Marvin Odor
Sr. Security Consultant

Experience:

- Over 7 years of experience in the information security field.
- With 4 years of experience conducting PCI gap analysis, PCI report on compliance (ROC) assessments and self-assessment questionnaires (SAQ), in retail, transportation, telecommunication, entertainment, and financial institutions.

- Professional Designations:
- CISSP : Certified Information Systems Security Professional
- CISA : Certified Information Systems Auditor
- PCI QSA : Payment Card Industry Qualified Security Assessor
- PCIP : Payment Card Industry Professional
- LinkedIn: https://ca.linkedin.com/in/marvinodor

SO, YOU'RE THINKING ABOUT ACCEPTING CREDIT CARD PAYMENTS?

Go for Dough Bakery

Go-for-Dough.com

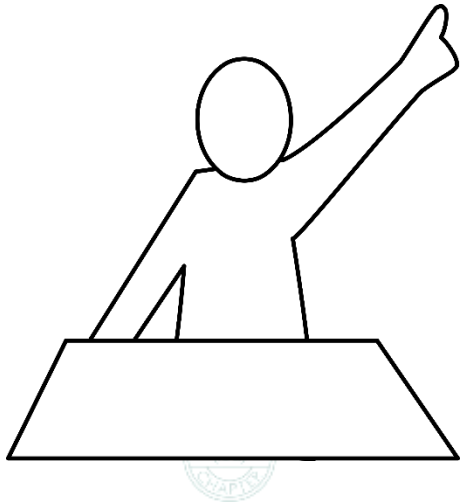
Overview

- **What is PCI DSS?**
- **PCI History**
- **Who needs to comply with PCI DSS?**
- **PCI Data Security Standard v3.1 Requirements**
- **Benefits of compliance**

What is PCI DSS?

- **The Payment Card Industry Data Security Standards (PCI DSS)**
  - Baseline
  - Minimum set of Technical and Operational requirements to protect account data.
  - Developed and managed by the Payment Card Industry Security Standards Council (PCI SSC) on a global basis.

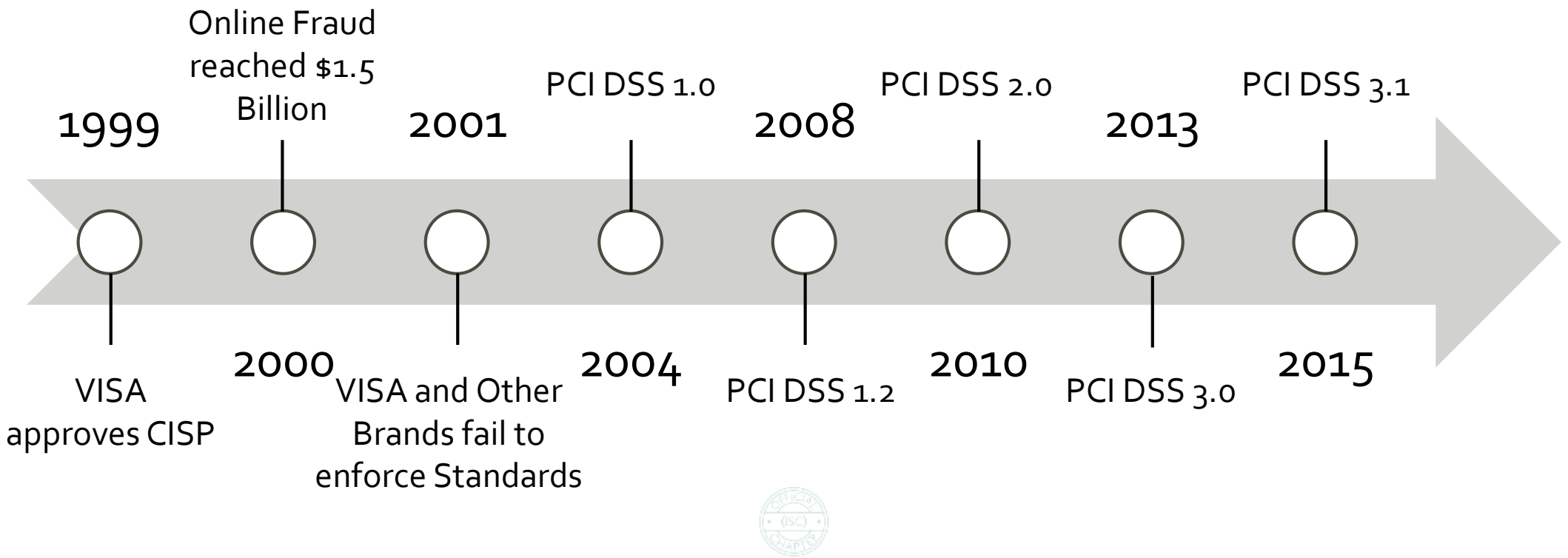
Q: Why is PCI DSS managed by the Payment Card Industry Security Standard Council (PCI SSC)?



