Deloitte.

PCI compliance – the “what” and the “why”

Executing through excellence

Tejinder Basi, Partner
Tarlok Birdi, Senior Manager

May 27, 2009

Agenda

1. Introduction
2. Background
3. What problem are we trying to solve?
4. What are the consequences of non-compliance?
5. Questions

Speaker bio

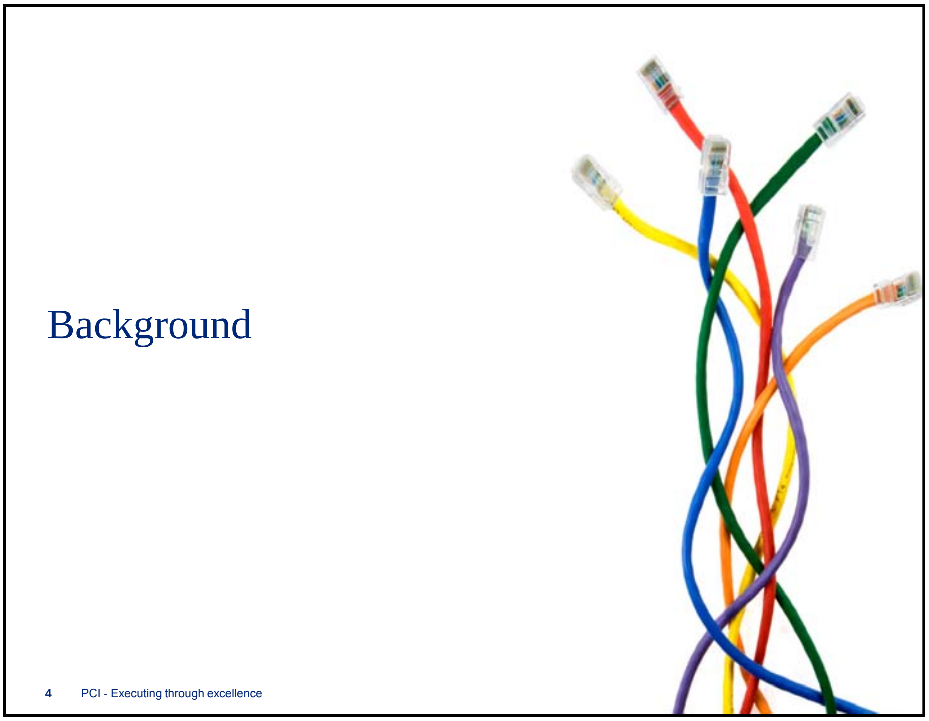
Tejinder Basi, Partner, Deloitte

- Tejinder Basi is a partner with Deloitte & Touche. He is part of Deloitte’s National and BC Public Sector Industry Practice leadership group.
- Tejinder and his team have proudly supported the public sector within BC with a wide variety of strategic advisory and implementation services over the last 10+ years.
- His specific area of focus is Security and Privacy. He leads Deloitte’s Security and Privacy practice for Western Canada, within the Enterprise Risk Services group. He has over 15 years of experience as a Security, Audit and Control professional spanning Europe and North America.
- His team’s motto is “helping clients manage risk from the boardroom to the network”.
- Deloitte is proud to be the Official Supplier of Professional Services to the Vancouver 2010 Olympic and Paralympic Winter Games.

