

# Compliance with PCI Data Security Standard

presented to

## HASDIA

August 26, 2011

# Introduction to Experis (History and Direction)



- Three of the most successful brands in talent management and project solutions – Jefferson Wells, Manpower Professional and COMSYS – have combined forces to form Experis.
- In the past, each company has brought you the solutions to immediate business problems.
- \$1.3 billion part of ManpowerGroup, a \$19 billion company with combined operations in over 80 countries.
- We help clients accelerate their success and create a competitive advantage globally .
- Our strategic direction is based on business growth through multiple delivery channels
  - Local Experis offices
  - Centers of Expertise
  - Strategic Client Management.

# Experis Finance Practices

Risk Advisory	Tax	Finance & Accounting
<ul style="list-style-type: none"> <li>• Internal Audit, Controls and Regulatory Compliance</li> <li>• Governance and Risk Management</li> </ul>	<ul style="list-style-type: none"> <li>• Federal Tax Compliance and Consulting</li> <li>• Tax Accounting Reporting and Consulting</li> <li>• Tax Risk Management</li> </ul>	<ul style="list-style-type: none"> <li>• Financial Reporting and Compliance</li> <li>• Process Optimization</li> <li>• Finance Transformation</li> <li>• Finance Organization Support</li> </ul>

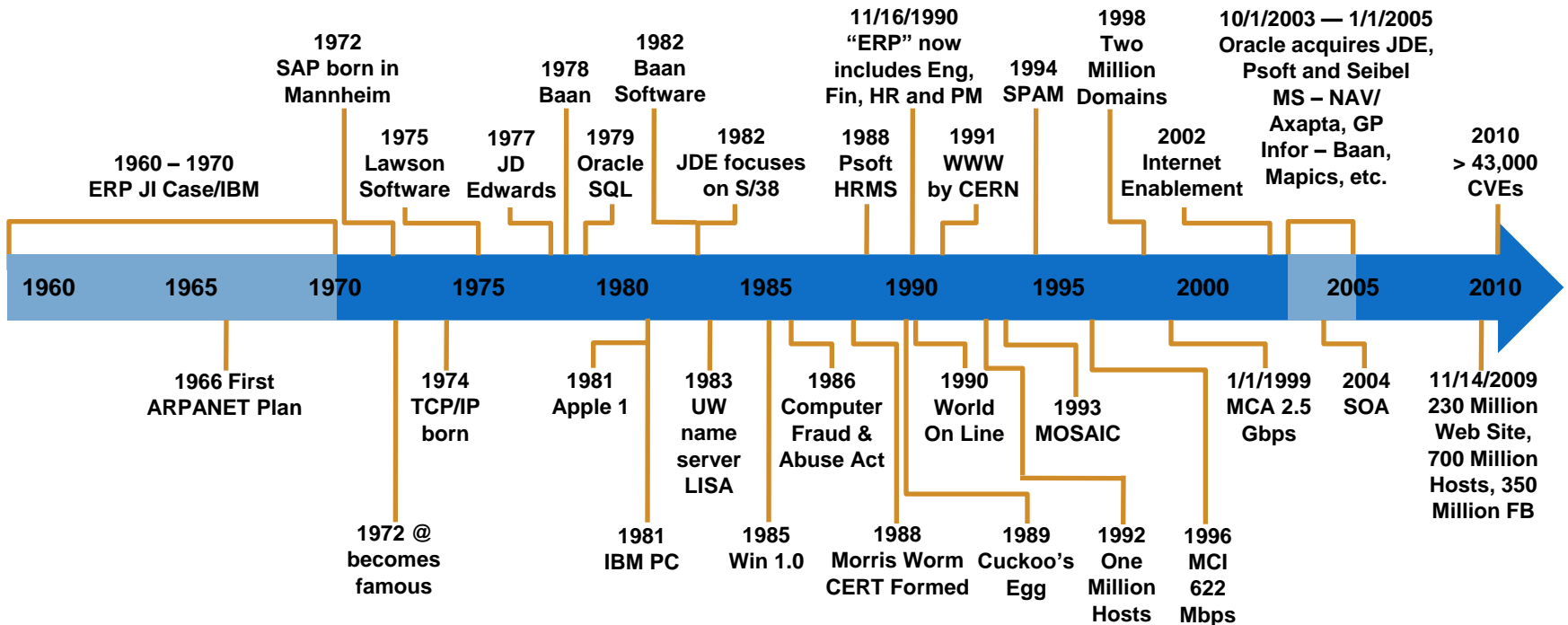
## Centers of Expertise by Practice

<ul style="list-style-type: none"> <li>• Business System Services Center of Expertise</li> <li>• Construction Services Center of Expertise</li> <li>• Financial Institution Business Services Center of Expertise</li> <li>• <b>Information Security Center of Expertise</b></li> </ul>	<ul style="list-style-type: none"> <li>• International Tax Center of Expertise</li> <li>• Transfer Pricing Center of Expertise</li> <li>• State and Local Tax Center of Expertise</li> <li>• Tax Accounting Automation Center of Expertise</li> </ul>	<ul style="list-style-type: none"> <li>• Technical Accounting and Financial Reporting Center of Expertise</li> </ul>
---	---	--