Prior to e-commerce and PCI DSS

- Between 1988 to 1998 Visa/MasterCard International credit card fraud losses totaled approximately 750 Million Dollars in the United States. Note, this is a very small amount compared to credit card charge volume of 750 billion dollars for the same time period.
- Visa USA developed Cardholder information security program (CISP) in 1999.
- Early collaboration between MasterCard and Visa to protect cardholder data introduced gaps and in-consistencies between programs.
- Another problem was the other major payment card brands were running their own program.
  - Discover - Discover Information Security & Compliance (DISC)
  - MasterCard - Site Data Protection Program (SDP)
  - Amex - Data Security Operating Policy
  - JCB - JCB Data security Program (JDSP)
  - Visa Canada - Account Information Security (AIS)

PCI History Timeline



Who needs to comply with PCI DSS?

- All entities:
  - Merchants
  - Issuers
  - Service providers (third-party vendors, gateways, processors)

- That:
  - Store, Process or Transmit Cardholder data or sensitive authentication data

What is account data?

Account Data	Data Element
Cardholder Data	Primary Account Number (PAN)
	Cardholder Name
	Expiration Date
	Service Code
Sensitive Authentication Data	Full Track data (Magnetic-Stripe data or equivalent on a chip)
	CAV2/CVC2/CVV2/CID
	Personal Identification Number (PINs) / PIN Block

What can be Stored?

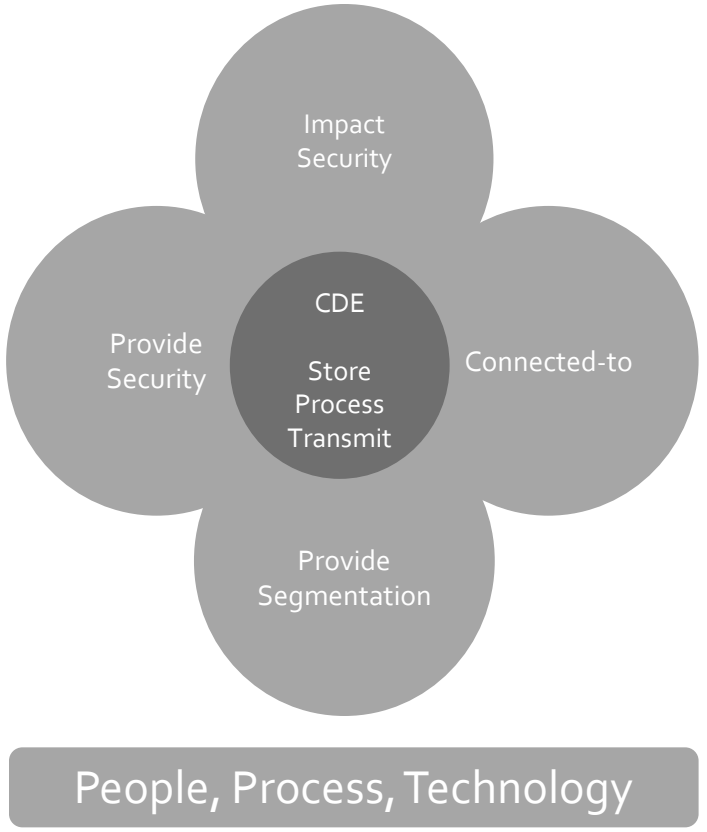
Account Data	Data Element	Storage Permitted	Render stored data Unreadable per Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data	Full Track Data	No	Cannot be stored after authorization
	CAV2/ CVC2/CVV2/CID	No	Cannot be stored after authorization
	Personal Identification Number (PIN) / PIN Block	No	Cannot be stored after authorization

- All cardholder data must be protected as per PCI DSS requirements.
- Sensitive authentication data must not be stored after authorization (even if encrypted).

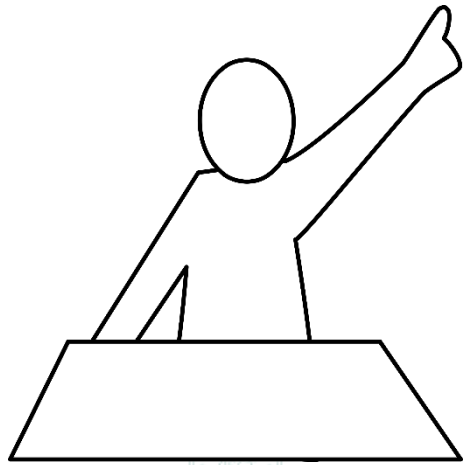
Scope Overview

- Where does cardholder data flow?
  - Document all cardholder data flows, between applications, systems and network infrastructure
  - Have a good inventory

- Where is cardholder data stored?
  - Storage locations
  - Thorough search of all systems
  - Prevent cardholder data leak



Q:Why is it important to review PCI scope at least on an annual basis?



PCI Scope Reduction

All cardholder data must be protected as per PCI DSS requirements.

- Do not store cardholder data (Data Removal)
- Encrypted cardholder data**
- Tokenization
- Point- to-Point encryption solution.