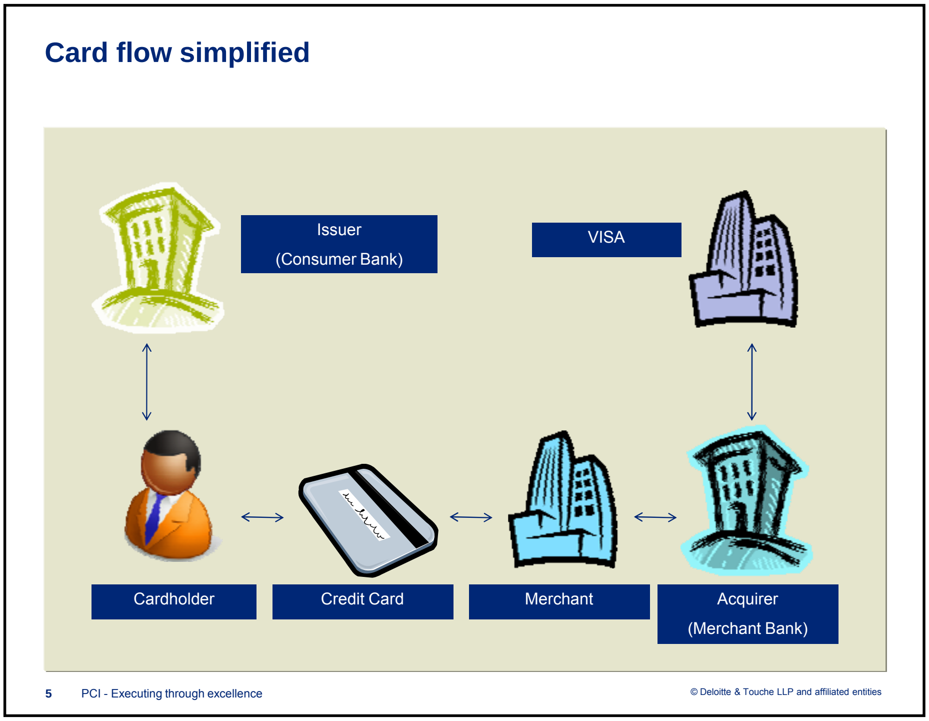
Speaker bio

Tarlok Birdi, Senior Manager, Deloitte Vancouver

- Tarlok has over 14 years of experience in the IT field. He has worked in several industry sectors including healthcare, government, telecommunications, financial and retail. He specializes in secure infrastructure design, including multi-vendor network and server systems design for clustered and distributed applications, as well as developing process and controls for enterprise security. Tarlok has lead several network server systems vulnerability assessment and vulnerability exploitation projects. Tarlok has worked with local merchants and service providers in the government, food/beverage, hospitality, retail and telecommunications industries, performing PCI gap analysis and remediation planning, developing PCI compliance readiness strategies and performing PCI compliance audits.
- Tarlok holds a Master of Computer Science degree, the CISSP and CISM designations. Additional certifications include QualysGuard Certified Specialist, and PCI Qualified Security Assessor (QSA).



Background



Card flow simplified

Issuer
(Consumer Bank)

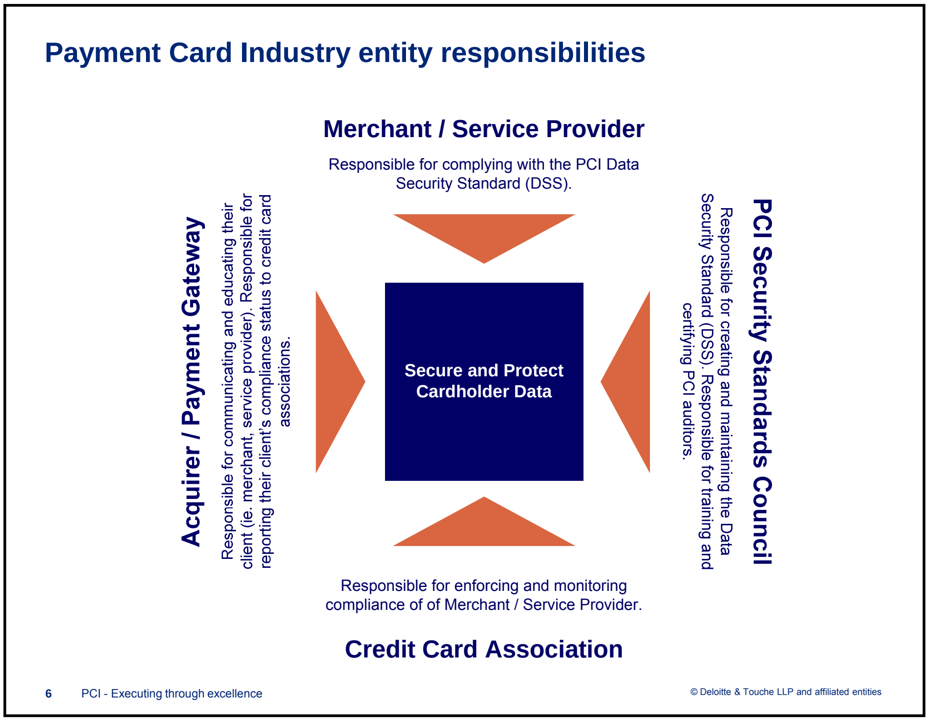
VISA

Cardholder

Credit Card

Merchant

Acquirer
(Merchant Bank)



Payment Card Industry entity responsibilities

Merchant / Service Provider

Responsible for complying with the PCI Data Security Standard (DSS).

Acquirer / Payment Gateway

Responsible for communicating and educating their client (ie. merchant, service provider). Responsible for reporting their client's compliance status to credit card associations.

