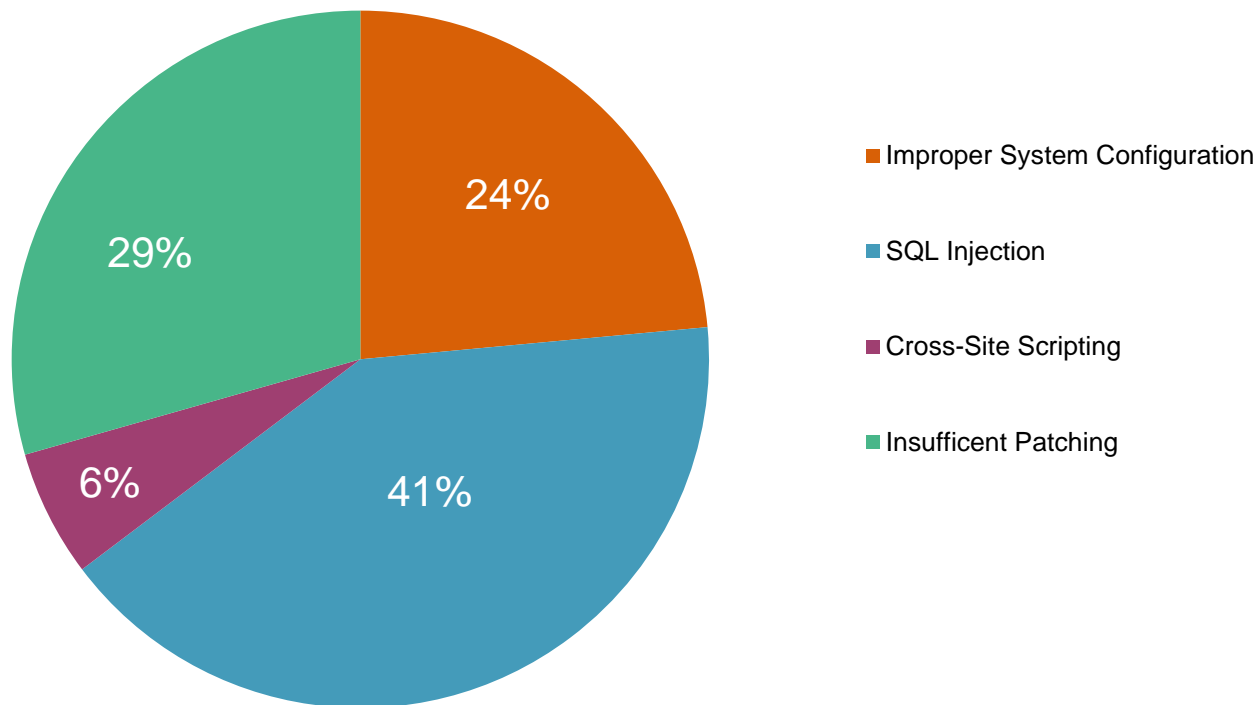
**Source: Trustwave 2014 Security Pressures Report*

PCI Vulnerabilities Leading to ADC Breaches (2013)