PCI Data Security Standard v3.1

Goals	Req #	Requirements
Build and Maintain a Secure Network	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect credit card information	**3**	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5**	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7**	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	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 for all personnel

PCI Data Security Standard v3.1

Goals	Req #	Requirements
Build and Maintain a Secure Network	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters

PCI Data Security Standard v3.1

Goals	Req #	Requirements
Protect credit card information	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks

PCI Data Security Standard v3.1

Goals	Req #	Requirements
Maintain a Vulnerability Management Program	**5**	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications

PCI Data Security Standard v3.1

Goals	Req #	Requirements
Implement Strong Access Control Measures	**7**	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data

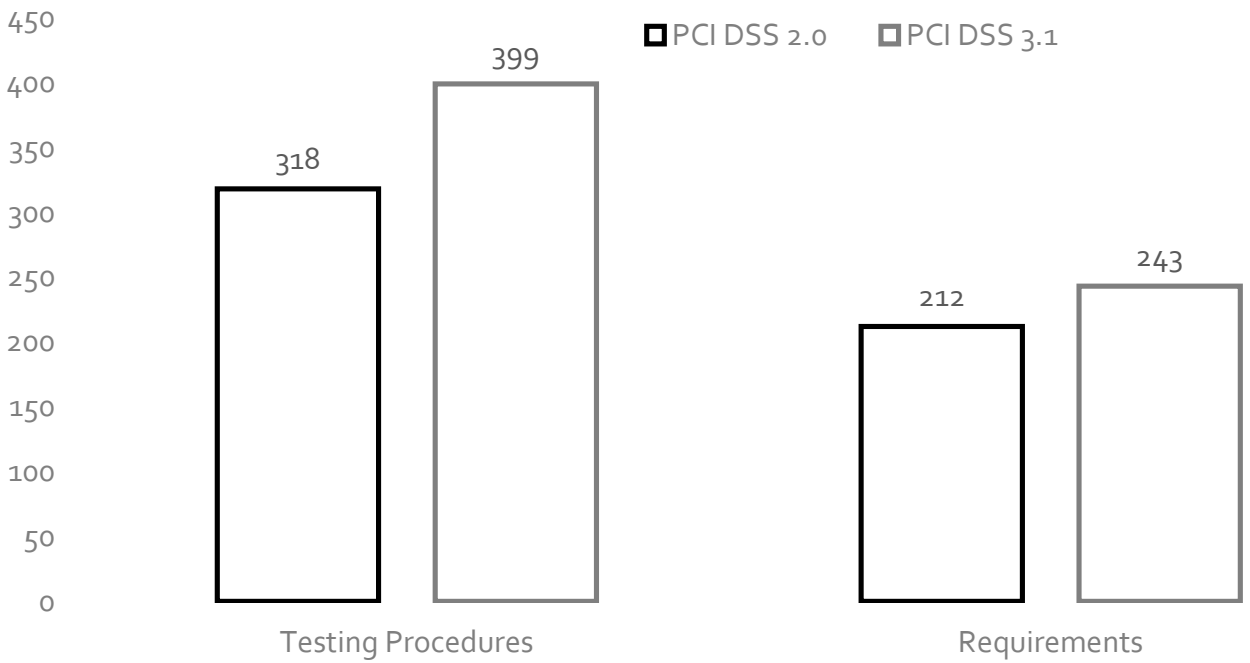
PCI Data Security Standard v3.1

Goals	Req #	Requirements
Regularly Monitor and Test Networks	**10**	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes

PCI Data Security Standard v3.1

Goals	Req #	Requirements
Maintain an Information Security Policy	**12**	Maintain a policy that addresses information security for all personnel

What has changed in PCI DSS v 3.1

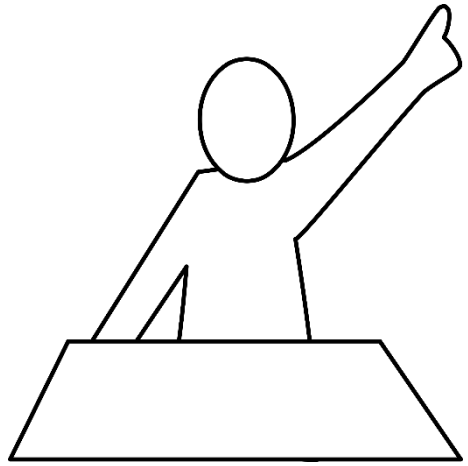


New Requirements and Clarifications

Benefits of compliance

- Improve security posture of the organization
- Protects cardholder/sensitive data
- Prevents (reduces) identity theft
- Reduces risk for the organization
- Now days it is used as sales pitch! for organizations,
- Improves reputation with payment brands.
- Indirect benefits, better prepared to comply with other regulations.

Questions?



sources

- PAYMENT CARD INDUSTRY SECURITY STANDARD COUNCIL
- PAYMENT CARD INDUSTRY DATA SECURITY STANDARD
- Visa Europe Processing e-commerce Payments Guide
- Discover - Discover Information Security & Compliance (DISC)
- MasterCard - Site Data Protection Program (SDP)
- Amex - Data Security Operating Policy
- JCB - JCB Data security Program (JDSP)
- Visa Canada - Account Information Security (AIS)