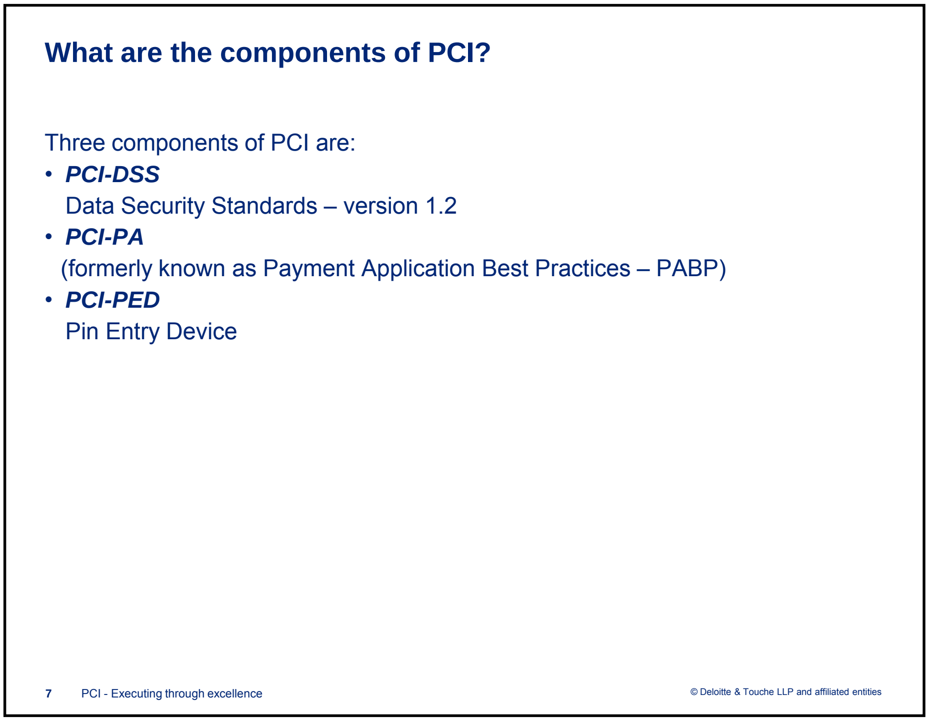
Secure and Protect Cardholder Data

PCI Security Standards Council

Responsible for creating and maintaining the Data Security Standard (DSS). Responsible for training and certifying PCI auditors.

Responsible for enforcing and monitoring compliance of of Merchant / Service Provider.

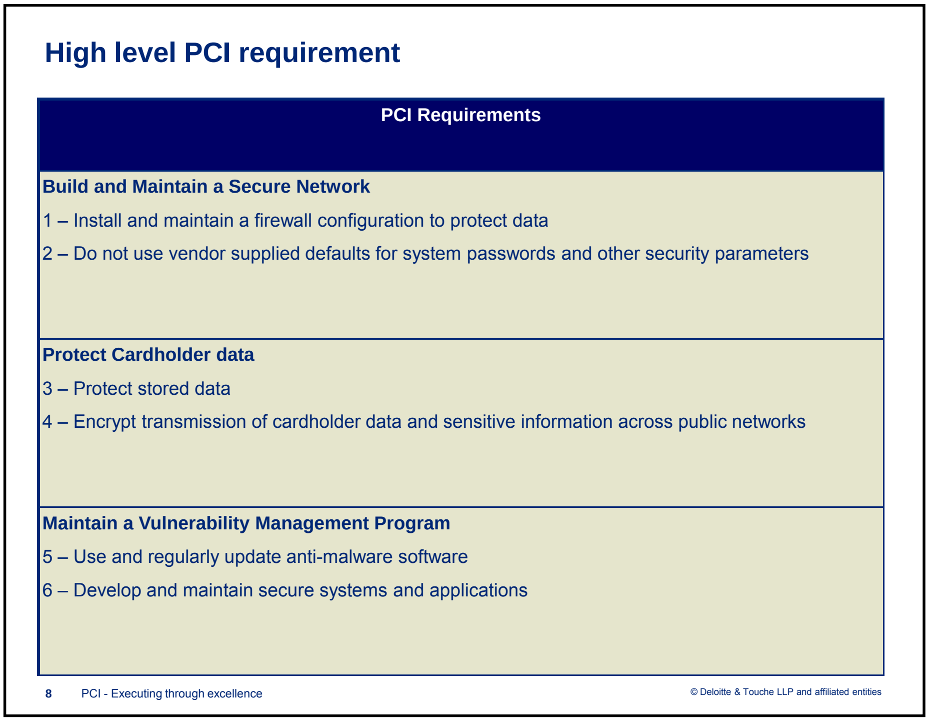
Credit Card Association



What are the components of PCI?

