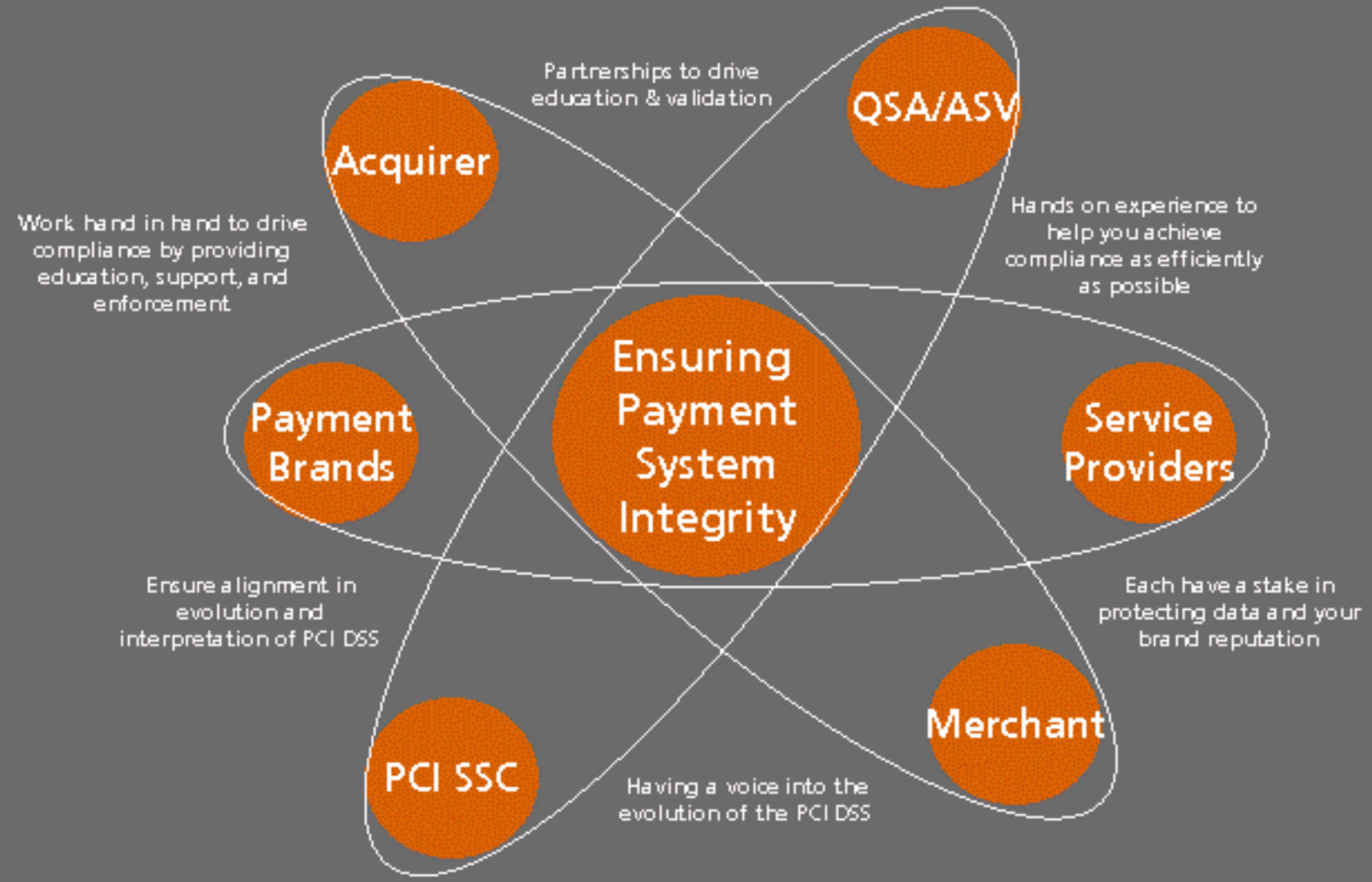
Sally Ramadan
Payment System Integrity

MasterCard Worldwide

Compliance Validation and Beyond

We are all stakeholders in data protection

MasterCard Worldwide



PCI and SDP Compliance

MasterCard Worldwide

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 Registration of Merchant with 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.