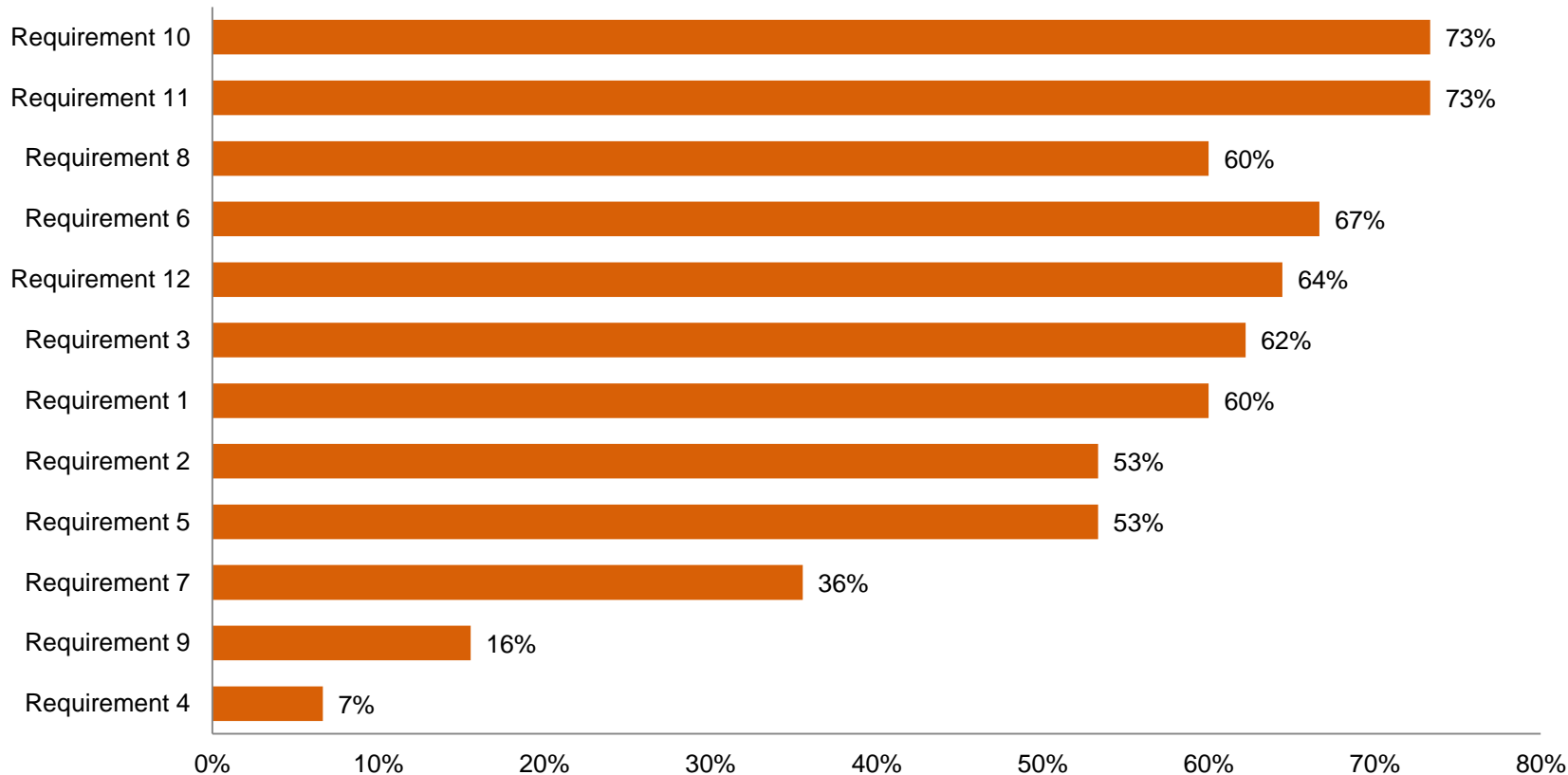
Source Data: MasterCard investigated Account Data Compromises resulting in forensic investigations with conclusive evidence of a security breach

Primary Attack Vector for e-Commerce Merchants (2013)



Source Data: MasterCard investigated Account Data Compromises resulting in forensic investigations with conclusive evidence of a security breach

PCI Requirements Not “In-Place” at Time of Breach (2013)



Source Data: MasterCard investigated Account Data Compromises resulting in forensic investigations with conclusive evidence of a security breach

PCI DSS - Six Goals, Twelve Requirements



Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors

Maintain Secure Environments

Why we fail to maintain secure Environments ?