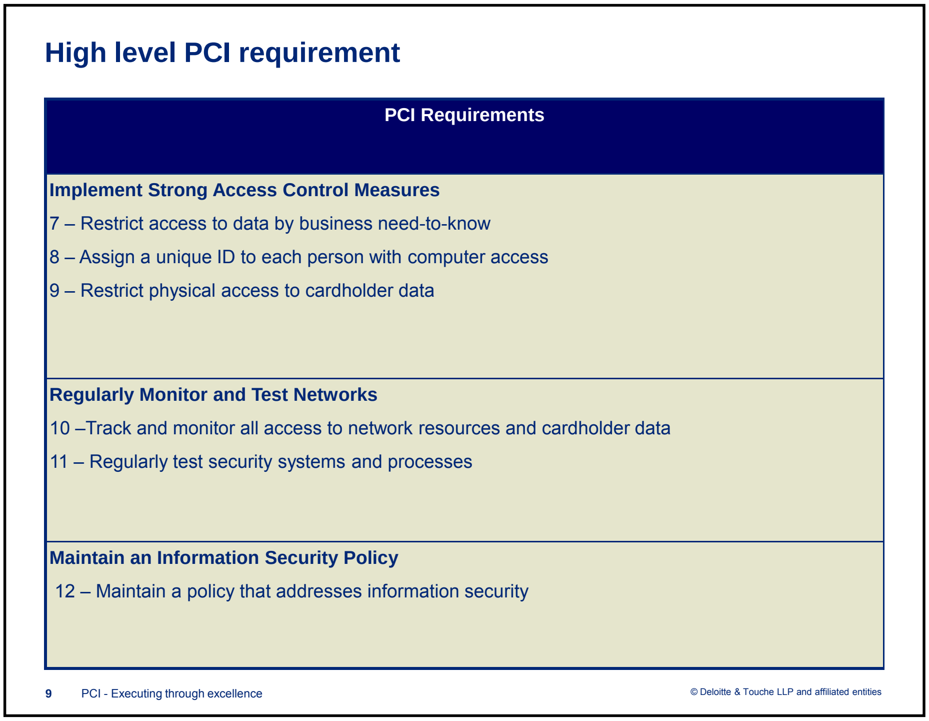
Three components of PCI are:

- ***PCI-DSS***
  Data Security Standards – version 1.2
- ***PCI-PA***
  (formerly known as Payment Application Best Practices – PABP)
- ***PCI-PED***
  Pin Entry Device



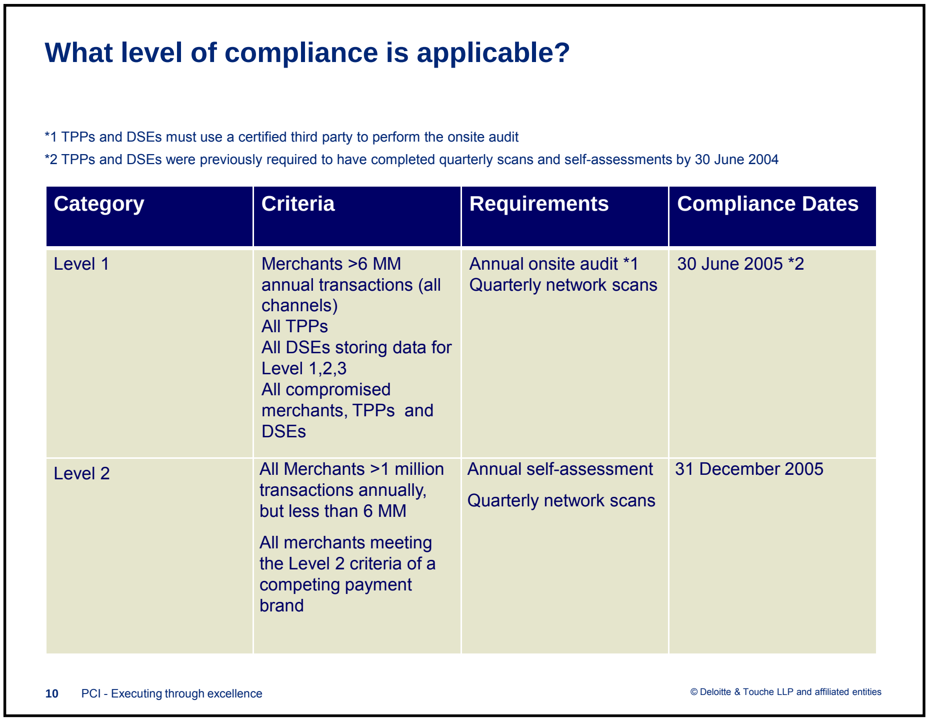
High level PCI requirement

PCI Requirements
Build and Maintain a Secure Network 1 – Install and maintain a firewall configuration to protect data 2 – Do not use vendor supplied defaults for system passwords and other security parameters
Protect Cardholder data 3 – Protect stored data 4 – Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program 5 – Use and regularly update anti-malware software 6 – Develop and maintain secure systems and applications