PCI Compliance + SDP Compliance = **Safe Harbor**

MasterCard SDP Compliance Levels

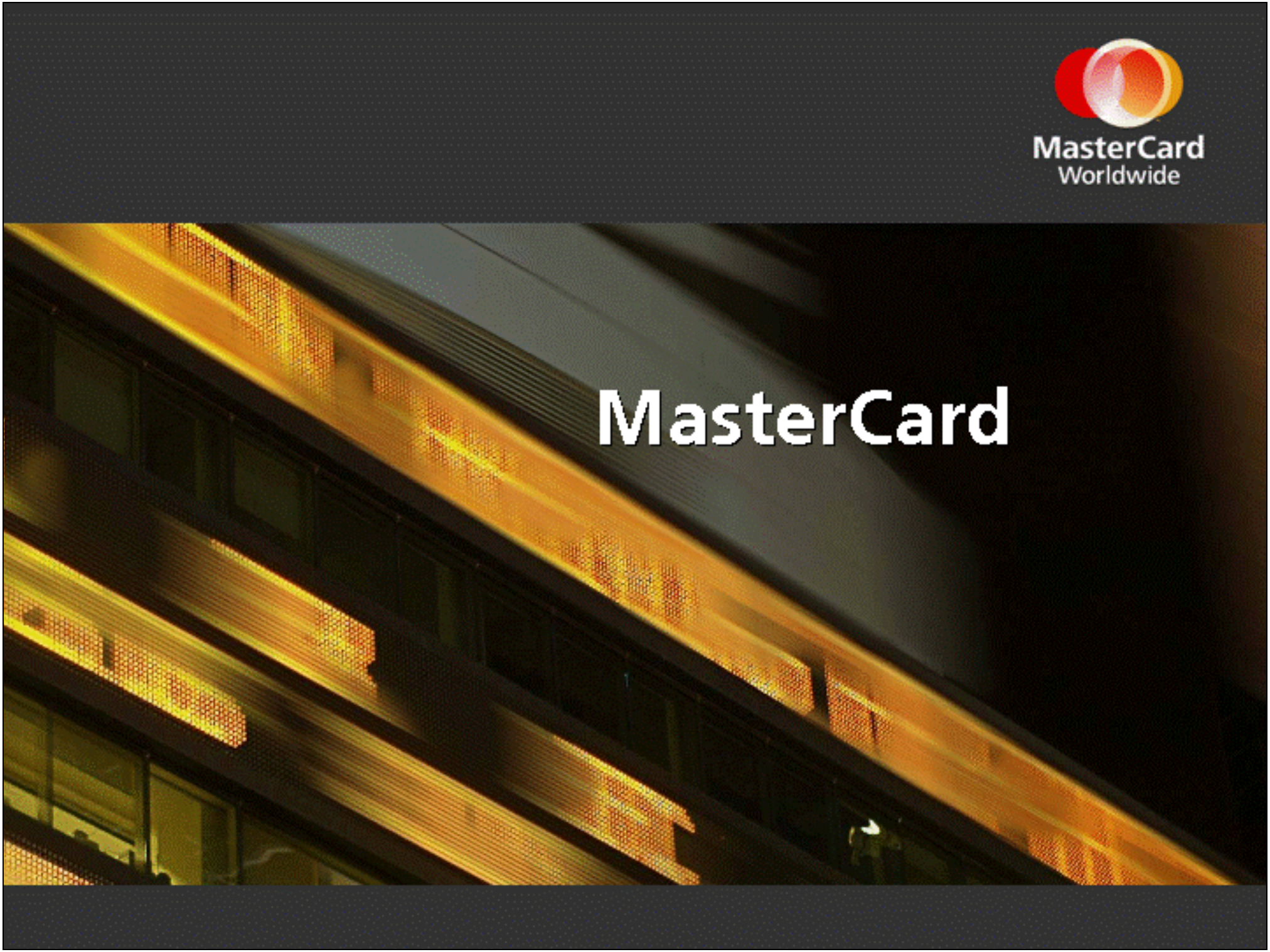
MasterCard Worldwide

Category	Criteria	Requirements
Level 1	• Merchants > 6 MM annual total transactions (all channels – POS, MOTO, eComm) • All compromised entities	• Annual onsite audit* • Quarterly network scan
Level 2	• Merchants > 1 and < 6 MM annual total transactions (all channels – POS, MOTO, eComm) • All merchants meeting Level 2 criteria of a competing brand	• Quarterly network scan • Annual self assessment
Level 3	• Merchants > 20,000 annual e-commerce transactions but less than 1 MM total transactions • All merchants meeting Level 3 criteria of a competing brand	• Quarterly network scan • Annual self assessment
Level 4	• All other merchants	• Quarterly network scan • Annual self assessment