# The IS COE offers security capabilities across the spectrum of planning and implementation for the protection of information

Information Security Capabilities					
Information Security Governance	Privacy & Regulatory Compliance	Cyber Security	PCI/TG3 Validation	Business Continuity	Technical Security Solutions
Security Organization Assessment & Development	Industry Regulatory Assessments & Remediation Support (e.g., HIPAA, GLBA)	Computer Forensics	Readiness Assistance	Business Impact Analysis	Risk remediation design, implementation and management
Information Security Enterprise Risk Assessments	Privacy Assessments & Remediation Support	Penetration Testing	Compliance Validation (Report on Compliance and Attestation)	Business Continuity Planning & Testing	Security Technology Architectures
Information Security Strategy Development	Information Security Audits	Customized Goal-Oriented Penetration Exercises	Remediation Assistance	Disaster Recovery Strategy and Planning	Identity Management
Security Policies & Frameworks (e.g., ISO 27000)	Security Policies/Procedures Alignment Analysis	Vulnerability Assessments	Compliance Mgt Program Services		Application Security
Security Awareness & Training	Security Compliance Training & Education	Network, Wireless and Web Application Security Reviews	ASV Services		Cloud & Virtualization Security
Data Protection & Loss Prevention			TG3 ATM Network Reviews		System & Network Security Controls

# Evolution of technology - Technology timeline



## Agenda

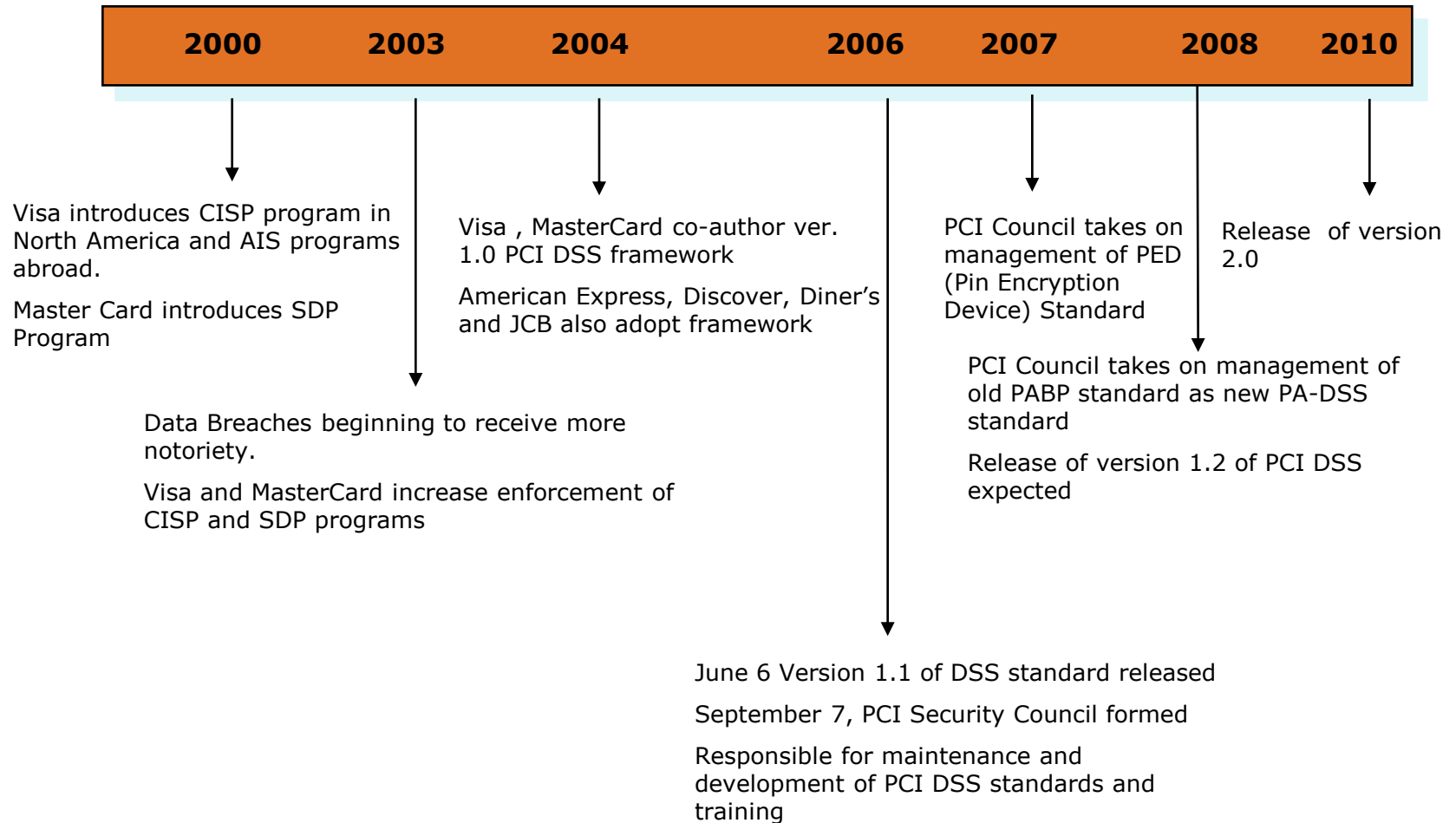
- Introductions
- Objectives
- Overview of PCI and Status to Date
- Changes to the Payment Card Industry (PCI) Landscape
- Compliance Pitfalls
- Open Discussion and Questions?

# Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a common security framework agreed upon by the six major card brands, Visa, MasterCard, American Express, Diner's Club, Discover and JCB. The primary purpose of the PCI DSS standard is to protect cardholder information by:

- Aligning data security initiatives that are critical to safeguarding the payment infrastructure
- Ensuring a consistent standard of care is used to protect payment account, transaction and authorization data
- Providing a uniform framework aimed at standardizing security measures for the protection of cardholder data
- Providing a consistent methodology for assessing potential risk to cardholder data

# PCI has evolved over the past 10 years



# PCI Standards

- **PCI Standards include:**
  - **PCI DSS**
  - **Payment Application-DSS  
(formerly Payment Application Best Practices [PABP])**
  - **PIN Transaction Security  
(PTS - formerly PIN encryption device [PED])**

# Data Security Standard - Overview

PCI DSS Requirement	Summary Objectives
<b>Build and maintain a secure network (38)</b>	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
<b>Protect cardholder data(34)</b>	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
<b>Maintain a vulnerability management program (33)</b>	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
<b>Implement strong access control measures (50)</b>	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
<b>Regularly monitor and test networks(39)</b>	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
<b>Maintain an information security policy(39)</b>	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security</li> </ol>

## Compliance Requirements

- Any entity that stores, processes or transmits cardholder information **MUST COMPLY** with PCI Data Security Standard (DSS)
- Entities include but are not limited to:
  - **Acquirers**
  - **Merchants**
  - **Service providers**
  - **Trusted third parties**
  - **Issuers (with some exceptions)**
- Each brand has its own process for validating compliance based on this general standard

# What is a Merchant?

- **Any business entity that accepts credit cards, payment cards, debit cards, etc., as payment for goods and services**
- **Can be traditional brick-and-mortar business, Internet, telemarketing or mail order**
- **Not a payment card brand member or service provider**

## What is a Service Provider?

- **Any business entity directly involved with processing, storage, transmission and switching of transaction data or cardholder data**
- **Not a payment card brand member or merchant**
- **Includes companies that provide services to merchants, service providers or brand members that control or could impact the security of cardholder data**

## Examples of Service Providers

- Transaction processors
- Payment gateways
- Independent sales organizations (ISO) or external sales agents (ESA)
- Credit reporting services
- Customer service functions
- Plastic card embossing
- Remittance processing
- Managed firewall and IDS service providers
- Telecommunication companies are **NOT** included

