Victor O. Schinnerer & Company, Inc.

PCI Fines and Assessments
A Little Insight to the Process

Jason Bucher, Senior Underwriting Manager

An Introduction to PCI Fines and Assessments

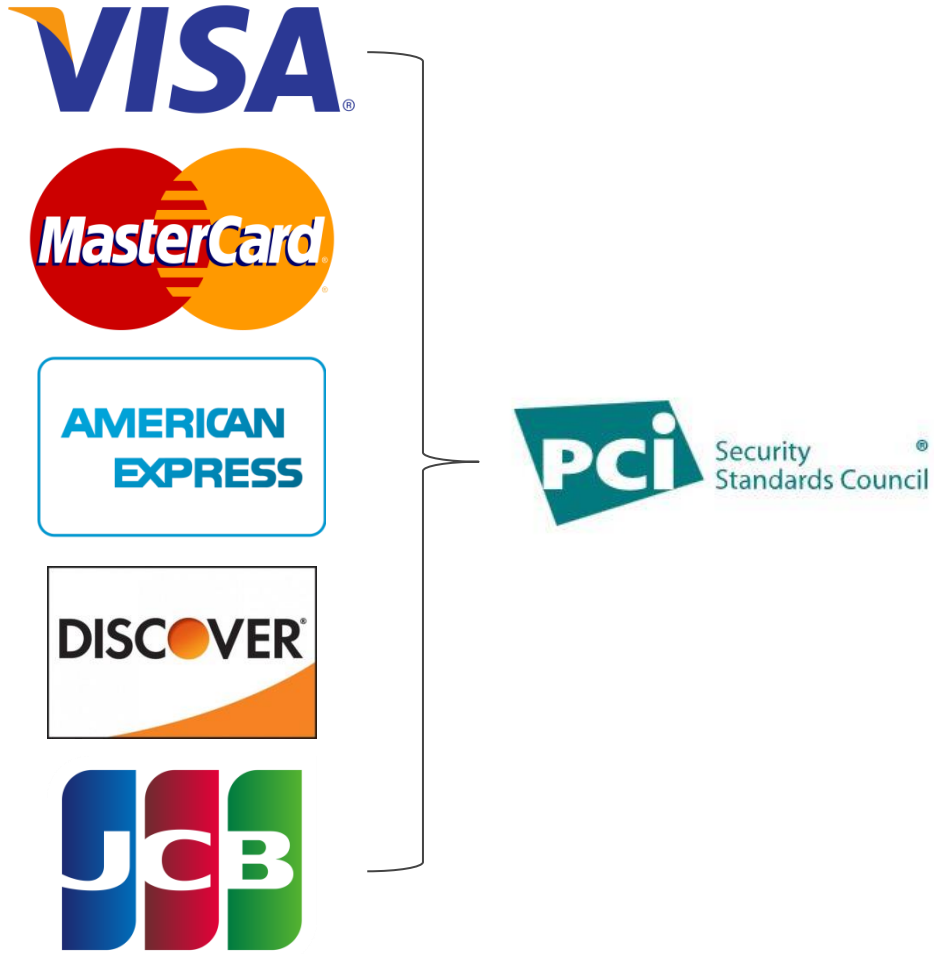
- Why are we talking about this?
- What are PCI Fines and Assessments?
- What is a Common Point of Purchase?
- Where does Cyber Insurance Come Into Play?
- Additional Cyber Insurance Considerations
- Questions

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
- PCI Fines are the stick used to motivate for PCI DSS compliance
- PCI monetary assessments are the primary source to recoup losses sustained by card issuing banks from stolen card data

PCI Fines and Assessments

- Fines and Assessments are two wholly different items
- PCI Fines
  - Fines are brought against the merchant by the credit card brands for non-compliance with PCI DSS
  - Fines generally continue until the merchant is able to confirm compliance
- Monetary impact – generally not significant for merchants, but can be up to $10,000 for first time offense



PCI DSS Assessments

- A PCI Assessment is an audit for validating compliance with PCI DSS
- Post Breach/Compromise, finding non compliance with PCI DSS, the assessment process will calculate the costs attributed to the fraud losses and expenses arising from the stolen card data
  - Counterfeit purchases made using stolen data
  - Costs to reissue cards by impacted issuing banks
  - Costs to investigate misuse of card data
- Monetary impact – can be significant
- Monetary process – amount is generally pulled direct from merchant account

The Common Point of Purchase

- For many small businesses, this is the “discovery” of a data breach
- Issuing banks will report fraudulent purchases to the card brands (Visa, MasterCard, etc.)
- Forensic investigation will search for commonalities
- Investigation may hit upon a “Common Point of Purchase”
- This Common Point of Purchase is where the compromised cards intersect and may indicate source of a data breach or compromise.

Common Point of Purchase Investigation

- Merchant been identified as a Common Point of Purchase will receive notification
- Per terms of the Merchant Agreement, a Qualified Security Assessor (QSA) may arrive shortly to execute a forensic investigation
- The QSA is simply seeking to identify:
  - was card data compromised
  - number of cards compromised
  - PCI DSS compliance of the merchant
  - Occurrence of Fraud on compromised cards
- The QSA investigator is *not* looking to identify source/cause of the breach
- Fines and Monetary assessments/penalties may follow the QSA investigation

PCI Security Standards Council™

QUALIFIED SECURITY ASSESSOR

PCI Fines and Assessments – Cyber Insurance

- Cyber coverage must be specifically granted
  - PCI Fines and Assessments are driven by Merchant Agreement contract
- Forensic Expense
  - QSA: will confirm that a breach/ compromise of cards collected by merchant has occurred
- Costs for Legal Review
  - Service Provider hired to analyze indemnification rights noted in insured's contract
  - Following forensic investigation, it may be discovered that the compromise occurred down stream

PCI Fines and Assessments – Additional Considerations

- Forensic Investigation for the Merchant – QSA is *not* on their side
- Monetary Assessments don't begin until 15,000 cards have been compromised
- Monetary Assessments can be negotiated
- Not covered by insurance
  - Fines for continued non-compliance
  - Costs to improve/amend in order to comply with PCI DSS
  - Inability to accept payment cards due to continued non-compliance

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.