Merchant Identification

MasterCard Worldwide

- The PCI DSS applies to any entity that stores, transmits, or processes cardholder data – thus uniformly to merchants of all levels (1,2,3, and 4)
- The SDP Program mandate applies only to Level 1, 2, and 3 merchants
- Your Acquirer may require a formal attestation, if you do not store, transmit, or process cardholder data


MasterCard
Worldwide
MasterCard

Communications

MasterCard Worldwide

Case Studies

Site Data Reflection Security Articles

Webinars

Promotions & Offers

Public Relations

Website

Trade Ads

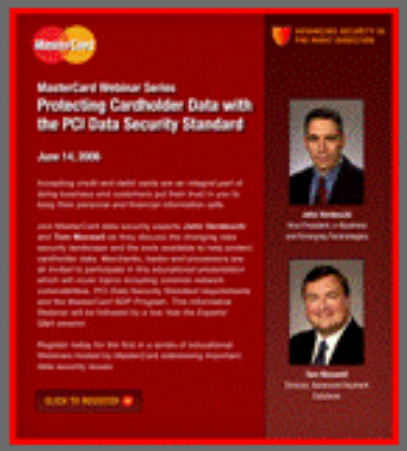
Conferences

Site Data Reflections

- Publication focused on account data security issues
- Shares MasterCard experiences in data security
  - SDP Program
  - Forensics investigation findings
- Relevant educational material targeting acquirers, merchants, and third parties storing data
- Acquirers, merchants, and third parties may submit topics

Merchant Education Outreach

- 2007 Merchant Education Webinar Series
- PCI related Webinars
  - Introduction to the PCI Data Security Standard
  - Preparing for a PCI Audit
  - Data Security Requirements for Acquirers and Processors
- Online and print campaign
  - Print ads in trade related magazines
  - Banner Ads
  - MasterCard website promotions
- Live sessions with Acquirers



Free Scan Promotions

MasterCard Worldwide

- Partnership with PCI Vendors
  - ATW
  - Comply-Guard Networks
  - Cybertrust / Verizon Business
  - One-Sec
  - Qualys
  - SRC

MasterCard
Worldwide

The Acquirer as your Advocate

MasterCard Worldwide

- Your voice to the payment industry through membership in the PCI Security Standards Council

- Partnership with the vendor community to secure favorable rates for compliance services and education

Sample Acquirer Activities

MasterCard Worldwide

- Communication and education on the standard and validation requirements through
  - Webinars
  - Newsletters
  - Face to Face Training
  - Vendor alliances