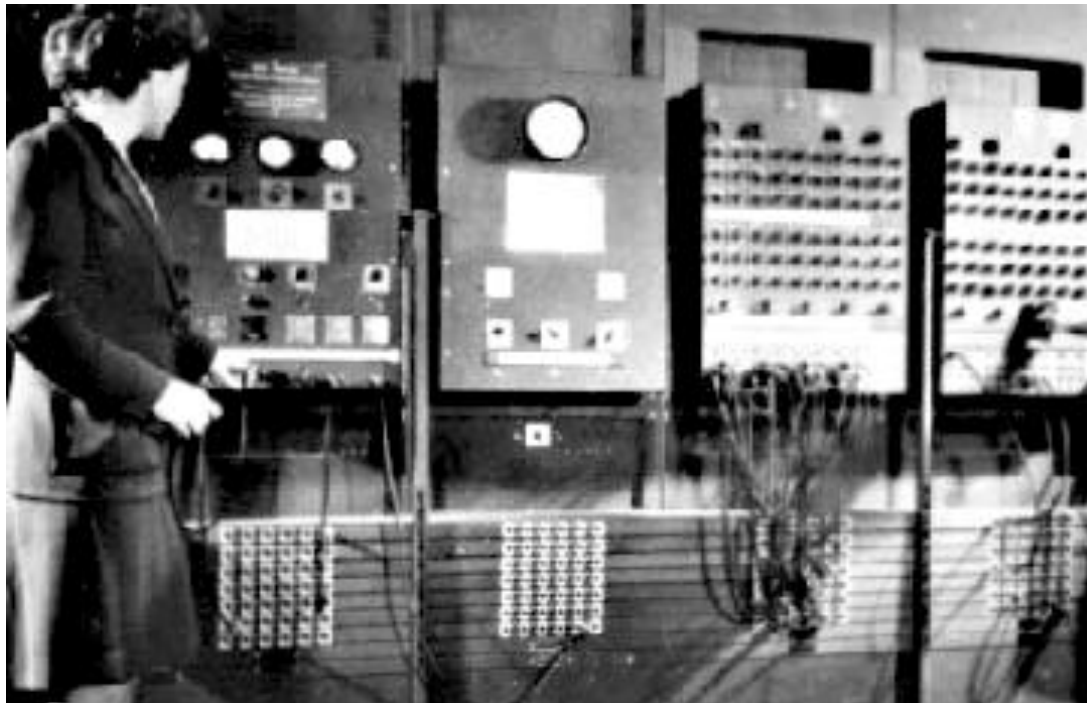
## Validation Requirements - Merchants

- All merchants must comply with the PCI DSS (all brands)
- Validation of merchant requirements vary by payment brand
- Defined merchant levels are based upon transaction volume
  - Compliance validation requirements are based upon these levels

# Appreciate the past...

Rear Adm. Grace M. Hopper

ENIAC Team/COBOL - 1940s and forward



# Appreciate the past...

## 09/09/45 – “debugging” was born...

Photo # NH 96566-KN First Computer "Bug", 1945

92

9/9

0800 Antan started  
 1000 " stopped - antan ✓  
 13°C (032) MP - MC ~~1.582647000~~  
 (033) PRO 2 2.130476415  
 correct 2.130676415

{ 1.2700 9.037 847 025  
 9.037 846 995 correct  
 4.615925059(-2)

Relays 6-2 in 033 failed special speed test  
 in relay " 11.00 test.

Relay  
 2145  
 Relay 2371

1100 Started Cosine Tape (Sine check)  
 1525 Started Multi-Adder Test.

1545



Relay #70 Panel F  
 (moth) in relay.

1630 Antan started.  
 1700 closed down.  
 First actual case of bug being found.

# Validation Terminology

- **ASV - Approved Scanning Vendor**
- **QSA – Qualified Security Assessor**
- **SAQ – Self Assessment Questionnaire (associated characteristics)**
  - **SAQ A** = no CHD in electronic format, ecommerce site OK, 3<sup>rd</sup> party compliance
  - **SAQ B** = no CHD in electronic format, imprint only or telephone dial out
  - **SAQ C** = no electronic CHD, standalone store with Payment Application
  - **SAQ D** = everyone else that isn't required to do a RoC, and does not qualify for A,B or C
- **RoC - Report on Compliance – Full Security Audit Procedures**
- **iRoC – Interim RoC**
- **AoC - Attestation of Compliance**

# Validation Levels - Merchants

## Global Merchant Levels

Level	American Express	Discover	JCB	MasterCard	Visa Inc.	Visa Europe
1	Merchants processing more than 2.5 million American Express transactions annually or otherwise deemed a Level 1 by American Express	Merchants processing more than 6 million Discover transactions annually or otherwise deemed Level 1 by Discover Merchants required by other payment brands to report as Level 1	Merchants processing more than 1 million JCB transactions annually, or compromised Merchants	Merchants processing more than 6 million MasterCard transactions annually or those that have experienced an account data compromise Merchants identified by another payment brand as Level 1	Merchants processing more than 6 million Visa transactions annually (all channels) or global Merchants identified as Level 1 by any Visa region	Merchants processing over 6 million Visa transactions annually (all channels) or compromised Merchants
2	Merchants processing 50,000 to 2.5 million American Express transactions annually or otherwise deemed a Level 2 by American Express	Merchants processing 1 million to 6 million Discover transactions annually Merchants required by another payment brand to validate and report as Level 2	Merchants processing less than 1 million JCB transactions annually	Merchants processing 1 million to 6 million MasterCard transactions annually All Merchants meeting the Level 2 criteria of a competing payment brand	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	Merchants processing 1 million to 6 million Visa transactions annually
3	Merchants processing less than 50,000 American Express transactions annually	Merchants processing 20,000 to 1 million Discover Card not present only transactions annually Merchants required by another payment brand to validate and report as Level 3	N/A	Merchants processing 20,000 to 1 million MasterCard e-commerce transactions annually All Merchants meeting the Level 3 criteria of a competing payment brand	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually
4	N/A	All other Discover Card merchants	N/A	All other MasterCard Merchants	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other Merchants up to 1 million transactions annually	All other Merchants processing up to 1 million Visa transactions annually