High level PCI requirement

PCI Requirements
Implement Strong Access Control Measures 7 – Restrict access to 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

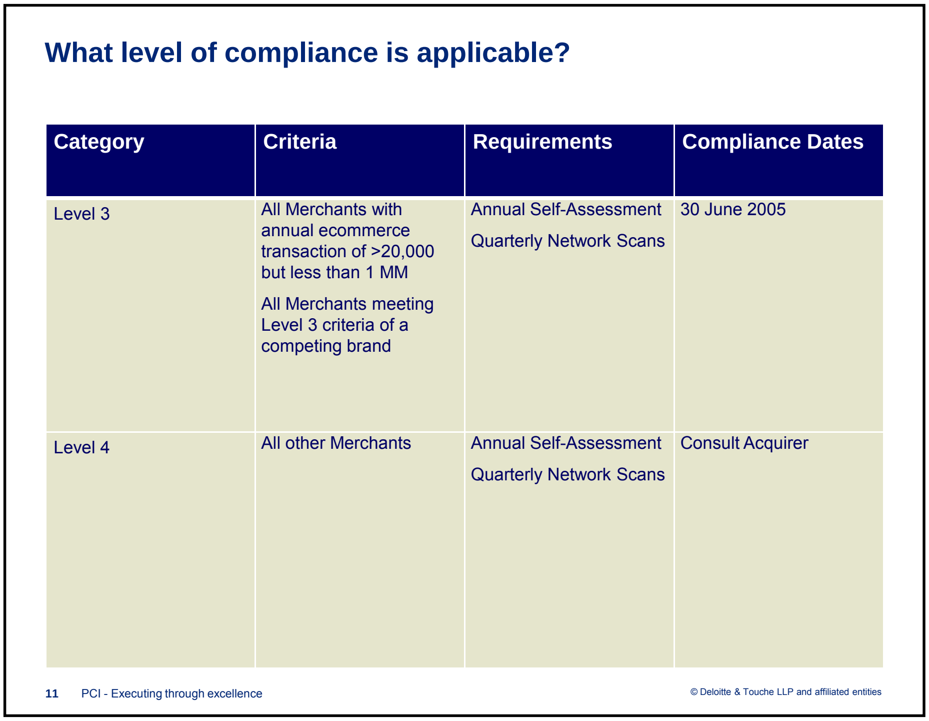


What level of compliance is applicable?

*1 TPPs and DSEs must use a certified third party to perform the onsite audit

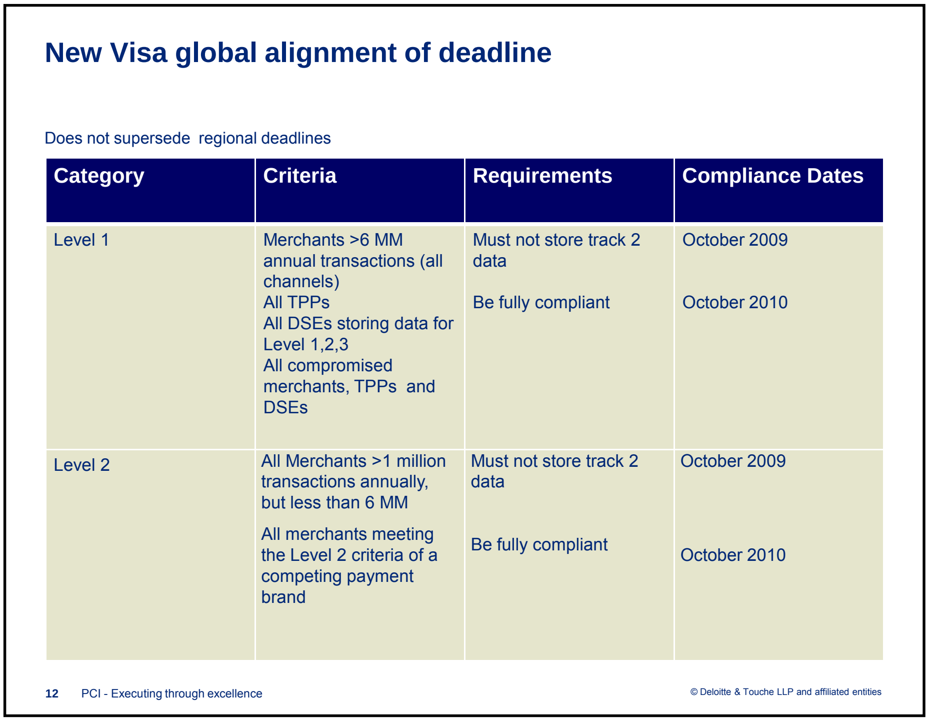
*2 TPPs and DSEs were previously required to have completed quarterly scans and self-assessments by 30 June 2004

Category	Criteria	Requirements	Compliance Dates
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 scans	30 June 2005 *2
Level 2	All Merchants >1 million transactions annually, but less than 6 MM All merchants meeting the Level 2 criteria of a competing payment brand	Annual self-assessment Quarterly network scans	31 December 2005



What level of compliance is applicable?

