



Security
Standards Council

The PCI Security Standards Council

11/12/2008

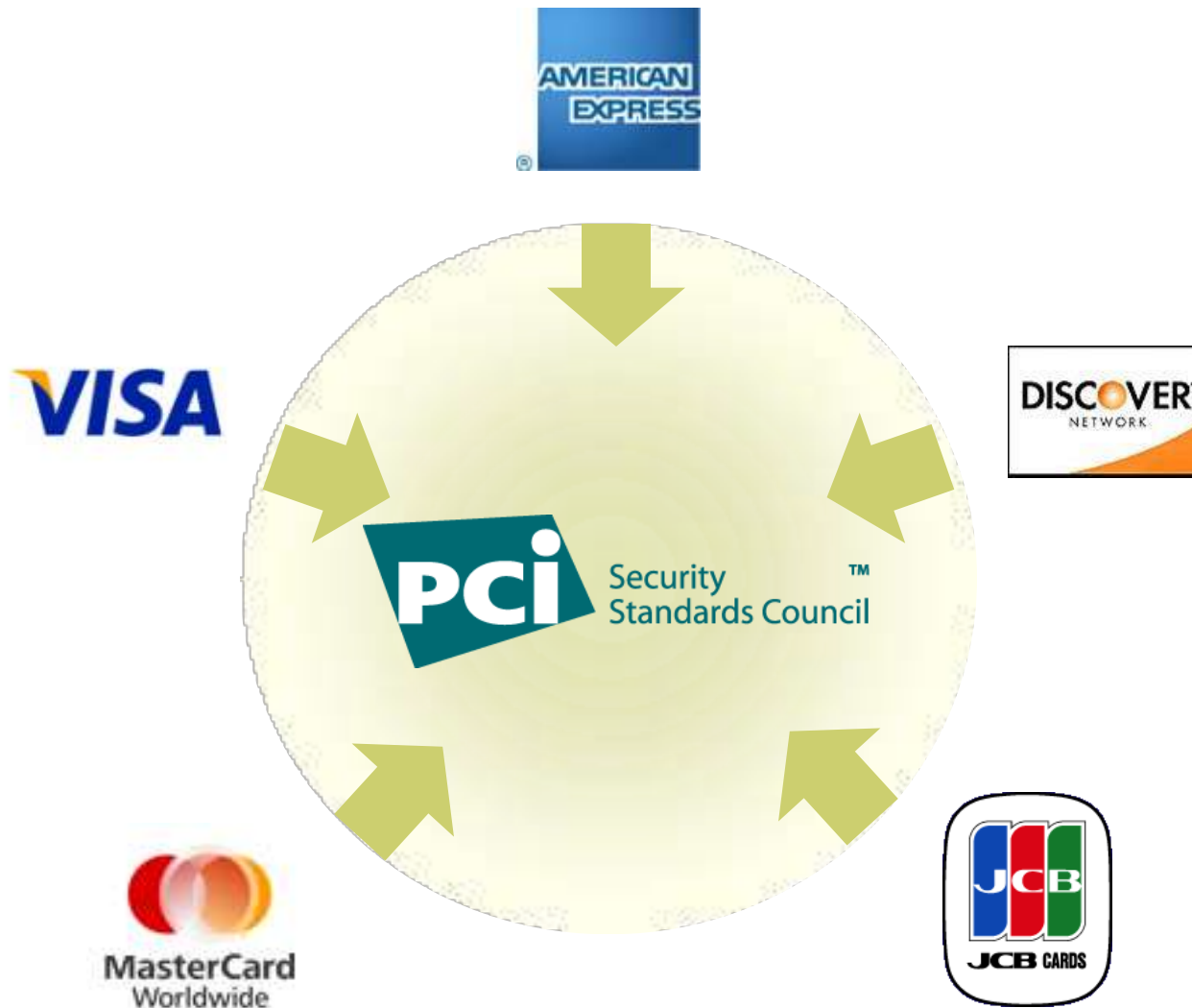
- An open global forum, launched in 2006, responsible for the development, management, education, and awareness of the PCI Security Standards, including:
 - Data Security Standard (DSS)
 - Payment Application Data Security Standard (PA-DSS)
 - Pin-Entry Device (PED)



PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data





Assessor Servicing Markets per Region

Asia Pacific: 29

Canada: 16

CEMEA: 28

Latin America & Caribbean: 27

United States: 87

Europe: 57

- Over 500 Participating Organizations around the world
- Successful Community Meetings with over 700 attendees from around the world
- Board of Advisors driving special interest groups
 - Wireless
 - Pre-authorization
- 164 current QSA Companies, of these 74 are also ASV Companies
- Total QSAs (individuals) trained to date is 1,063
- Additional devices added to PED Standard
- Implemented two-year lifecycle process for DSS & SAQ
- PCI SSC participated in 33 events worldwide

PCI SSC....