# Validation Requirements - Merchants

## Merchant Validation Requirements

Level	American Express	Discover	JCB	MasterCard	Visa Inc.
1	Annual on-site assessment by Qualified Security Assessor (QSA) (or internal audit if signed by officer of Merchant company) Quarterly network scans by Authorized Security Vendor (ASV)	Annual on-site assessment by QSA or internal audit Quarterly network scans by ASV	Annual on-site assessment by QSA Quarterly network scans by ASV	Annual on-site assessment by QSA Quarterly network scans by ASV	Annual on-site assessment by QSA* Quarterly network scans by ASV Attestation of Compliance form
2	EU Only: Annual Self Assessment Questionnaire (SAQ) Quarterly network scans by ASV	Annual SAQ Quarterly network scans by ASV	Annual SAQ Quarterly network scans by ASV	<b>Annual SAQ or Annual On site</b> Quarterly network scans by ASV	Annual SAQ** Quarterly network scans by ASV Attestation of Compliance form
3	Quarterly network scans by ASV (recommended) EU Only: SAQ (recommended)	Annual SAQ Quarterly network scans by ASV	N/A	Annual SAQ Quarterly network scans by ASV	Annual SAQ** Quarterly network scans by ASV Visa Europe: Either complete annual SAQ and quarterly network scans OR use PCI DSS Certified Payment Service Providers for all payment processing, storage and transmission
4	N/A	Compliance validation requirements determined by acquirer Recommended validation: Annual SAQ and quarterly network scans	N/A	Compliance validation is at discretion of acquirer To validate: Annual SAQ and quarterly network scans	Annual SAQ recommended Quarterly network scans by ASV recommended Compliance validation requirements set by acquirer

## Validation Requirements – Service Providers

- **All payment brands require that service providers comply with the PCI DSS requirements**
- **Service providers include acquirers, third-party processors (TPPs), data storage entities (DSEs) or any other entity that stores, processes or transmits cardholder data**
- **Compliance requirements and validation requirements vary by brand**
- **Visa and MasterCard**
  - **Categorize service providers according to transaction volume and/or the type of service provider**
  - **PCI compliance validation is according to the service provider level**
- **American Express, Discover and JCB**
  - **Service providers are not categorized according to transaction volume**
  - **All service providers are required to comply with PCI DSS**

# Validation Levels – Service Providers

## Global Service Provider Levels

Level	American Express	Discover	JCB	MasterCard	Visa Inc.	Visa Europe
1	All Third-Party Processors (TPPs)	All Service Providers, including but not limited to TPPS and Payment Service Providers (PSPs)	All TPPs	All TPPs All Data Storage Entities (DSEs) that store, transmit or process more than 1 million total combined MasterCard and Maestro transactions annually All compromised TPPs and DSEs	VisaNet processors or any service provider that stores, processes and/or transmits more than 300,000 transactions per year	VisaNet processors or any Service Provider that stores, processes and/or transmits more than 300,000 transactions per year
2				All DSEs that store, transmit or process less than 1 million total combined MasterCard and Maestro® transactions annually	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year	Any Service Provider that stores, processes and/or transmits less than 300,000 transactions per year

# Validation Requirements – Service Providers

## Service Provider Validation Requirements

Level	American Express	Discover	JCB	MasterCard	Visa Inc. / Europe
1	<p>Annual on-site security assessment by QSA (or internal audit if signed by officer of Service Provider)</p> <p>Quarterly network scans by ASV</p>	<p>Quarterly network scans by ASV and one of the following:</p> <ul style="list-style-type: none"> <li>Annual on-site security assessment by QSA (or internal audit if signed by officer of Service Provider)</li> </ul> <p>Annual SAQ D</p>	<p>Annual on-site review by QSA</p> <p>Quarterly network scans by ASV</p>	<p>Annual on-site review by QSA</p> <p>Quarterly network scans by ASV</p>	<p>Annual Report of Compliance by QSA</p> <p>Quarterly network scans by ASV</p> <p>Attestation of Compliance form</p> <p>Included on Visa's list of PCI DSS-Compliant Service Providers</p>
2				<p>Annual SAQ</p> <p>Quarterly network scans by ASV</p>	<p>Annual SAQ</p> <p>Quarterly network scans by ASV</p> <p>Attestation of Compliance form</p> <p>Not included on Visa's list of PCI DSS-Compliant Service Providers</p>

