Jennifer Mack, Vice President
Fraud Management Solutions

MasterCard Worldwide

A look into the new Self Assessment Questionnaire

SAQ A through D

Topics

- History
- Industry Feedback
- New Targeted SAQ
- Instructions and Guidelines
  1. PCI DSS – How it All Fits Together
  2. Why is PCI Compliance Important
  3. Tips and Strategies
  4. Selecting the Right SAQ for Your Company
     - Validation Type
     - SAQ Version A
     - SAQ Version B
     - SAQ Version C
     - SAQ Version D
- MasterCard PCI Compliance Levels & Key FAQ's
- How to Find More Information

History

- Self Assessment Questionnaire (SAQ)
  - Validation tool primarily used by merchants and service providers not required to undergo an onsite assessment in self evaluating their compliance with the PCI DSS
- Current SAQ based on the 2005 version of the PCI DSS Audit Procedures v1.1
- February 2008 New SAQ becomes available

Industry Feedback

Participating Organization Feedback

- PCI SSC solicited feedback from over 250 participating organizations
- Feedback received focused on 3 areas:
  - Complexity of issues experienced by small/medium merchants
  - Security concerns for small/medium merchants
  - Understanding available supporting documentation
- Results: SAQ restructured to form 4 new versions of SAQ

New Targeted SAQ

Self Assessment Questionnaire

Available February 2008

SAQ A - Merchants
No Storage, Processing, or Transmission of Cardholder Data

SAQ B - Merchants
Imprint Machines, or Stand-alone Dial-out Terminals Only, no Cardholder Storage

SAQ C - Merchants
Payment Application Connected to Internet, No Cardholder Data Storage

SAQ D – Merchants and Service Providers
All other Merchants and all SAQ-Eligible Service Providers

Guidelines & Instructions

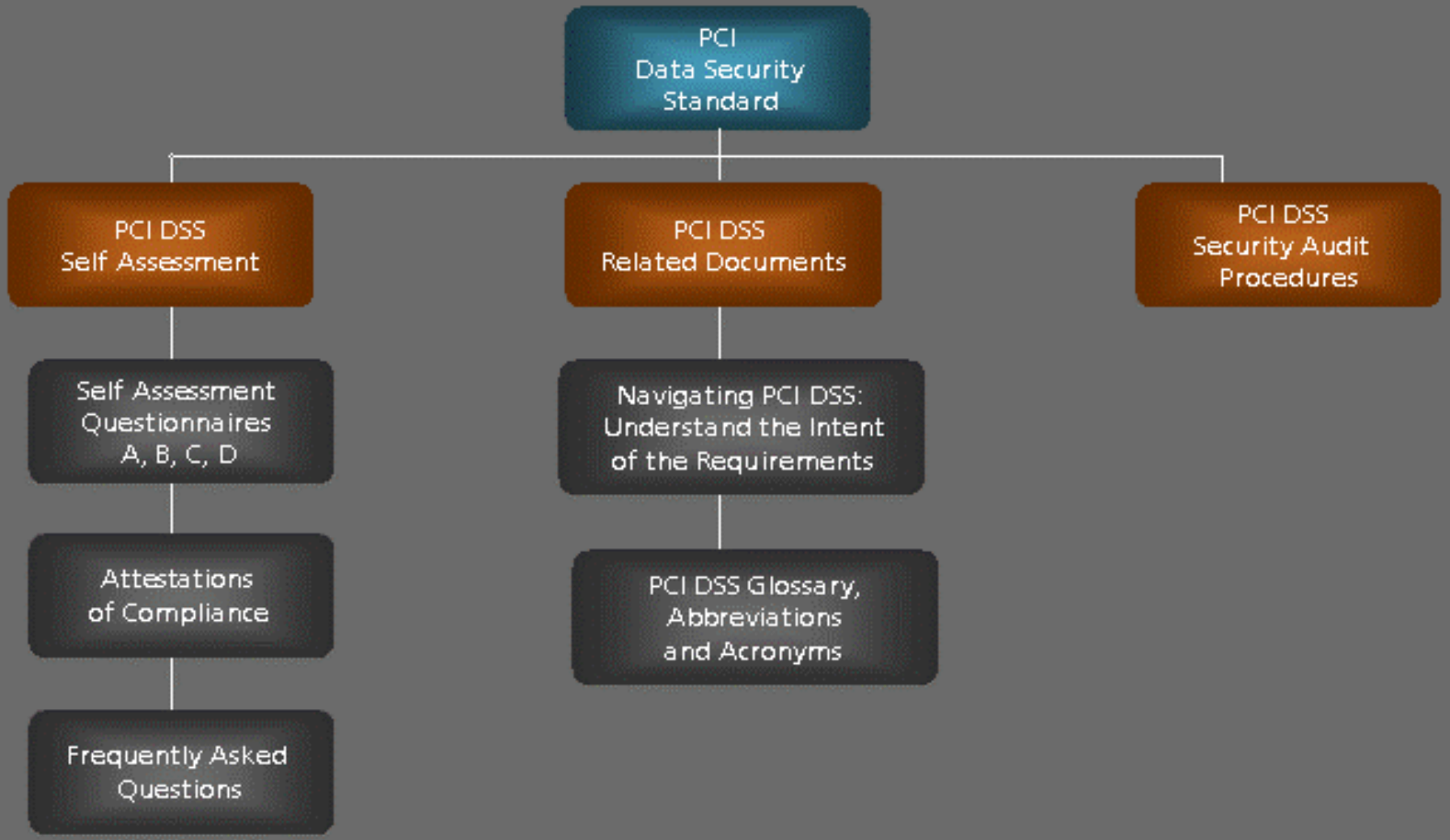
1. **The PCI DSS Self Assessment**
   How it all fits together

