WHAT HAPPENS IF *"IT NEVER HAPPENS TO ME"* HAPPENS?

Effective Responses to a Data Breach

Presenters

- Steve Cannon Chairman and Managing Partner, Constantine Cannon LLP
- Prior to joining Constantine Cannon, General Counsel and Senior Vice President at Circuit City
- Former Deputy Attorney General for the Antitrust Division of the Dept. of Justice

- Mark G. Haley, CHTP Partner, The Prism Partnership, LLC
- Founding partner of hospitality technology & marketing consulting firm based in Boston
- Prior to establishing consulting practice in 1997, Director of Property Technology for ITT Sheraton Corporation
- Author of The PCI Compliance Planning Process for Lodging Establishments

HospitalityLawyer.com

What If "It Never Happens...."

- It Can Happen to You!
- The Response Continuum
- What Happens Next

It Can Happen To You!

- CardSystems PCI Breach – 2005
  - At the time, alleged to be the largest security breach in history
  - Press reports claimed the breach exposed 40 million accounts
  - Visa notified CardSystems that processing contract would be terminated in 90 days
  - Federal Trade Commission investigation ensued
  - CardSystems was eventually sold to Pay By Touch

It Can Happen To You!

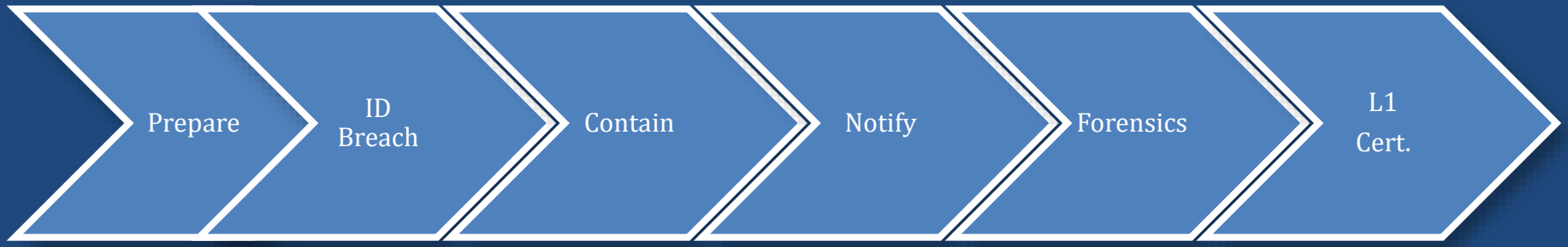
- TJX PCI Breach – 2007
  - Parent company to retailers like TJ Maxx and Marshalls
  - Potential exposure of 94 million credit and debit card numbers
  - Total breach costs may have exceeded $150 million, including a $41 million class action settlement to issuing banks
  - One analyst estimated that the total costs to TJX may have totaled $1 billion

It Can Happen To You!

- Hannaford Brothers PCI Breach – 2008
  - Supermarket chain in New England and Florida
  - 4.2 million credit card accounts exposed
  - Hannaford was certified as PCI compliant at the same time the breach was underway
  - Multiple class action lawsuits followed

The Response Continuum

- Prepare for as part of Compliance effort
- Identification of a Breach
- Containment
- Notification Requirements
- Forensic Investigation & Remediation
- Certify/Re-certify as a Level 1 Merchant



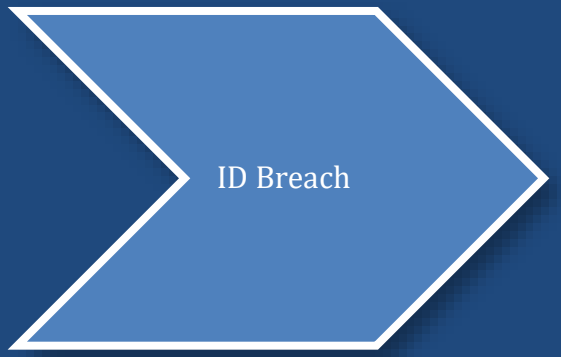
HospitalityLawyer.com

Preparation

- Prepare for a breach
- Part of Compliance Planning
- ID a Breach Response Team
- Communications Plan
- Vendor Relations
  - QIRA
  - Mailing House
  - Communications/PR