## Visa Safe Harbor

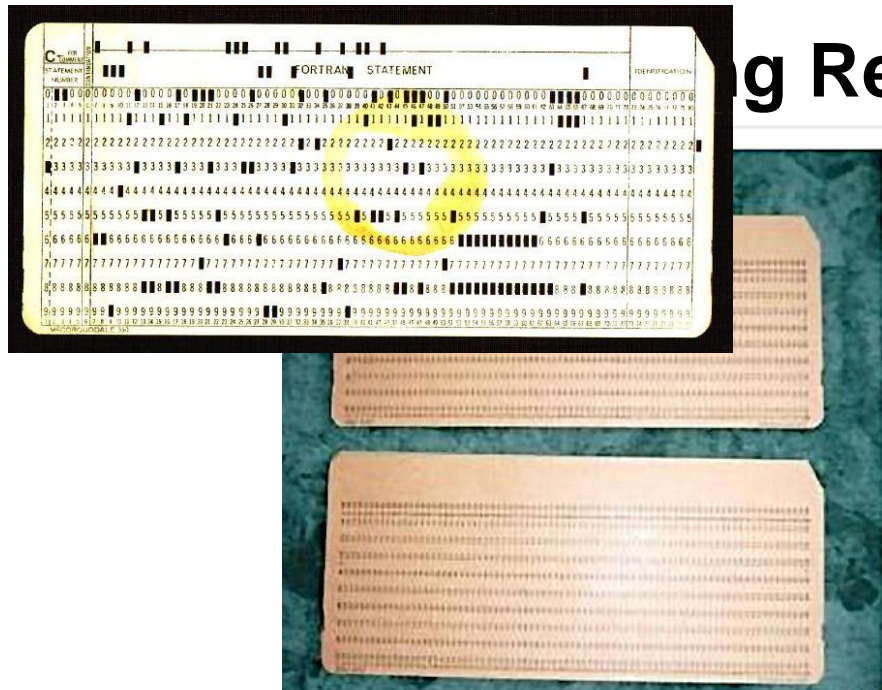
Safe harbor provides members protection from Visa fines in the event its merchant or service provider experiences a data compromise. To attain safe harbor status:

- A member, merchant, or service provider must maintain full compliance **at all times**, including at the time of breach as demonstrated during a forensic investigation
- A member must demonstrate that prior to the compromise their merchant **had already met** the compliance validation requirements, demonstrating **full compliance**

In other words, the submission of compliance validation documentation, in and of itself, does not provide the member safe harbor status. The entity must have adhered to all the requirements **at the time** of the compromise

# Appreciate the past...

## Herman Hollerith – 1890s



## ing Recording Co.

### 10 Vintage Computer Punch Cards VGC

Item condition: --

Time left: 6d 05h (31 Mar, 2010 19:47:22 BST)

Bid history: 0 bids

Starting bid: **£1.99**  
Approximately EUR 2.22

Enter maximum bid: £   
(Enter £1.99 or more)

[Place bid](#)

[Watch this Item](#)

