MITIGATING LARGE MERCHANT DATA BREACHES

VISA

Tia D. Ilori
Ed Verdurmen

January 2014

DISCLAIMER

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

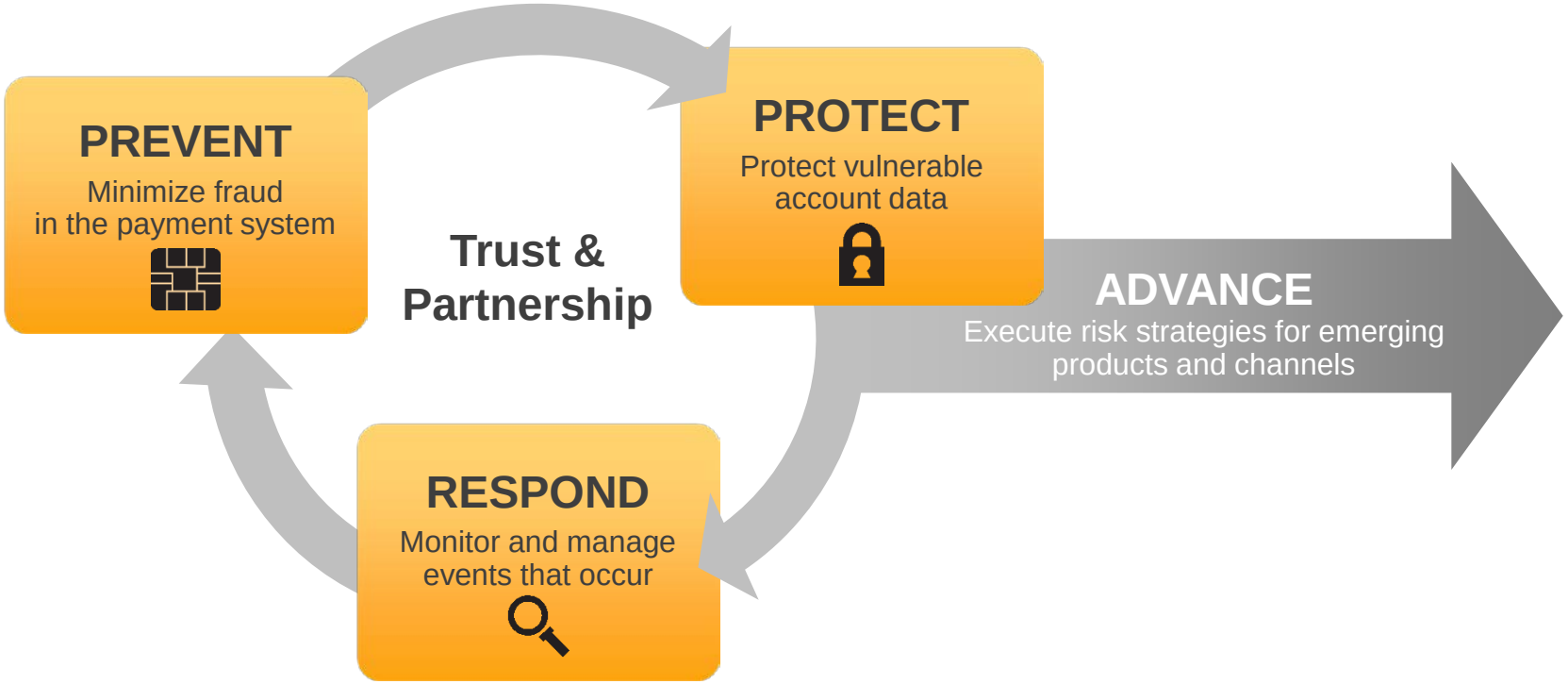
AGENDA

- Global Compromise and Threat Landscape
- Anatomy of a Breach
  - Top 3 Attack Vectors
  - Actionable Mitigation Strategies
- Leveraging Technology to Strengthen Security
- Incident Response and What To Do If Compromised
- Q&A

VISA'S MULTI-LAYERED STRATEGY

MITIGATING FRAUD THROUGH CONTINUOUS LEADERSHIP, COORDINATION AND INVESTMENT

- Maintaining and enhancing stakeholder trust in Visa as the most secure way to pay and be paid



ANATOMY OF A BREACH

Ed Verdurmen

CHARACTERISTICS OF ATTACKERS

Sophisticated attackers use **unsophisticated** methods to reach sensitive information

Source: Based on presentation by FusionXSource: "How Attackers Identify and Exploit Software and Network Vulnerabilities"

TOP THREE SECURITY VULNERABILITIES

Vulnerability	Examples
Insecure Domain Controllers	Use of weak password hash algorithm
	Unrestricted logon rights for privileged accounts stored in the local SAM
	Allowing Internet access
Zero-day Malware (RAM scraper, Key Logger)	RAM scraper is the #1 malware used by hackers to steal full track data in memory
	Citadel malware is used to steal VPN credentials and exploit the payment card environment
Inadequate Monitoring	Systems
	Application logs
	Access control lists (ACLs)