2. **Why is PCI Compliance Important?**
   Decrease risk of Account Data Compromise

3. **Tips and Strategies to Prepare for Compliance Validation**
   Strategies for beginning PCI DSS compliance validation efforts

4. **Selecting the SAQ and Attestation**
   How to determine which SAQ and Attestation is best suited to your organization

1. The PCI DSS Self Assessment



2. Why is PCI Compliance Important?

MasterCard Worldwide

Compliance Advantages	Non Compliance Consequences
– Improved organizational Security	– Regulatory notification requirements
– Hackers Deterred	– Loss of reputation
– Confident & Repeat Customers	– Loss of customers
– Brand Reputation	– Potential financial liability
– Validate to Business Partners	– Litigation
– Industry Level Compliance	– Non-compliance fines

Reduce Risk of Account Data Compromise

3. Tips and Strategies to Prepare for Compliance Validation

MasterCard Worldwide

- Sensitive Authentication Data
- POS System Security
- Cardholder Data Storage
- Need for Cardholder Data
- Compensating Controls
- Professional Assistance

4. Selecting the Right SAQ and Attestation

MasterCard Worldwide

SAQ Validation Type	Description	SAQ
1	Card-Not-Present (e-commerce or MO/TO) merchants, all cardholder data functions outsourced. This would never apply to face to face merchants	A
2	Imprint-only merchants with no cardholder data storage	B
3	Stand alone dial-up terminal merchants, no cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A, B or C above) and **all** service providers defined by a payment brand as eligible to complete an SAQ	D

4. Selecting the Right SAQ and Attestation

Validation Type

Validation Type

- Validation Type or Attestation you select corresponds to the Self Assessment Questionnaire best suited for your organization

Self Assessment Questionnaire

TYPE 1

No Storage, Processing or Transmission of Cardholder Data

- Company handles only card-not-present transactions (ecomm/MO/TO)
- Does not store, process or transmit cardholder data on premises, services provided entirely on 3rd party service provider
- Has confirmed 3rd party Service Provider is PCI DSS Compliant (www.mastercard.com/sdp)
- Retains only paper receipts and reports with cardholder data, not received electronically
- Does not store cardholder data electronically