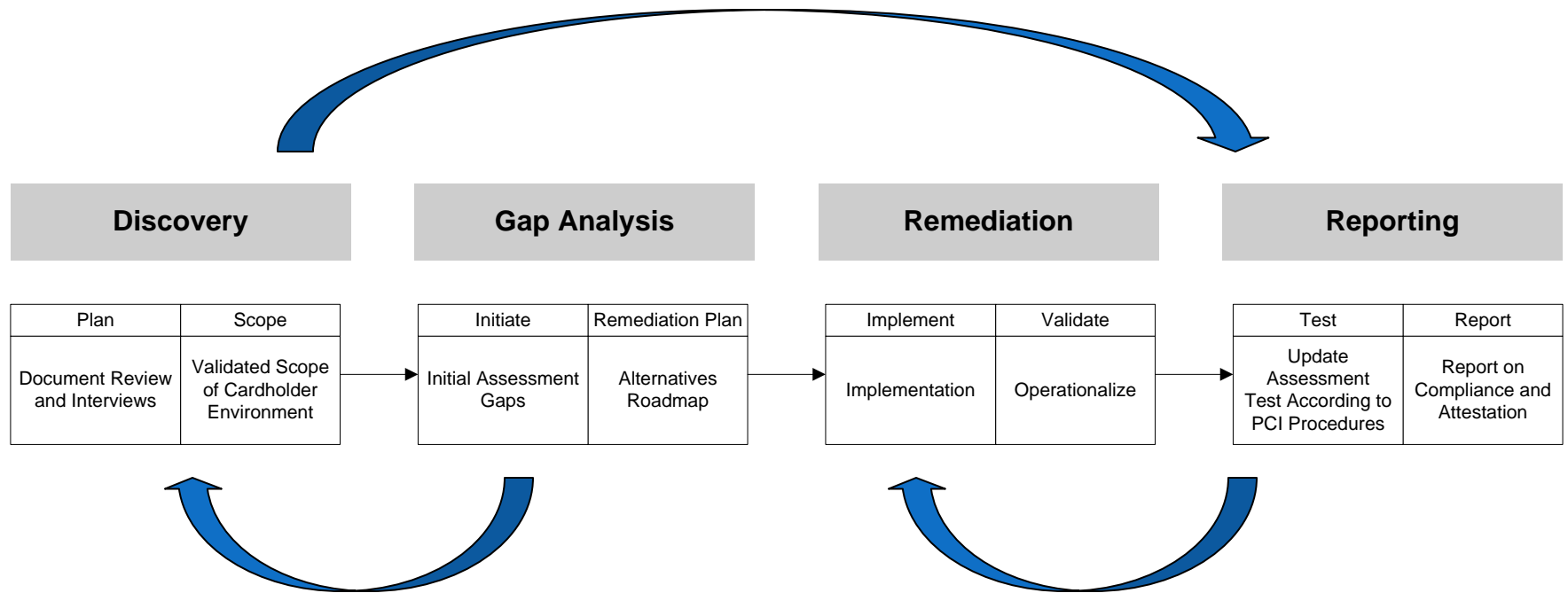
# What Data Can be Stored

	<b>Data Element</b>	<b>Storage Permitted</b>	<b>Protection Required</b>	<b>PCI DSS Req. 3.4</b>
<b>Cardholder Data</b>	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	Yes	<b>No</b>
	Service Code	Yes	Yes	<b>No</b>
	Expiration Date	Yes	Yes	<b>No</b>
<b>Sensitive Authentication Data</b>	Full Magnetic Stripe	<b>No</b>	<b>N/A</b>	<b>N/A</b>
	<u>CVV2</u> / CID/ CAV2/ CVC2	<b>No</b>	<b>N/A</b>	<b>N/A</b>
	PIN/ PIN Block	<b>No</b>	<b>N/A</b>	<b>N/A</b>

# Cardholder data storage

- What parts of the cardholder data is allowed to be stored, transmitted or processed?
  - *PAN, expiration date, service code, and name*
- What methods should be used to protect the PAN when it is stored?
  - ***Rendered unreadable: encryption, hashing, masking or truncation***
- What cardholder data can not be stored post-authorization?
  - *Full track data*
    - Track 1
    - Track 2
  - *CID, CAV2, CVC2, and CVV2*
  - *PIN block*

# Planning and Reaching Compliance



# Changes to the PCI Landscape — Where do they come from?

- **Major contributors to change**
  - **PCI Council**
    - **Changes to the Payment Card Industry Data Security Standards (PCI DSS)**
    - **Changes to the Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) programs**
    - **Special interest groups**
  - **Card brand companies**
    - **Merchant and Service Provider classifications**
    - **Validation requirements**

## Changes to the PCI Landscape — Where do they come from? (Continued)

- **Major contributors to change**
  - **State and federal legislation**
    - **PCI-specific**
    - **Privacy**
    - **Breach**
  - **Technology**
    - **Virtualization**
    - **Cloud computing**
    - **End-to-end encryption**
  - **Breaches**

## Changes — Who do they affect?

- **Merchants and service providers**
  - **The PCI DSS Standards**
  - **Card brand company classifications and validation requirements**
  - **State and federal legislation**
  - **Technology**
  - **Breaches**
- **QSA and ASV companies**
  - **Changes to the QSA, ASV and Payment Application (PA)-QSA programs**

# Changes — PCI DSS

- PCI DSS
  - Version 1.2 released October 2008
  - Version 1.2 SAQ released October 2008
  - Requirement 6.6 as of 6/30/2008
  - Wireless
    - No new Wired Equivalent Privacy (WEP) as of 3/31/2009
    - No WEP after 6/30/2010
  - Version 1.2.1 release July 2009
    - Minor corrections
  - Version 2.0 release October 2010
    - Mostly corrections and clarifications

# Changes —Special Interest Groups (SIGs)

- SIG Examples
  - Pre-authorization
  - Scoping
  - Virtualization
  - Wireless
  - Voice recording
  - Tokenization

# Changes —Wireless Guidance

- Requirement 11.1
  - Verify no rogue Wireless Access Points (WAPs), either by wireless IDS/IPS or quarterly scans
  - An organization may not sample but must scan all locations quarterly
  - IDS for rogue WAP detection acceptable
  - Sampling may be used to verify requirement during assessment

# Changes — Wireless Guidance

(Continued)

- Requirement to comply with entire PCI DSS with extra attention to:
  - Physical security of wireless devices
  - Changing default values and passwords
  - Logging or wireless access and intrusion prevention
  - Strong authentication and encryption
  - Strong cryptography and security protocols
  - Development and enforcement of wireless usage policies

# Changes —PA-DSS

- Formerly Visa's PABP program
  - Responsibility assumed by PCI Council on April 15, 2008
    - Release version 1.1 of PA-DSS formerly PABP version 1.4
    - Change included clarifications and enhancements to Standard
    - Released version 1.2 of PA-DSS October 2008
    - Changes between 1.1 and 1.2 all clarifications

## Changes —PA-DSS (Continued)

- VISA announcements on June 24, 2009
  - Require all VISA clients to use PA-DSS-compliant applications by July 1, 2012
    - Phase 1 – all newly signed merchants and agents must use PA-DSS-compliant apps by July 1, 2010
    - Phase 2 – all remaining merchants and agents must use PA-DSS-compliant apps by July 1, 2012

# Changes —PTS

- PIN transaction security
  - Formally PED (PIN Encryption Device) Standard
  - Expanded focus to include
    - Point-of-sale (POS) devices
    - PED
    - Hardware security modules
    - Unattended payment terminals

## Changes — Card Brands

- Responsible for compliance programs
  - VISA – Cardholder Information Security Program (CISP)
  - MasterCard – Site Data Protection (SDP)
  - American Express – Data Security Operating Policy (DSOP)
  - Discover - Discover Information Security and Compliance (DISC)
  - JCB – JCB Data Security Program
- Set classification levels and validation requirements
- Define reporting requirements