Source: Data Breach Forensic Reports

PCI DSS REQUIREMENTS
COMMON SECURITY DEFICIENCIES

	Vulnerability	Applicable Requirement
Network Security	Default or no firewall / router rules	Requirement 1
	No DMZ	Requirement 1
	Insecure remote access, no 2-factor authentication	Requirement 8
Host-based Security	Insecure operating systems and databases	Requirement 6
	No patching	Requirement 6
	No or outdated anti-virus signatures	Requirement 5
	No password management or access control lists (ACL)	Requirement 7
	Use of default or shared usernames and passwords	Requirement 2
	No system logging	Requirement 10
	No file integrity monitoring	Requirement 10, 11
Application Security	SQL injection / other web-based exploits	Requirement 6
	No secure coding, independent code review, or penetration testing process in place	Requirement 6
Incident Response	No incident response plan	Requirement 12
Monitoring	No monitoring of systems, logs, access control, etc.	Requirement 10

PROFILE OF LARGE U.S. MERCHANT BREACHES

BASED ON FORENSIC REPORTS FROM A SAMPLE OF 11 LARGE U.S. MERCHANTS THAT EXPERIENCED A DATA BREACH:

- 9 had privileged credentials compromised
- 9 had sysadmin ids exploited
- 8 had weak application security testing
- 8 did not have adequate monitoring
- 6 had malware installed on POS systems
- 6 had weak segmentation between corporate and cardholder data environment
- 5 had completed PCI DSS validation prior to the breach
- 2 had a weak audit function

EXAMPLES OF ISSUES LEADING TO COMPROMISE OF PRIVILEGED CREDENTIALS
Security staff using infected USB stick
Citadel Trojan
Root compromise through Vendor
Domain IDs had simple passwords with no expiration, no history and high number of lockout attempts
Contractor with infected machine
Default POS admin IDs and passwords
Open web server console
Weak domain password in development
Compromised PC belonging to administrator

PHISHING REMAINS SUCCESSFUL

PHISHING SUCCESS FACTORS

PREVENTING PHISHING

1. Establish internal phishing policy
2. Educate and train employees on phishing indicators
3. Identify a contact for employees to send suspected phishing
4. Test phishing policy on regular basis

Source: Based on presentation by FusionXSource: "How Attackers Identify and Exploit Software and Network Vulnerabilities"

POINT-OF-SALE SECURITY

- Companies use the term POS to describe both lab-tested PIN-Entry Devices (PED) and electronic cash registers (ECRs)
- When merchants deploy one or the other, it is often an ECR
- When merchants deploy encryption solutions, they must choose where to terminate the encryption service in the encrypted payment application on both the customer side and the acquiring bank or processor side
- Merchants should NOT terminate customer side encryption services at the ECR without clear, tested solutions for preventing and identifying memory scraping malware
- QSAs should NOT exempt ECRs from PCI DSS requirements

PIN-Entry Devices (PEDs)

Electronic Cash Registers (ECRs)

ACTIONABLE MITIGATION STRATEGIES

ATTACK PREVENTION: SECURITY STRATEGIES AND ACTIONABLE ITEMS

The following slides will cover strategies and actionable items for these security domains:

1. Network Security
2. Administrator Accounts
3. Point-Of-Sale Security
4. Secure Web-based Applications
5. Mitigating Third Party Risk

1) NETWORK SECURITY
ACTIONABLE ITEMS

- Secure domain controllers (DCs) and implement a process to have a repeatable and secure deployment of DCs
- Segregate the payment processing network from other non-payment processing networks
- Implement strict inbound and outbound filtering on the firewall rule sets (critical on outbound traffic)
- Apply access control lists (ACLs) on the router configuration to limit unauthorized traffic to payment processing networks
- Implement data leakage prevention/detection tools to detect and help prevent data exfiltration
- Perform penetration testing to identify security gaps
- Identify systems (such as jump servers) that have access to the payment card and ensure systems are secure
- Deny Remote Desktop Protocol (RDP) logons

Source: “POS Malware Technical Analysis: Indicators for Network Defenders” 1/16/14 – USSS/DHS/NCCIC/FS-ISAC/iSIGHT Partners

2) ADMINISTRATIVE ACCOUNTS
ACTIONABLE ITEMS

- Use two-factor authentication when accessing the payment processing networks
- Limit administrative privileges for users and applications
- Periodically review systems (local and domain controllers) for unknown and dormant users
- Apply same security on database users
- Do not use weak encryption algorithm for passwords

Source: “POS Malware Technical Analysis: Indicators for Network Defenders” 1/16/14 – USSS/DHS/NCCIC/FS-ISAC/iSIGHT Partners