- Is an Independent Industry Standard
- Manages the technical and business requirements for how payment data should be stored and protected
- Maintains List of Qualified PCI Assessor Community
 - QSAs, ASVs, PA-QSA and PED Labs

PCI SSC Does Not...

- Manage or Drive Compliance
 - Each brand continues to maintain its own compliance programs
 - Identifies stakeholders that need to validate compliance
 - Definitions of Validation Levels
 - Fines and Fees



- Security standards and supporting documents
- Frequently asked questions
- List of approved QSAs, ASVs, PA-QSAs, PED Labs
- Education and outreach programs
 - Webinars
 - Newsletters/bulletins
Council appeared in almost 300 pieces of coverage globally since January
- Searchable FAQ tool for all standards-related questions
- Participating organization membership, community meetings, qualifications standards feedback
- One global voice for the industry

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name ^[1]	Yes	Yes ¹	No
	Service Code ¹	Yes	Yes ¹	No
	Expiration Date ¹	Yes	Yes ¹	No
Sensitive Authentication Data ^[2]	Full Magnetic Stripe Data ^[3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

^[1] These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

^[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

^[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

- Go to: www.pcisecuritystandards.org and find information on:
 - Frequently Asked Questions
 - PCI Documentation
 - Contact Information
- Participating Organization Information



The screenshot shows the PCI Security Standards Council website. The header includes the PCI Security Standards Council logo, a search bar, and navigation links for Site Map, Contact Us, Privacy Policy, and Terms & Conditions. The main navigation menu includes Security Standards, QSA/ASV, Participation, Education, News & Events, and About Us. The left sidebar contains buttons for Join Now, FAQ, Resources for Merchants & Service Providers, and Career Opportunities. Below these are quick links for getting the PCI DSS, DSS Self-Assessment Questionnaire (SAQ), PIN Entry Devices (PED), Payment Application DSS (PA-DSS), finding a QSA or ASV, and becoming a QSA. The main content area features a welcome message, a description of the council's mission, and a news item about the release of PCI Data Security Standard 1.2 on October 1, 2008. There are also sections for the PCI Data Security Standard and the PIN Entry Device (PED) Standard.



Security
Standards Council

Thank You!

11/12/2008

Data Security Operating Policy

American Express International Inc.