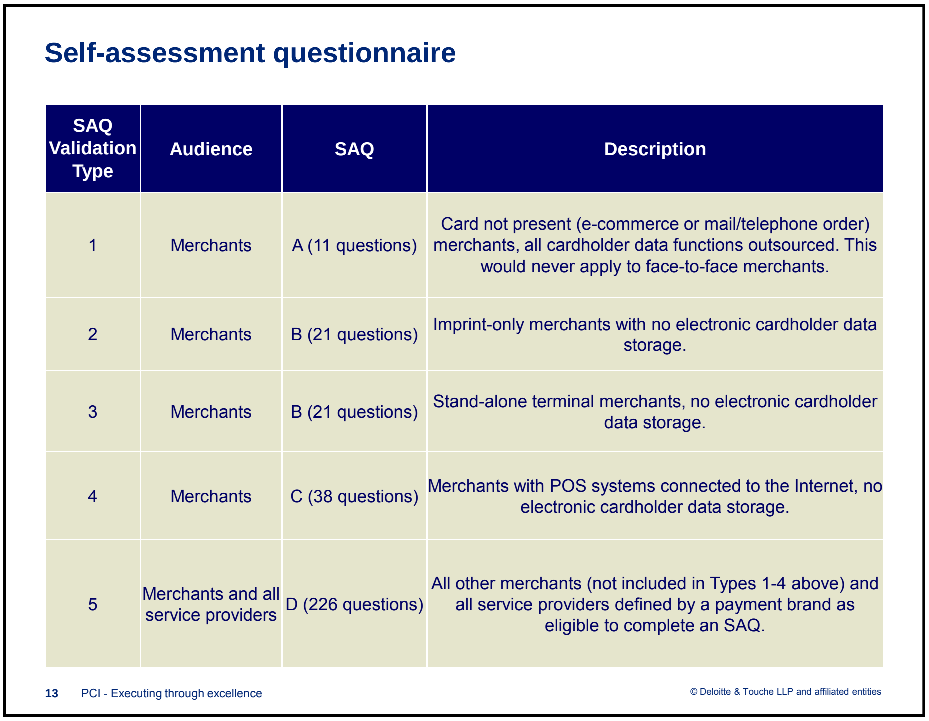
Category	Criteria	Requirements	Compliance Dates
Level 3	All Merchants with annual ecommerce transaction of >20,000 but less than 1 MM All Merchants meeting Level 3 criteria of a competing brand	Annual Self-Assessment Quarterly Network Scans	30 June 2005
Level 4	All other Merchants	Annual Self-Assessment Quarterly Network Scans	Consult Acquirer



New Visa global alignment of deadline

Does not supersede regional deadlines

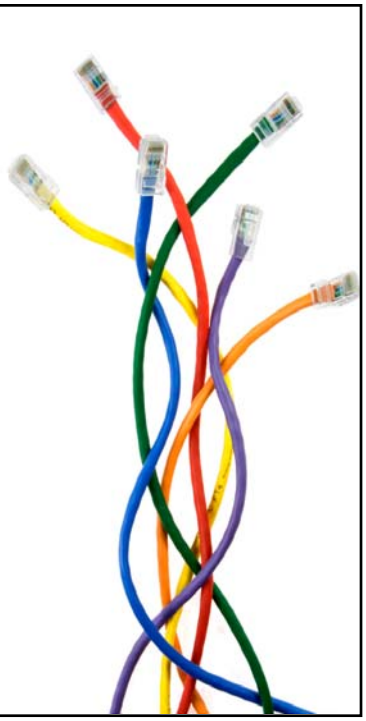
Category	Criteria	Requirements	Compliance Dates
Level 1	Merchants >6 MM annual transactions (all channels) All TPPs All DSEs storing data for Level 1,2,3 All compromised merchants, TPPs and DSEs	Must not store track 2 data Be fully compliant	October 2009 October 2010
Level 2	All Merchants >1 million transactions annually, but less than 6 MM All merchants meeting the Level 2 criteria of a competing payment brand	Must not store track 2 data Be fully compliant	October 2009 October 2010



