

PCI DSS: Payment Card Industry Data Security Standards

- **What is PCI DSS?**
 - Combination of Visa's Cardholder Information Security (CISP) / Account Information Security (AIS) Program and MasterCard's Site Data Protection (SDP) Program
 - Defines a common set of standards and measurements for the safe handling and protection of sensitive cardholder information
 - Focuses on prevention, detection and reaction to security incidents
 - Technical Specifications: Detailed requirements for the transmission, processing and storage of cardholder data
 - Known as the "Digital Dozen"
 - Testing Methodologies: Detailed auditing and network scanning procedures
 - Represents an ANNUAL program where ALL stakeholders must comply
 - All merchants fall into scope – differing processes through which compliance must be demonstrated

PCI Data Security Standard

- PCI = harmonization of Card Association programs
- Global Data Security standard for:
 - Visa
 - MasterCard
 - American Express
 - Discover
 - JCB
- 12 major requirements, 221 sub-requirements

PCI Data Security Standard

- Applies to all entities that “transmit, process, or store cardholder data”
- Not just e-commerce or even brick-and-mortar, but...
 - Healthcare
 - Higher Education
 - Utilities
 - State and Local Government
 - Insurance
 - Banking

PCI Data Security Standard: “Digital Dozen”

*

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
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.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors.

PCI DSS: Understanding The Fundamental Elements

Merchant Level	Compliance Criteria	Required Validation Action
Level 1	Any Merchant processing over 6 million transactions per year or compromised in the past year. Regardless of acceptance channel	Completion of an annual on-site assessment conducted by a certified QSA. Quarterly IP address scans conducted through a certified scanning tool.
Level 2	Any merchant processing 1 million to 6 million transactions per year. Regardless of acceptance channel.	Completion of an annual self-assessment questionnaire. Quarterly IP address scans conducted through a certified scanning tool.
Level 3	Any merchant processing 20,000 to 1 million e-commerce Transactions per year.	Completion of an annual self-assessment questionnaire. Quarterly IP address scans conducted through a certified scanning tool.
Level 4	Any merchant processing less than 20,000 e-commerce transactions per year, and all other merchants processing up to 1 million transactions/ year.	Completion of an annual self-assessment questionnaire. Quarterly IP address scans conducted through a certified scanning tool MAY be required by payment processing organization.

Clear Direction from Visa, MasterCard, etc. Has Been a Challenge!!



What is the Pain?

*

Retailers have been slow to adopt PCI... Only about 40% of the largest retailers in the US have achieved compliance.

PCI Project Management is complex... Due to the comprehensive technical and business requirements.

Retailers should prioritize their PCI efforts... Focus on risk reduction and reducing the most risk at the least cost.

NRF's Criticisms of Current PCI Guidelines

- All or nothing approach... no “Degrees of Compliance”
- Poor communication of PCI compliance status
- Not enough resources to review Reports of Compliance
- Banks and Card Processors have no infrastructure or experience in performing the volume of audits
- No clear guidance on “Compensating Controls”