- Lack of awareness by IT practitioners
- Incentive to keep security a primary focus
- Quickly evolving technology landscape
- Rapid development and distribution of new solutions
- Still unnecessary exposure of card holder data



MasterCard
Worldwide

Briefing on Changes with PCI V3.0

Short Briefing on Changes with PCI V3.0



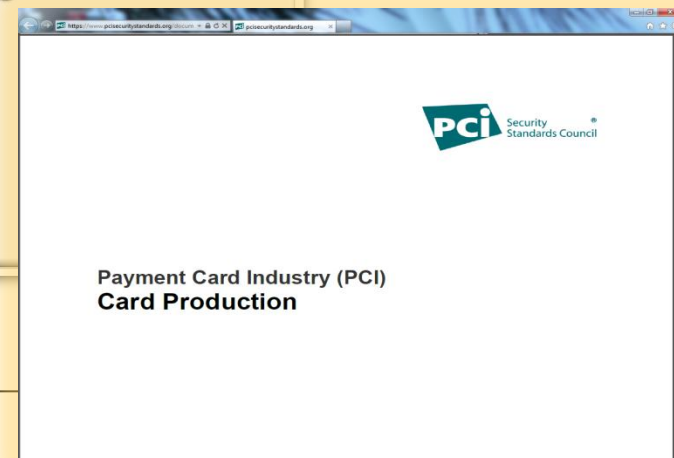
- 12 core security principles of PCI DSS remain the same
- Several new sub-requirements that will impact PCI DSS security efforts*
- Future implementation dates provided for more significant changes
- Clarified PCI DSS Applicability
- Enhanced testing procedures to clarify level of validation expected for each requirement
- Aligned language between requirements and testing procedures for consistency
- Instructions for Report on Compliance (ROC) reporting now separate ROC reporting template

New MC Requirement for Card Vendors under PCI Changes with PCI V3.0



Card Vendor Certification Standards

22 November 2013



Site Security Compliance *



Compliance Certificate

MasterCard Global Vendor Certification Program




Certificate of Compliance



Certificate Holder:
Sample
 Address line 1
 Address line 2
 City 12345
 Country

MasterCard hereby confirms that the security configuration of your premises located at the address stated above is in compliance with the MasterCard Physical Security Standards for Plastic Card Vendors and Logical Security Requirements for Card Personalization. As a result, the MasterCard Certification Body has issued this certificate valid until April 30, 2013 confirming authorization to perform the following checked card production activities. The stated location is not authorized to perform services that are not checked.

Card Manufacturing Chip Embedding	<input checked="" type="checkbox"/> Card Personalizing
	<input checked="" type="checkbox"/> Card Embossing
	<input checked="" type="checkbox"/> Card Encoding
<input checked="" type="checkbox"/> Mobile Provisioning	<input checked="" type="checkbox"/> Chip Personalizing
	<input checked="" type="checkbox"/> Card Mailing

Werner Fischer <small>On behalf of MasterCard</small>	December 22, 2011 Issuance Date	1101172 Certificate Number	
MasterCard Worldwide 2000 Purchase Street Purchase, New York 10577 USA	April 30, 2013 Expiration Date	12345 ICA Number	  

- *) NEW Vendor's categories:
- Vendors
 - Specialized Vendors
 - Suppliers

Briefing on Changes with PCI V3.0



Effective Dates for v3.0 PCI DSS

Version 3.0 was effective on 1 January 2014

Version 2.0 is valid until 31 December 2014

Different supporting documents:

- New AOC,
- Reporting Template,
- SAQ

Check our website for the latest documents

Do not mix and match



MasterCard
Worldwide



MasterCard Site Data Protection (SDP) Program

PCI SSC's Role vs. MasterCard's Role in Data Security



MasterCard expects acquirers to actively deploy a PCI program for their merchants and to manage compliance as an ongoing concern and performs the following functions **independent** of the PCI SSC

- **PCI compliance tracking and enforcement**
- **Approval and posting of compliant the service providers (TPP and DSE)**
- **Forensics and response to Account Data Compromise (ADC) events**

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

PCI and SDP Compliance



PCI Compliance

- PCI Onsite Assessment
- PCI Self Assessment
- PCI Quarterly Network Scanning

The successful completion of the above applicable compliance requirements means the merchant is compliant with the PCI Data Security Standard.