Self-assessment questionnaire

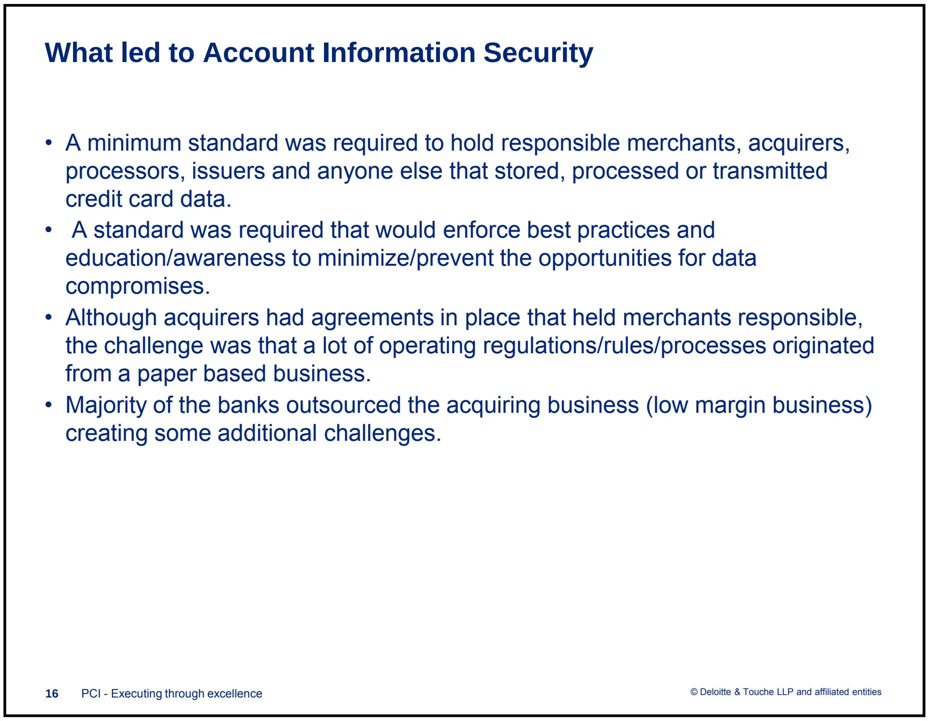
SAQ Validation Type	Audience	SAQ	Description
1	Merchants	A (11 questions)	Card not present (e-commerce or mail/telephone order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.
2	Merchants	B (21 questions)	Imprint-only merchants with no electronic cardholder data storage.
3	Merchants	B (21 questions)	Stand-alone terminal merchants, no electronic cardholder data storage.
4	Merchants	C (38 questions)	Merchants with POS systems connected to the Internet, no electronic cardholder data storage.
5	Merchants and all service providers	D (226 questions)	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.

What problem are we trying to solve?