Dr. Kathrin Schier

7th November 2008

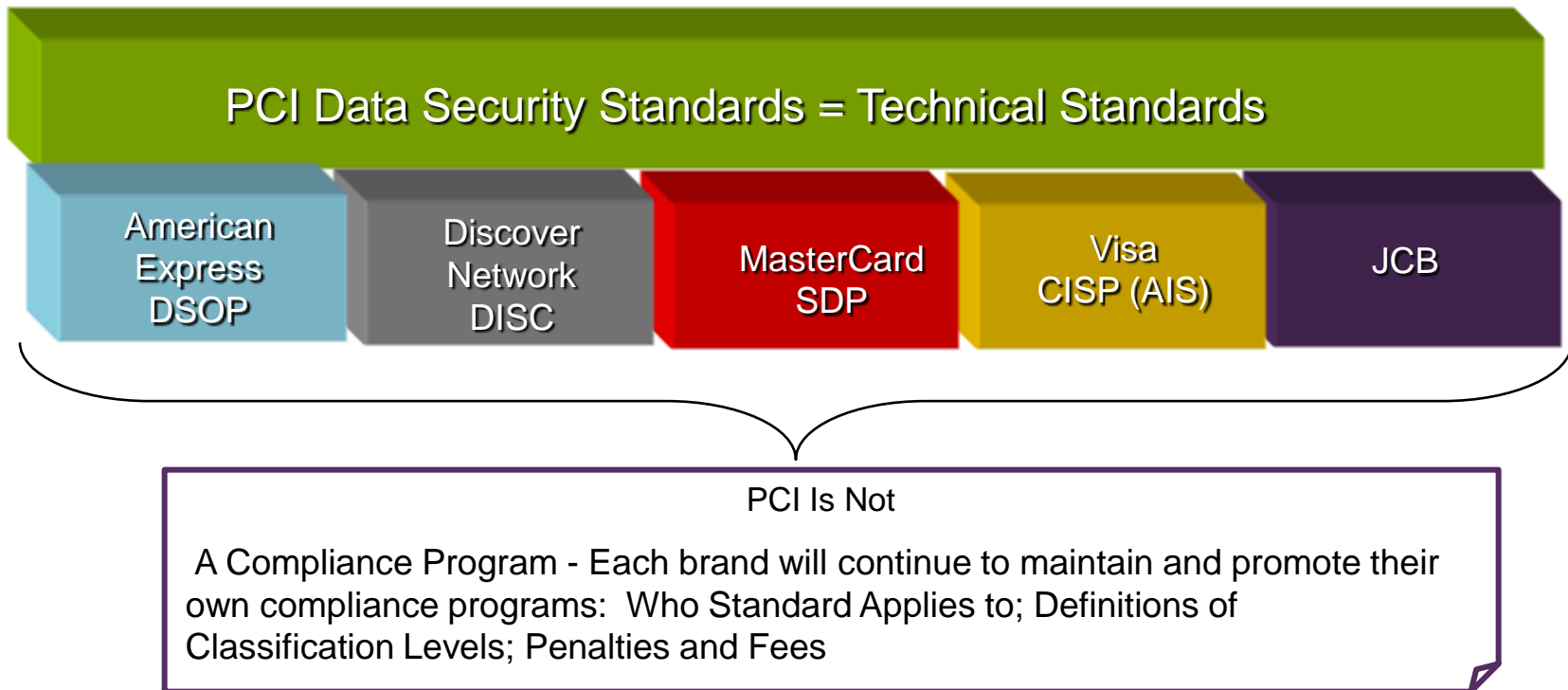
Agenda

- Payment Card Industry Data Security Standard
- American Express Data Security Operating Policy (DSOP)
- How to comply
- In case you have a breach

Payment Card Industry (PCI) Data Security Standards

Previously, Visa, MasterCard, American Express, JCB and Discover had their own variation of a data security standards and policies with different compliance regulations, which caused confusion among merchants.

In order to alleviate the confusion, **they joined together and formed a single approach to establishing standards that safeguards customer information while maintaining their own policy and compliance regulations.** This is known as the **Payment Card Industry (PCI) Data Security Standards.**



American Express Data Security Operating Policy

Level	Definition	Validation	Requirements	Deadline
LEVEL 1	<ul style="list-style-type: none"> •2.5 M or more American Express txns p/yr •Any merchant that has had a data compromise •Any merchant that American Express deems a Level 1 as well as ALL Service Providers 	Annual Onsite Security Audit AND Quarterly Network Scan	1. Executive Summary Report from Audit AND Scan as Proof of Compliance OR 2. Project Plan for Compliance (includes Audit and Scan)	31 March 2008
LEVEL 2	<ul style="list-style-type: none"> •50,000 to 2.5 M American Express txns p/yr 	Quarterly Network Scan AND Self Assessment Questionnaire	1. Executive Summary Report from Scan and Self Assessment Questionnaire OR 2. Project Plan for Compliance	
LEVEL 3	<ul style="list-style-type: none"> •Less than 50,000 American Express txns p/yr 	Quarterly Network Scan	(recommended)	

American Express Data Security Operating Policy

Validation Process

- Annual Onsite Audit
 - Also known as a Report On Compliance (ROC), an onsite audit demonstrates whether or not you are in compliance for all requirements.
- Quarterly Network Scan
 - Process that remotely audits your internet-connected computer networks and their web servers to ensure they are continually kept in a secure state. Scanning tests for potential weaknesses and vulnerabilities
- Self Assessment questionnaire
- Project Plan
 - If the merchant is in the process of becoming compliant, we will accept a project plan that includes remediation efforts and expected date of completion.
- Exception form
 - Some merchants who meet strict requirements may be eligible for an exception to the network scan requirement – please contact our Security Partner – Trustwave if you think you may qualify..

How To Comply

Here are a few easy steps to help you complying with the American Express Data Security operating Policy

1) To find an assessor here is the link:

QSA: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

ASV: https://www.pcisecuritystandards.org/pdfs/asv_report.html

2) To submit the validation documentation here is a contact to obtain secure portal information:

americanexpresscompliance@trustwave.com

3) If you have any questions, please feel free to contact either

americanexpresscompliance@trustwave.com

OR

americanexpressdatasecurityEMEA@aexp.com

In case you have a breach

Merchants and their vendors that store American Express Cardmember information* are obligated to notify American Express immediately if the data is (or may be) accessed or used without authorization or used in any way that is not in accordance with the Card Acceptance Agreement.

If you believe that Cardmember information has been compromised, contact your Client Manager or call the American Express Enterprise Incident Response Program (EIRP) at + 1 (602)537-3021. You may also notify American Express EIRP sending an email to EIRP@aexp.com or fax to (602) 537-7998.

Thank you very much for your attention!

* stored only as permitted in our Card Acceptance Agreement