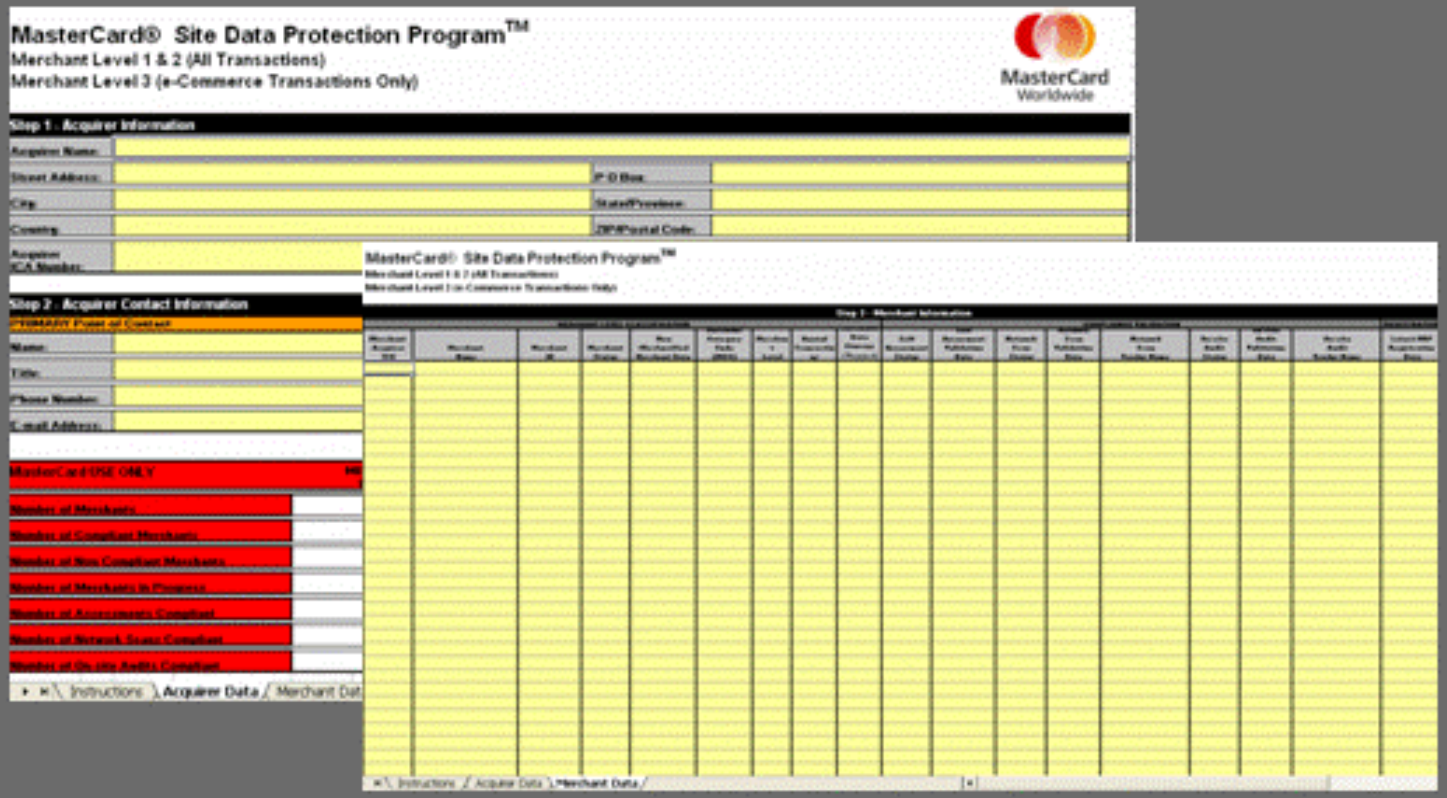
Compliance Validation Requirements

MasterCard Worldwide

- Merchants are required to achieve compliance with the PCI DSS and complete the following
  - On-site Assessment
  - Self Assessment Questionnaire (SAQ)
  - Network Scan
- Submitting evidence of compliance is the act of validating compliance with your Acquirer

Compliance Status Reporting

Your Acquirer is responsible for reporting compliance status and milestones



Level 4 Merchants

MasterCard Worldwide

- Compliance with the PCI Data Security Standard is required for all Level 4 merchants
- The only optional aspects of compliance for Level 4 merchants are:
  - Active compliance validation with your acquirer
  - Card Brand specific steps (e.g., registration)
- To be compliant with the PCI DSS, Level 4 merchants must successfully complete the following:
  - An annual self assessment
  - Quarterly network scans

Registration with MasterCard

- Once an Acquirer has successfully validated a merchant's compliance, it must register the merchant on the MasterCard Registration Program
- Your Acquirer is required to renew a merchant's registration annually if the merchant is still in compliance

Making the case for compliance

MasterCard Worldwide

- Securing payment card data makes good business sense.
- Companies that suffer account data compromises experience
  - Damage to reputation
  - Loss of consumer confidence
  - Cost of re-issuance and monitoring of cards
- Participation in the payment card system requires adherence to payment brand rules and safeguarding cardholder data

Remain Diligent

MasterCard Worldwide

- Institutionalize data security at your organization.
- While validation requirements are quarterly for scans and annual for assessments, compliance is an ongoing activity
- If your compliance lapses, communication with your Acquirer is key to get back on track

Who to contact

- How the PCI DSS applies to your organization

  Contact your Acquirer

- PCI Data Security Standards documents:

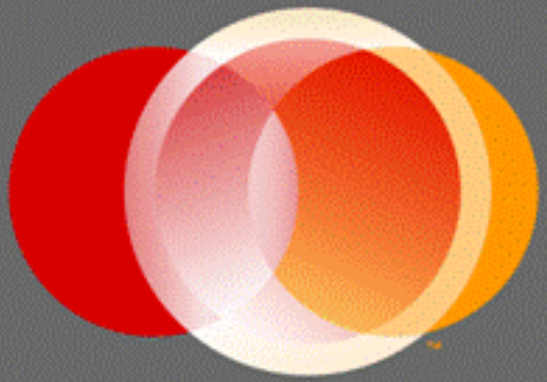
  www.pcisecuritystandards.org

- General Site Data Protection information:

  www.mastercard.com/sdp

- Other MasterCard security initiatives:

  www.mastercardsecurity.com



MasterCard
Worldwide

The Heart of Commerce™