SDP Compliance

- Compliance Validation with Acquirer
- Quarterly Merchant Reporting via the SDP Acquirer Submission and Compliance Status Form

The successful completion of the above compliance requirements means the merchant is compliant with the PCI Data Security Standard AND compliant with the MasterCard SDP Program requirements.

MasterCard PCI compliance Merchant Level Definitions (based on annual MC transaction volume)



Category	Criteria	Validation Requirements	Compliance Date
Level 1	<ul style="list-style-type: none"> Any merchant that has suffered a hack or an attack that resulted in an account data compromise Any merchant having greater 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 	<ul style="list-style-type: none"> Annual Onsite Assessment (ISA)¹ Quarterly Network Scan conducted by an ASV³ 	30 June 2011 ⁵
Level 2	<ul style="list-style-type: none"> Any merchant with greater 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 	<ul style="list-style-type: none"> Annual Self-Assessment² Onsite Assessment at Merchant Discretion² Quarterly Network Scan conducted by an ASV³ 	30 June 2011
Level 3	<ul style="list-style-type: none"> Any merchant with greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro ecommerce transactions annually Any merchant meeting the Level 3 criteria of Visa 	<ul style="list-style-type: none"> Annual Self-Assessment Quarterly Network Scan conducted by an ASV³ 	30 June 20'05
Level 4	<ul style="list-style-type: none"> All other merchants⁴ 	<ul style="list-style-type: none"> Annual Self-Assessment Quarterly Network Scan conducted by an ASV³ 	Consult Acquirer

¹Effective 30 June 2011, Level 1 merchants that choose to conduct an annual onsite assessment using an internal security assessor (ISA) 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.

²Effective 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 QSA rather than complete an annual self-assessment questionnaire.

³ Quarterly Network Scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV).

⁴ Level 4 Merchants are required to comply with the PCI Data Security Standard. Level 4 Merchants should consult their acquirer to determine if compliance validation is also required.

⁵ 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.

MasterCard Service Provider Level Definitions



Category	Criteria	Validation Requirements
Level 1	<ul style="list-style-type: none">• All TPPs• All DSEs with greater than 300,000 annual transactions	<ul style="list-style-type: none">• Annual Onsite Assessment conducted by a QSA¹• Quarterly Network Scan conducted by an ASV²
Level 2	<ul style="list-style-type: none">• All DSEs with less than 300,000 annual transactions	<ul style="list-style-type: none">• Annual Self-Assessment• Quarterly Network Scan conducted by an ASV²

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

² Merchant and Service Providers must conduct quarterly network scans using a PCI SSC Approved Scanning Vendor

Main Categories of the SDP Program



SDP Program – For Acquiring Banks

Acquirer Responsibilities

- Submit a completed SDP Acquirer Submission and Compliance Status Form to sdp@mastercard.com **quarterly**, reporting merchants' PCI compliance progress for L1, L2 and L3 merchants (L4 is optional)
- Acquirers must register merchants in the MasterCard Registration Program (MRP) once they have validated PCI compliance. MRP SDP merchant registration signifies overall compliance with the SDP Program mandate.