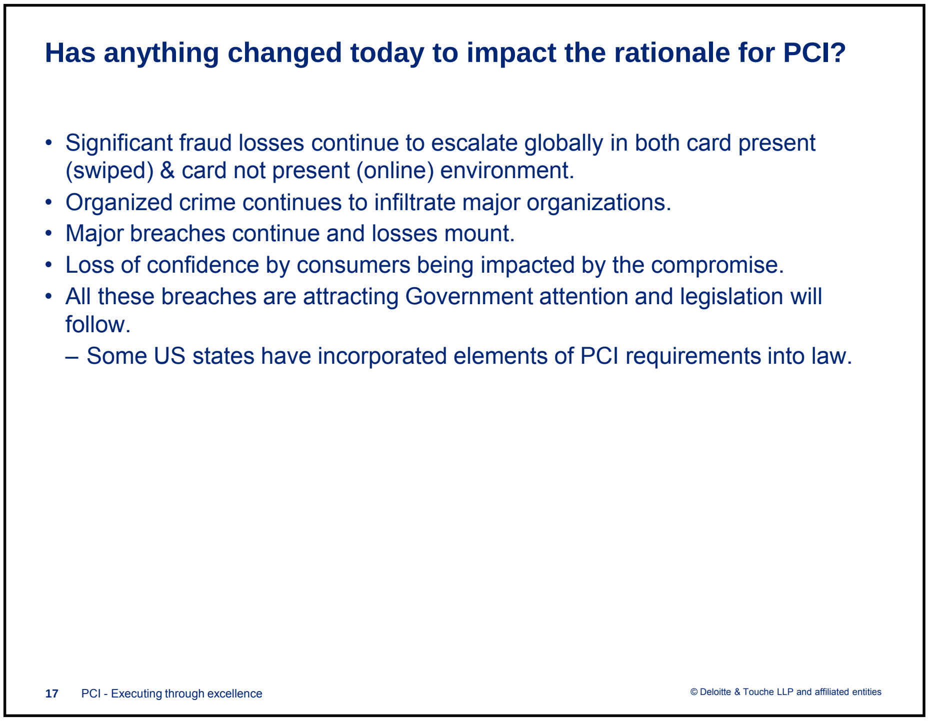
Background to the development of PCI

- Significant fraud losses were occurring globally in both card present (swiped) & card not present (online) environment:
  - – Stored data was not protected by acquirers/merchants
  - – Data was not protected by processors
  - – Transmission of credit card data in clear text, making it easy to compromise
  - – Organized crime infiltrated major organizations
  - – High proportion of compromise had a major internal component
  - – Lot more information continues to be stored than needed
- Brand impact can be significant, resulting in loss of confidence by consumers being impacted by the compromise.
- Significant costs to manage the fraud losses, not to mention loss of business.
- Visa was concerned that fraud losses were becoming acceptable as “cost of doing business”.



What led to Account Information Security

- A minimum standard was required to hold responsible merchants, acquirers, processors, issuers and anyone else that stored, processed or transmitted credit card data.
- A standard was required that would enforce best practices and education/awareness to minimize/prevent the opportunities for data compromises.
- Although acquirers had agreements in place that held merchants responsible, the challenge was that a lot of operating regulations/rules/processes originated from a paper based business.
- Majority of the banks outsourced the acquiring business (low margin business) creating some additional challenges.



Has anything changed today to impact the rationale for PCI?

- Significant fraud losses continue to escalate globally in both card present (swiped) & card not present (online) environment.
- Organized crime continues to infiltrate major organizations.
- Major breaches continue and losses mount.
- Loss of confidence by consumers being impacted by the compromise.
- All these breaches are attracting Government attention and legislation will follow.
  - Some US states have incorporated elements of PCI requirements into law.

Current threat environment

Point of Sale

- Cardholder data in transaction logs and memory (in particular magnetic strip data).
- Lack of encryption during store-fwd mode.
- Legacy equipment: non-unique accounts; inadequate activity monitoring.
- Physical security (POS terminal, PIN PAD, receipts, room keys).

Wireless

- Encryption strength.
- Continual surveillance/rogue device detection/regular scans.
- Vulnerabilities introduced through inadequate wireless architectures.

Web applications

- SQL injection/cross-site scripting/authentication by-pass.
- Poor coding practices/lack of security built into SDLC.

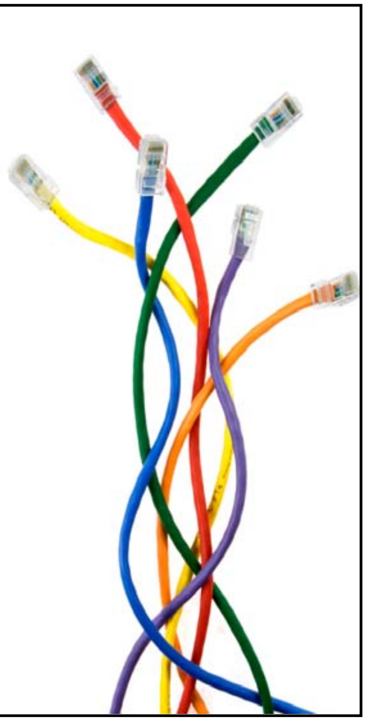
Data leakage/Data integrity

- Lack of role-based access control.
- Lack of adequate audit logging.
- Dealing with data at rest (database encryption, data retention).

Social engineering

- Internal breaches.
- Phishing/pharming.

What are the consequences of non-compliance?



Consequences of non-compliance

SCENARIO 1

- If an organization can demonstrate commitment, plans and steps taken towards compliance, whilst they may not be penalized by Visa or MasterCard, they are still responsible for the fraud as technically "they are still non-compliant". Regulatory authorities would probably also take sympathetic approach on penalties. Compliance date was Dec 31, 2005. Visa operating regulations has had this requirement since 2001.

- Visa has announced a global alignment of compliance validation deadlines. They do not supersede previously announced regional deadlines

Consequences of non-compliance

SCENARIO 2

- If an organization has complied with PCI requirements and has been validated as such, they are granted safe harbor. They will be responsible for only the fraud transactions under the chargeback rules.

SCENARIO 3

- If a company is not compliant and has NOT demonstrated to Visa or MasterCard that they have the commitment, plans and taken steps towards full compliance, they are not only subjected to penalties as in the case of a major US Retailer, but also liable for all fraud and punitive damages that courts may award, as well costs of replacement cards. Brand damage is a separate issue, as is action by regulatory authorities which can possibly impact the survival of the business based on the circumstances and extent of the breach.

Deloitte.