## Changes — Service Providers

- Consolidation of Service Provider Levels
  - Went from three to two
  - Level 1 requires on-site assessment
  - Level 2 can complete Self-Assessment Questionnaire (SAQ)
  - All must complete external scans
  - VISA lowered transaction limit to 300,000 from 1,000,000
  - Only Level 1 providers will be included on list of compliant providers

## Changes — Merchants

- December, 2009 — MasterCard changes validation requirements
  - Level 1 Self Assessors must file ROC
  - Level 2 merchants may chose to complete on site by QSA or SAQ by MQSA
  - Must contract with a QSA to perform on site assessment
  - Validation by certified assessor (MQSA or QSA) must be performed by June 30, 2011

# Changes — QSA Program

- PCI Council launches QA Program
  - Third quarter 2008
  - Provide mechanism to monitor and assess quality of QSA companies
  - Provide a level of consistency within the industry
  - Ensure competence among QSA companies

## Common Pitfalls = Top Ten Technical Safeguards?

- Internal Accountability
- Lack of Planning/Short Compliance Window
- Trusted Third Parties
  - Access and Compliance
- Section 6.6 Code Review or Application Firewall
- Wireless Scanning
- Network Without Secure Zones
- Monitoring and Logging
- Application Compliance
- File Integrity Monitoring

# Appreciate the past...



## Jefferson Wells Qualifications

- Qualified Security Assessor Company (QSA)
  - *Over 35 Qualified Security **Assessor** Professionals*
  - *200 **PCI-related** engagements*
  - *A provider of PCI-related services since 2003*
  
- Approved Scanning Vendor (ASV)
  - *Performed over hundreds of **PCI-related** scans*
  - *Offer Penetration Testing services for PCI Req. #11.3*
  - *Offer Wireless Security Audits for PCI Req. #11.1*

# Fun Fact

**Patented in 1970, it was originally called the "X-Y Position Indicator for a Display System".**

**What is it called today?**

# Fun Fact



**Invented in 1963 by Douglas Engelbart  
at Stanford Research Institute**

# Useful Links

- PCI Council Home Page
  - <https://www.pcisecuritystandards.org/>
- PCI Council Press Releases
  - [https://www.pcisecuritystandards.org/news\\_events/press\\_releases.shtml](https://www.pcisecuritystandards.org/news_events/press_releases.shtml)
- PCI DSS Supporting Documentation
  - [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_supporting\\_docs.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml)

# More Useful Links

- Visa Media Center for Press Releases
  - <http://corporate.visa.com/media-center/press-releases/main.jsp>
- Summary of changes PA-DSS 1.1 to 1.2
  - [https://www.pcisecuritystandards.org/pdfs/pci\\_pa-dss\\_summary\\_changes\\_%20v1%20-%20v12.pdf](https://www.pcisecuritystandards.org/pdfs/pci_pa-dss_summary_changes_%20v1%20-%20v12.pdf)

# Additional Information

- Visa USA
  - <http://www.visa.com/cisp>
- Visa Canada
  - <http://www.visa.ca/ais>
- Visa Europe
  - <http://www.visaeurope.com>
- MasterCard
  - <http://www.mastercard.com/sdp>

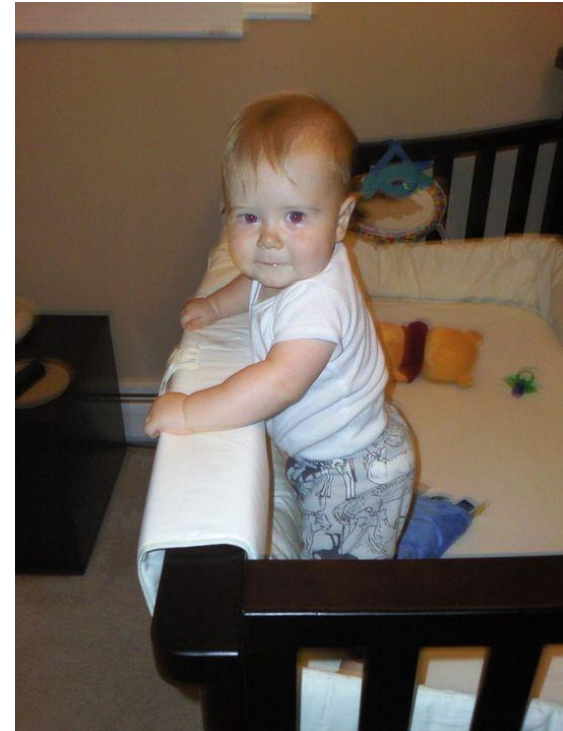
# John Hainaut

Information Security Center of Expertise  
Practice Director

[john.hainaut@experis.com](mailto:john.hainaut@experis.com)

**312-980-4910**

**[www.experis.com](http://www.experis.com)**



Thank you for your participation!