



VICTOR D.
SCHINNERER
& COMPANY, INC.

Payment Card Industry Data Security Standards

Jason Bucher, Senior Underwriting Manager



An Introduction to PCI DSS Compliance

- Why are we talking about this?
- What is PCI?
- What is PCI DSS?
- What does PCI DSS compliance entail?
- PCI and cyber insurance impact
- Questions

Why Are We Talking About This?

- Every business that signs Merchant Agreement to accept payment cards is impacted
- Includes specific indemnification and performance requirements agreed to by both parties
- Security policies and procedures are key component
- PCI DSS compliance requirements apply to *ANY* organization that accepts, transmits or stores cardholder data



What is PCI?

- PCI = Payment Card Industry
- Founded in September 2006
- This council was designed to create a set of security and procedure requirements to reduce credit card fraud and losses
- NOT a government regulation or governmental regulatory body



What is PCI DSS?

- PCI DSS = Payment Card Industry Data Security Standard
- Comprehensive set of network requirements, security software components, access control, ongoing administration and procedural protocols
- PCI DSS 3.2 released April 2016



Common Misconceptions



Chip and Pin



Point of Sale (POS) vendor

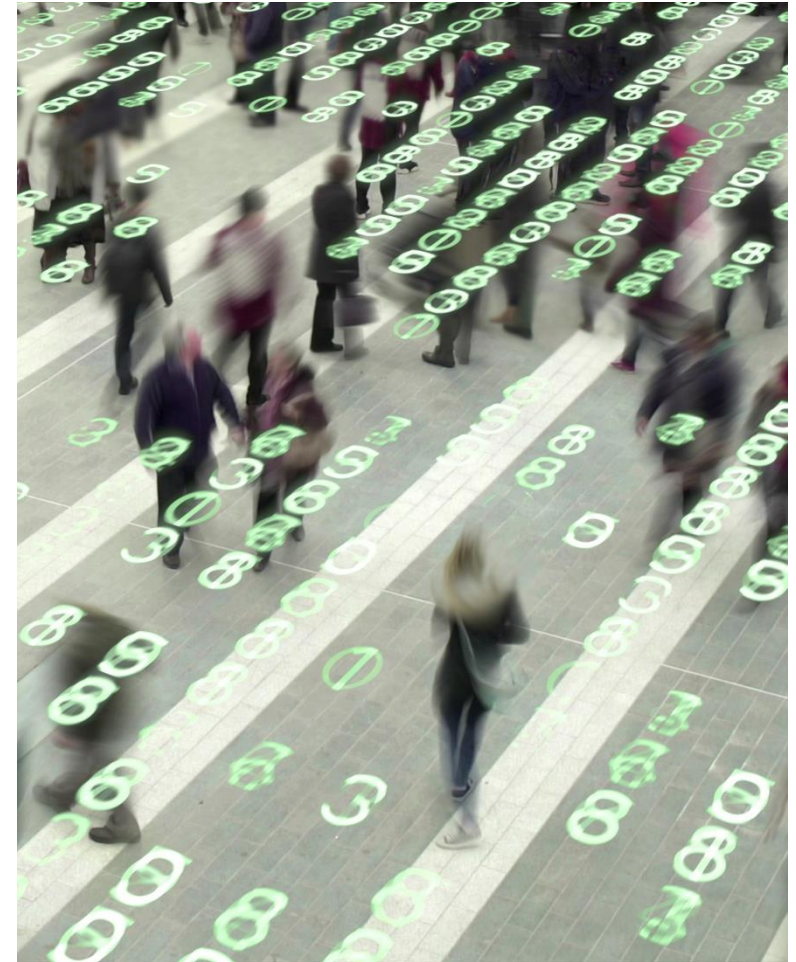
What Does PCI DSS Compliance Entail?

1. Determine Merchant level
 - Levels 1-4 depend on number of transactions processed per year
2. Determine which Self Assessment Questionnaire must be used to validate compliance
 - Online business?
 - POS terminal?
 - Virtual terminal card reader?
3. Complete Self Assessment Questionnaire
 - Reference: Self-Assessment Questionnaire C (used for a Level 4 merchant using POS terminal)
https://www.pcisecuritystandards.org/documents/SAQ_C_v3.pdf
4. Complete and obtain evidence of a passing vulnerability scan
5. Complete the Attestation of Compliance and submit to acquiring bank



PCI and Cyber Insurance

- PCI Compliance is a contractual agreement agreed to by the Insured
 - Breach of Contract Exclusion must be addressed in order to deliver PCI coverage
- PCI fines/assessments
- Schinnerer does not require PCI compliance affirmation for coverage
- 82% non-compliance with PCI DSS
- PCI compliance exclusion



Available Resources

- www.pcicomplianceguide.org
- www.pcisecuritystandards.org
- Data Response Team
- Your Schinnerer Cyber underwriters



Jason Bucher



Mark Schulz



Denise Mahoney

Contact Us



Jason Bucher

Senior Underwriter

Phone: (913) 685-6166

jason.bucher@schinnerer.com



Matt Kletzli

Management Liability Leader

Phone: (301) 961-9820

Matthew.Kletzli@Schinnerer.com



VICTOR O.
SCHINNERER
& COMPANY, INC.