SDP Program – For Acquiring Banks/Reporting

To ensure compliance with the MasterCard SDP Program the Acquirer :

- For each Merchant under L1-L3 must complete and submit quarterly “Status Report” via an e-mail message to sdp@mastercard.com using the form (SDP Acquirer Submission and Compliance Status Form) provided on the SDP Program Web site,
- Communicate the SDP Program requirements to each L1-L3 Merchants, and validate the Merchant’s compliance with the *PCI DSS* by reviewing its SAQ and the ROC,
- Communicate the SDP Program requirements to each L1-L Service Provider, and ensure that Merchants use only compliant Service Providers,
- The Acquirer must ensure, with respect to each of its Merchants L1-L3 and all Service Providers that use any third party-provided payment applications must validate that each payment application used is listed on the PCI SSC Web site at www.pcisecuritystandards.org as compliant with the *PCI PA DSS*

Merchant Responsibilities*

- Work with Acquirer to determine merchant level based on most recent 52 week transaction volume
- Review PCI documentation and applicable compliance validation requirements
- Engage an Approved Scanning Vendor (ASV) or Qualified Security Assessor (QSA) as appropriate and follow the compliance procedures
- Report PCI DSS Compliance status to their acquirer



MasterCard SDP Program Revisions EMV-All Regions (“Exemption Program”)



Merchants (L1 & 2) that are predominantly EMV may be exempt from annual validation if all program requirements are met

- At least 75% of merchant’s annual total MasterCard and Maestro transaction count is processed through **dual interface hybrid POS terminals**
- No Storage of Sensitive Authentication Data
- No Account Data Compromise for past 12 months
- Annual testing of ADC Incident Response Plan
- Has validated PCI DSS compliance or has submitted satisfactory remediation plan to MasterCard within previous 12 months
- Annually confirms compliance to the above requirements

Service Provider (TPP & DSE) Responsibilities

- Determine Service Provider level and applicable compliance validation requirements
- Review PCI documentation and compliance validation requirements
- Engage an Approved Scanning Vendor (ASV) or Qualified Security Assessor (QSA) as appropriate and follow the compliance procedures
- Submit an Attestation of Compliance (AOC) form or a PCI action plan for review and approval



SDP Program – For Service Providers Validation Requirements



- Requires an Attestation of Compliance (AOC)
 - Send AOC to PCIReports@MasterCard.com
 - After each annual assessment (re-validation), new AOC is to be forwarded to above addresses
- MasterCard will not accept or review a ROC (Report on Compliance)
- Non compliant Service Providers will need to disclose their Compliance status via an Action Plan. The MasterCard Action Plan format is based on the Prioritized Approach workbook
- Service Providers will not be listed on MasterCard list of compliant service providers until AOC is received

MasterCard Worldwide

Home

- ▶ Merchants
- ▶ Service Providers
- ▶ Service Provider Levels Defined
- ▶ Service Provider Requirements
- ▶ Compliance Considerations
- ▶ Compliant Service Providers
- ▶ Learn More
- ▶ Vendors
- ▶ Acquirers
- ▶ PCI Merchant Education Program
- ▶ Special Offers and Promotions
- ▶ Documentation

Compliant Service Providers

Please find below the list of Service Providers that have been reported to MasterCard by Qualified Security Assessors (QSAs) as compliant with the PCI Standard as of the date indicated. To be reported by a QSA as PCI compliant, the Service Provider must have both:

- successfully completed a PCI onsite review conducted by a QSA; and
- successfully conducted network scans in compliance with the MasterCard Site Data Protection program.

A Service Provider reported to MasterCard to be compliant with the PCI Standard should have been provided a Certificate of Validation (COV) by a QSA. If you are considering using a Service Provider, MasterCard recommends that you ask to see and inspect the Certificate of Validation. Questions about compliance with the PCI Standard should be directed to the QSA.

To access a list of Qualified Security Assessors, please click on the following link:
www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

Please note that MasterCard does not endorse or make any representation of any kind as to the nature or quality of service or other performance of any QSA, or Service Provider. MasterCard disclaims any liability of any kind directly or indirectly resulting from the use of or reliance on information appearing or not appearing herein and makes no representation as to the accuracy of any such information.

▶ [Compliant Service Provider List](#)

As of January 1, 2009, MasterCard will no longer list those Service Providers who have only submitted an SAQ. The posting will contain only those entities who have successfully completed an annual onsite review.

