The Dark Side of a Payment Card Breach
Road Map

• Introduction
• The Rules of the Game
• Pitfalls & Strategies
• Takeaways
• Q&A
The Rules of the Game
What is the Game?

- Payment Card Industry Data Security Standard
- Data security breach of merchant involving “cardholder data”
- PCI Forensic investigator and report
- Fines, penalties and assessments determine by the card brands based on card brand rules
- Collection from the merchant by payment processors or merchant banks
What is the Exposure?

• **Fines and penalties**
  • For non-compliance with Card Brand Rules
  • $2,000 - $500,000 depending on violation

• **Assessments**
  • Operating expense recovery – card reissuance (set amount per card)
  • Fraud recovery – amount of fraud perpetrated on breached cards (depends on actual activity – can be in the millions)
Who are the Players?

• The Standards Setter – PCI Council
• The Rule Makers – Card Brands
• The Enforcers – Merchant Banks and Processors
• The Harmed Parties – Issuing Banks
• The Investigators – PCI Forensic Investigators
• The Liable Parties – Acquiring Banks / Merchants
The Rules of the Game

- PCI-DSS
- AMEX DSOP
- Visa GCAR
- MasterCard ADC
- Discover DISC
The PCI Contract Chain

- Card Brand Rules
- Membership Agreement
- Merchant Agreement

- Card Brands
- Merchant Banks
- Merchants
Key Merchant Agreement Terms

- PCI Compliance
- Compliance with card brand rules
- Reimbursement and indemnification
- Processor’s right to establish a “reserve fund”
- Right to terminate (with or without cause)
- Payment card “black list” (if merchant fails to pay assessment)
VISA GCAR Qualification

- “Account Data” and “Card Verification Value (CVV) Magnetic-Stripe Data”
- Violation of PCI-DSS “that could have allowed a compromise”
- At least 15,000 compromised cards “potentially at risk”
- A combined total of US $150,000 or more Counterfeit Fraud Recovery and Operating Expense Recovery for all Issuers involved in the event.
Pitfalls & Strategies
What Happens?

- Merchant receives notice from processor of potential breach (usually based on “Common Point of Purchase”) methodology
- Card brands/merchant bank requires PCI Forensic Investigator
- Lawyers
- PFI Investigation (scope and PCI-DSS)
- PFI Report
Significance of PFI Investigation

• PFI report is the key input into card brands’ assessment processes and calculations
• Gray areas often exist
• Key data can be lost (unplugging the machine / anti-virus)
• Determine PCI-DSS compliance
Significance of PFI Investigation

• Determine scope of incident and number of cards “potentially at risk” (“window of intrusion”)

• Limited depth of analysis

• Potential conflict of interest
PFI Investigation – Window of Intrusion

• Smaller window = less than 15,000 cards or less compromised cards
• Access v. acquisition
• Conclusive v. inconclusive findings
• What systems and data were actually affected?
PFI Investigation – Timing Issues

• Fraud may be ongoing
• Fraud counted 12 months back and 1 month forward (from “CAMS alert”)
• Delays in issuing a PFI report can result in higher fraud assessment
• May also be helpful if more fraud was perpetrated near the 12 month look back
The Right Entity?

• Lumping related but separate merchants (separate merchant ID) together for purpose of card or fraud count minimums
  - One merchant with 20,000 compromised cards -or- 5 merchants with 4,000 cards?

• Catastrophic Cap Calculations
  - 2-5% of annual Visa sales (parent and subsidiaries)
  - Look at the corporate structure and merchant / merchant bank relationships
Additional Strategic Considerations

• Financial stress / bankruptcy
• Fighting attitude / cost-benefit
• Look for mistakes
• Appeal rights
• Threat of litigation
Takeaways
Security & Forensics

• **Be Compliant.**

• **Before the breach ask yourself:**
  
  o Where does Cardholder Data exist in or pass through our environment?
  
  o How long do we hold Cardholder Data for and is it encrypted?
  
  o Do we keep log files for our firewalls and domain controllers for at least 90 days?

• **Contain the breach**

• **Review and challenge forensic findings BEFORE finalization/issuance of PFI report**
Legal

• Legal and independent forensic involvement ASAP (not after the PFI report has been issued)

• Understand potential conflicts of interest (PFI, Processor) and consider an independent forensic investigator

• Know the rules of the game (esp. ADCR/ADC)

• Work to get the best PFI report possible

• Get copies of qualification summaries and look for mistakes
The Dark Side of a Payment Card Breach
Thanks!

David Navetta, Esq., CIPP
InfoLawGroup LLP
303.325.3528
dnavetta@infolawgroup.com
www.infolawgroup.com

Serge Jorgensen
Sylint Group
941.951.6015
sjorgensen@usinfosec.com
www.usinfosec.com