



Data Security Webinar

“What to do if Compromised”

Tom Pageler

Enterprise Risk and Compliance

November 21, 2006

Enterprise Risk and Compliance Data Security Webinars Overview



- Encourage greater adoption of and adherence to Payment Card Industry Data Security Standards (“PCI DSS”)
- Promote security awareness
- Use frontline information
- Create clarity around PCI rules, roles and responsibilities

Agenda



- Top five data security vulnerabilities observed in merchant compromises – focus on proper network segmentation
- An overview of the Visa document entitled “What to do if compromised”
- Questions?



Top 5 Security Vulnerabilities

Hap Huynh

**Cardholder Information
Security Program**

November 21, 2006



Hackers are attacking:

- Brick-and-mortar merchants
- E-commerce merchants
- Processors and Agents

Hackers are looking for:

- Software that stores sensitive cardholder data
- Personal information to perpetrate identity theft
- Track data and payment account numbers

Top 5 PCI DSS Violations



- Inappropriate data storage (e.g. full track, CVV2, PIN blocks)
- Un-patched systems
- Vendor default settings and passwords (e.g. unsecured wireless)
- Poorly coded web-facing applications resulting in SQL injection
- Unnecessary and vulnerable services on servers

Source:

Network Segmentation



- No firewall to protect the POS system
 - If installed, default configuration is used; no firewall rules are implemented
- Wireless network is connected to wired network



Network Segmentation — Risk Mitigation Recommendations



- Use a firewall to isolate all business systems
- Configure firewall to only allow access between transaction flow systems
- Limit access to network ports necessary to perform desired business functions
- Apply access controls to inbound and outbound network traffic
- Enable logging and exception alerting on all network devices and business systems
- Use an encrypted connection when processing sensitive data (e.g., VPN, SSL, or IPSEC)
- Implement a switched network; more resistant to eavesdropping

What To Do If Compromised

Ingrid Beierly

Investigations and Fraud
Management

November 21, 2006

Introduction



Objective

- Why are we here?
- Roles and responsibilities

Types of compromise

- Lost or stolen receipts
- Lost or stolen equipment
- Network intrusion

Incident Notification Sources



- Acquirer
- Merchant
- Media
- Third-party
- Issuer reports a suspected common-point-of-purchase (CPP)
- Visa identifies a point-of-compromise (POC)

CPP Reports



- Visa validates CPP reported by an issuer
 - At a minimum, 10 accounts must be provided
 - Issuer performs due diligence
 - Visa analysis
 - Multiple issuer reports
 - All of the above are performed to provide compelling evidence to acquirers

Compromise Procedure

Requirements for Compromised Entities



- Immediately contain and limit the exposure
- To preserve evidence and facilitate the investigation:
 - Do not access or alter the compromised system
 - Isolate the system by unplugging from the network
 - Log all actions taken
 - Monitor the network and systems with cardholder data
- Alert your internal Information Security group and Incident Response Team
- Contact your merchant bank and provide documentation (sequence of events)
- If merchant bank unknown, contact Visa at (650) 432-2978
- Contact your local office of the United States Secret Service

Compromise Procedure Requirements for Members



- Member must report compromise to Visa at USFraudControl@visa.com, or by phone (650) 432-2978, within 24 hours
- Upon notification provide an incident report and initiate a preliminary investigation and provide documentation to Visa within 3 business days
- Include PCI DSS status
- Member to provide “What To Do If Compromised” document to its merchants www.visa.com/cisp
- Upload cardholder data to CAMS
- At-risk account numbers to be provided within 10 business days
- Visa may request an independent forensic investigation and members are responsible for cost

Compromise Procedure

Requirements for Members (continued)



Forensic investigation

- Provide preliminary report to Visa within 5 business days from the onsite review
- A final report must be provided to Visa within 10 business days from the onsite review containing:
 - Findings
 - Remediation items
 - Corrected items
- Members must ensure entity has contained the incident

Compromise Procedure

Requirements for Members (continued)



- **Regulatory Compliance**

- Members should notify their banking regulators of a high-profile compromise
- Visa will send a notice to the acquirer and the Federal Financial Institutions Examination Council (“FFIEC”) within 48 hours after a CAMS alerts involving 200k accounts

Additional Information



- A “What to Do If Compromised” guide is available to Members through VOL
 - usfraudcontrol@visa.com
 - 650-432-2978 (Fraud Hotline)
- For questions about data security requirements
 - cisp@visa.com
- For additional Information about CISP
 - <http://www.visa.com/cisp>
(Cardholder Information Security website)

Fraud Analysis

Craig O'Connell

Risk Intelligence Operations

November 21, 2006

Agenda



- **Overview**
- **CPP Common Pitfalls and Observations**
- **Methods of Analysis**

- CPP analysis is performed to:
 - Identify unreported compromised entities
 - Confirm or counter suspicions of internal/external customers
- Validate emerging patterns:
 - Authorization anomalies
 - Confirmed fraud
 - Merchant test sites

CPP Common Pitfalls and Observations



- Data extraction criteria for analysis is crucial for accuracy
- Biased data pulls produce biased analysis results
- Common method observed was selecting all accounts resulting in fraud AND all accounts with a legitimate transaction at merchant X

Common Point of Purchase Discovery

- CPP entities are identified through account validation/merchant test sites, confirmed fraud, member reports
- Background information is researched prior to analysis (e.g., member footprint, geographic area, criteria for suspicion)
- Analysis performed
 - 2 years of authorization activity is pulled on the provided data
 - Entities are ordered by the number of unique accounts processed
 - Industry baselines for specific merchants are used to remove expected account/entity distribution
 - Fraud rates post-legitimate use are reviewed

Merchant Fraud Introduction Rate



- Measures the percentage of accounts with legitimate activity for a specific merchant resulting in a future fraudulent transaction at a different merchant
- Helps to identify, confirm or counter claims of a common point of purchase
- Highly condensed methodology:

accounts with first confirmed fraud AFTER the legitimate transaction

accounts used at the merchant for a given time window

Peer Comparison



- Used when system averages are insufficient
- Certain MCCs have a different risk associated with accounts and should be viewed against related merchants for accuracy
- Incorporates the methods discussed in Common Point of Purchase Discovery and Merchant Fraud Introduction Rate

Additional Information



- www.visa.com/cisp
- www.visa.com/merchant

Thank You and Questions