ADC Safe Harbor = PCI Compliance + SDP Compliance



- The concept of Safe Harbor is to potentially shield the acquirer from a partial or full ADC assessment if two conditions are met:
 - If the merchant is determined to be PCI compliant **at the time** of the compromise by the forensic investigation
 - Emphasis is on *at the time of the compromise*. Compliance is a continual process and prior to consideration of Safe Harbor, it must be determined whether the merchant was still compliant when the compromise occurred.
 - If the merchant has a valid, current MRP registration at the time of the account data compromise
 - As Registered by their Acquirer

ADC Safe Harbor = PCI Compliance + SDP Compliance



PCI Compliance

- PCI Onsite Assessment
- PCI Self Assessment
- PCI Quarterly Network Scanning

The successful completion of the above applicable compliance requirements means the merchant is compliant with the PCI Data Security Standard.



SDP Compliance

- Compliance Validation with Acquirer
- Acquirer Reporting of Merchant to MasterCard

The successful completion of the above compliance requirements means the merchant is compliant with the PCI Data Security Standard AND compliant with the MasterCard SDP Program requirements AND registered through MRP Program.

PCI – Non-Compliance Assessment



Failure of the following to comply with the SDP Program mandate...

May result in an assessment of...

Classification

Violations per calendar year

Level 1 and Level 2 Merchants

Up to USD 25,000 for the first violation
Up to USD 50,000 for the second violation
Up to USD 100,000 for the third violation
Up to USD 200,000 for the fourth violation

Level 3 Merchants

Up to USD 10,000 for the first violation
Up to USD 20,000 for the second violation
Up to USD 40,000 for the third violation
Up to USD 80,000 for the fourth violation

Level 1 and Level 2 Service Providers

Up to USD 25,000 for the first violation
Up to USD 50,000 for the second violation
Up to USD 100,000 for the third violation
Up to USD 200,000 for the fourth violation

Noncompliance also may result in Merchant termination, deregistration of a TPP or DSE as a Service Provider, or termination of the Acquirer as a Customer

More Information and Additional Resources

The SDP Website - www.mastercard.com/sdp

- SDP Program information – sdp@mastercard.com with questions
- Merchant level definitions and compliance requirements

PCI 360 - www.mastercard.com/pci360

- Complimentary access to our PCI 360 webinar series

PCI Security Standards Council - www.pcisecuritystandards.org

- PCI SSC Merchant Resource Website : www.pcisecuritystandards.org/merchants

- PCI SSC Small Merchant Site: www.pcisecuritystandards.org/smb

For additional Fraud Prevention Tools and Resources

- www.mastercardsecurity.com
- http://www.mastercard.com/us/company/en/whatwedo/security/fraud_management.html



Last But Not Least..

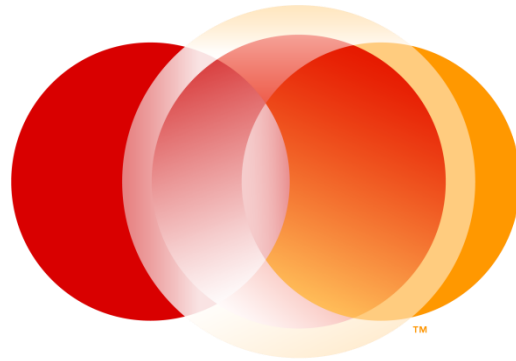
- Breaches will continue to occur
- EMV is not the total answer. It is probable a fraud shift will occur and present itself in card-not-present environments (e-commerce)
- Compliance is not synonymous with security
- PCI DSS is a set of minimal security controls that should be implemented
- PCI DSS is a security in depth framework
- Tokenization & P2PE are supplements to PCI DSS – they are not required. They offer an opportunity for scope reduction if implemented per validated and approved requirements
- PCI DSS should be a business as usual practice to remain compliant and reduce the risk of breach or compromise.





MasterCard
Worldwide





MasterCard

Worldwide

The Heart of Commerce™