Self Assessment Questionnaire

TYPE 2

B

Imprint Machines Only, No Cardholder Data Storage

- Company uses only an imprint machine to take customer payment information
- Does not transmit cardholder data either over the phone or the internet
- Retains only paper receipts and reports with cardholder data
- Company does not store cardholder data in electronic format

Self Assessment Questionnaire

TYPE 3

B

Stand-alone Dial-out Terminals Only, no Cardholder Data Storage

- Includes card present and card-not-present transactions
- Stand-alone, dial-out terminals are not connected to any other systems within your environment
- Stand-alone, dial-out terminals are not connected to the Internet
- Retains only paper receipts and reports with cardholder data
- Company does not store cardholder data in electronic format

Self Assessment Questionnaire

TYPE 4

C

Payment Application Connected to Internet, No Cardholder Data Storage

- The payment application system is on a personal computer that is connected to the Internet
- The payment application system is connected to the internet to transmit cardholder data

Self Assessment Questionnaire

TYPE 5

D

All Other Merchants and All Service Providers Defined by a Payment Brand as Eligible to Complete and SAQ

- Questions specific to wireless only need to be answered If wireless is present anywhere on network
- Questions specific to custom applications and code only need to be answered if company writes its own custom web applications
- Questions specific to data centers only need to be answered if company has a dedicated data center or server room

MasterCard PCI Compliance Levels

MasterCard Worldwide

Category	Criteria	Requirements	Compliance Date
Level 1	▪ Merchants >6 MM annual transactions (all channels) ▪ All TPPs ▪ All DSEs storing data for Level 1, 2, 3 ▪ All compromised merchants, TPPs and DSEs	▪ Annual Onsite Audit [1] ▪ Quarterly Network Scan	30 June '05 [2]
Level 2	▪ All merchants > 1 million total MasterCard transactions < 6 million total MasterCard transactions annually ▪ All merchants meeting the Level 2 criteria of a competing payment brand	▪ Annual Self-Assessment ▪ Quarterly Network Scan	31 December 2008
Level 3	▪ All merchants with annual MasterCard e-commerce transactions > 20,000 but less than one million total transactions ▪ All merchants meeting the Level 3 criteria of a competing payment brand	▪ Annual Self-Assessment ▪ Quarterly Network Scan	30 June '05
Level 4	All other merchants	▪ Annual Self-Assessment ▪ Quarterly Network Scan	Consult Acquirer

1 TPPs and DSEs must use a certified third party to perform the onsite audit
2 TPPs and DSEs were previously required to completed quarterly scans and self-assessments by 30 June 2004

Key FAQ's

- *When does the PCI Data Security Standard Self-Assessment Questionnaire (SAQ) Questionnaire version 1.1 become effective?*
  - The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) Questionnaire version 1.1 was released by the Council February 2008 and became effective immediately.

- *What is the sunset date for the Self-Assessment Questionnaire version 1.0?*
  - The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) Questionnaire version 1.1 was released by the Council in February 2008. Any SAQ submissions after April 30, 2008, must be completed using SAQ version 1.1.
    - Please note an entity must be compliant with the PCI Data Security Standard in its entirety. The questions in the SAQ version 1.0 do not cover all of the PCI DSS requirements. As such, an organization that is only compliant with the questions in SAQ version 1.0 in not considered to be compliant with PCI DSS based on the SAQ alone. The organization must verify that it adheres to all of the requirements stipulated in the PCI DSS.

Need More Information?

MasterCard Worldwide

- Go to: www.pcisecuritystandards.org and find information on:
  - SAQ A,B,C,D
  - Frequently Asked Questions
  - PCI Documentation
  - Contact Information

- PCI Webinar Series
  - www.webcasts/mastercardpci.com

Thank you.

MasterCard
Worldwide

The Heart of Commerce™