Identification of a Breach

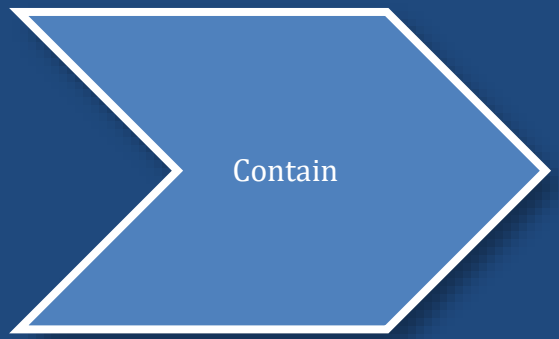
- Identification often a challenge
- Most likely identification will come from issuer or acquirer
  - Based on reported frauds linked by your merchant number
- Other means:
  - Monitoring of network traffic
  - Presence of unexplained archive or zip files
  - Review of system event logs



Containment

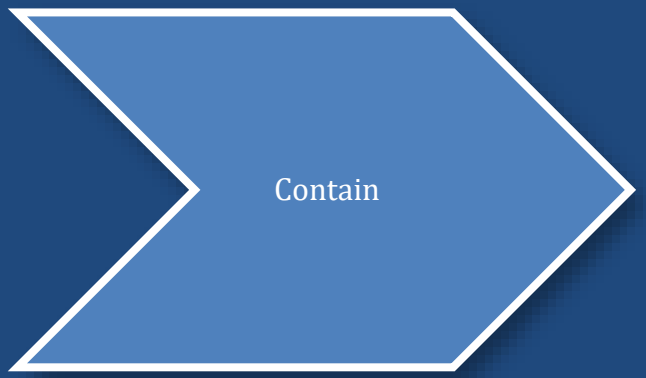
- Objectives of Containment
  - Prevent further exposure of cardholder data
  - Preserve evidence of breach for forensics

- Disconnect compromised system from network
  - Unplug cables
  - Take Core Dump
  - Do NOT turn off
  - Do not log into system
  - If wireless in use, change SSID at AP
    - Do not change at device



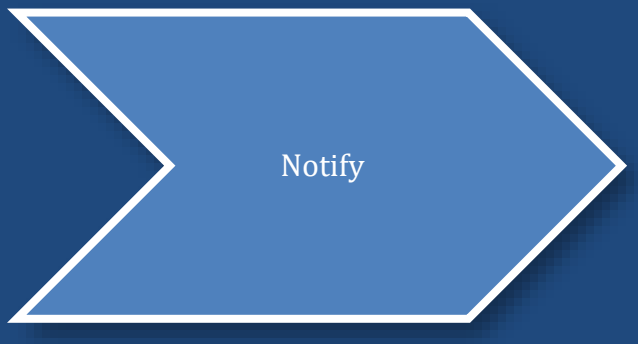
Containment

- Preserve all server logs
- Record all actions taken
- Escalate alertness levels
  - Monitor network traffic particularly closely
  - Monitor all other systems with cardholder data closely



Notification Requirements

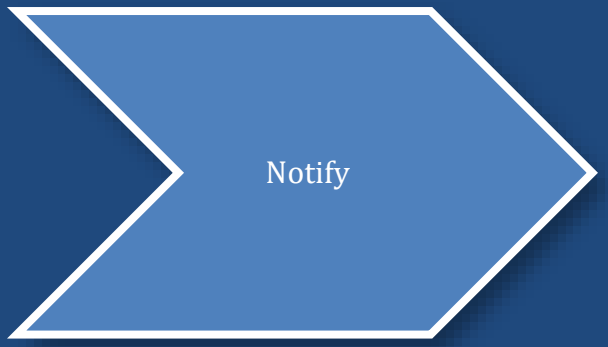
- Who do you need to notify?
  - Internal Breach Response Team
  - Acquiring Bank
  - US Secret Service
  - Other law enforcement agencies as required



- Expect Acquirer to escalate to Brands
  - They will demand engagement of QIRA

Notification Requirements

- Public and Consumer Notice
  - Follow lead of law enforcement/brands
- Communications Strategies
  - Fact-based, open communications
  - Acknowledge potential for change
  - Minimize importance of story to media
  - Apologize



Forensics

- Role of QIRA
  - Qualified Incident Response Assessor
  - Nature, Scope & Scale of breach
  - Reporting
    - Compromised Account Management System (CAMS)
- Remediate deficiencies

L1 Certification

- Certify/Re-certify as a Level 1 Merchant
- Must use QSA
- Most stringent level of compliance validation

Forensics

What Happens Next?

- Potential liability
  - PCI Compliance Certification ≠ Free Pass
  - Federal Trade Commission and State Attorney Generals
  - Private Suits
  - Processors
  - Card Issuing Banks