3) POINT-OF-SALE (POS) SECURITY
ACTIONABLE ITEMS

- Implement point-to-point encryption (P2PE) PEDs
  - EMV capability
  - Secure Reading and Exchange of Data (SRED)
  - Hardware-based encryption
- Install PA-DSS compliant payment applications
- Deploy the latest version of operating systems and ensure it is up-to-date with security patches, anti-virus, file integrity monitoring and a host-based intrusion-detection system
- Perform a binary or checksum comparison
- Disable unnecessary ports and services, null sessions, default users and guests

Source: “POS Malware Technical Analysis: Indicators for Network Defenders” 1/16/14 – USSS/DHS/NCCIC/FS-ISAC/iSIGHT Partners

3) POINT-OF-SALE (POS) SECURITY
ACTIONABLE ITEMS [CONTINUED]

- Enable logging of events and make sure there is a process to monitor logs on a daily basis
- Implement least privileges and access controls lists (ACLs) for users and applications on the system
- Implement a security policy that includes operating system security configuration to include the following:
  - Security installation guide
  - Password management guide to manage users on the system
  - Mechanism to ensure consistent security baseline on critical systems
- Implement an enterprise-wide cardholder data scan to identify storage of clear-text data and perform a secure delete of any data identified

Source: "POS Malware Technical Analysis: Indicators for Network Defenders" 1/16/14 – USSS/DHS/NCCIC/FS-ISAC/iSIGHT Partners

4) SECURE WEB-BASED APPLICATIONS ACTIONABLE ITEMS

- Review the current Open Web Application Security Project (OWASP) Top 10 Security Risks and protect against them
- Perform detailed and manual web application penetration testing against applications in your environment
- Review all web-based management consoles and ensure it is configured in a secure manner
- Ensure all web servers are hardened and up-to-date with the latest security patches and hotfixes
- Implement a Web Application Firewall (WAF) to help mitigate web-based attacks
  - A combination of insecure code and dangerous stored procedures could execute statements at a higher level privilege

5) THIRD PARTY MANAGEMENT

Avoid these common mistakes:

- Unrestricted access – sometimes to production environment
- No establishment of vendor DMZ
- Poor auditing of vendor's security practices
- Permitting remote maintenance
- Limited knowledge of "partner" operations

Source: Based on presentation by FusionXSource: "How Attackers Identify and Exploit Software and Network Vulnerabilities"

LEVERAGING TECHNOLOGY TO STRENGTHEN SECURITY

- Tia D. Ilori

LEVERAGING TECHNOLOGY TO STRENGTHEN SECURITY

Advance cardholder data security and future proof your security investment through the use of robust technologies:

- **EMV Chip Technology**
  - Chip cards used at EMV terminals protects against counterfeit transactions by replacing static data with dynamic
- **Point-to-Point Encryption (P2PE)**
  - Protects cardholder data from the point of data entry to the payment card processor
  - Shields against malware that “sniffs” and “captures”
- **Tokenization Technology**
  - Replaces cardholder data with surrogate values, or “tokens”
  - Allows merchants to limit or eliminate the storage of cardholder data

If properly implemented, all three can reduce the scope of PCI DSS compliance.

Source: Visa Best Practices for P2PE and Tokenization – www.visa.com/cisp

INCIDENT RESPONSE AND WHAT TO DO IF COMPROMISED

INCIDENT RESPONSE PLANNING

- Deploy Security Information and Event Management (SIEM)
- Implement Indicators of Compromise (IOC) signatures on your solution
- Review logs and offload to a dedicated server (e.g., syslog and in a secure location where hackers can't tamper with logs)
- Staff with computer forensic, investigation or incident experience will improve the speed of your response to an incident and ensure the PCI Forensic Investigator (PFI) has access to critical logs and system images
- Define an executive response team that will start an investigation, and the associated containment, public relations and legally required reporting tasks
- Research and select a PFI before there is a breach, sign a contract and place them on retainer https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php
- Test your incident response plan

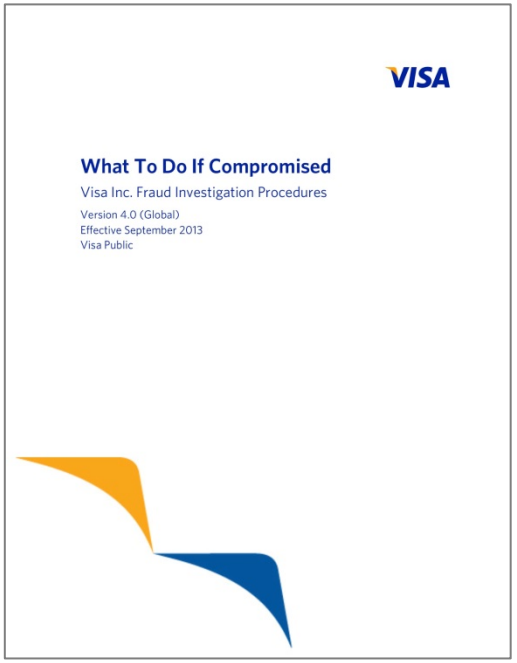
WHAT TO DO IF COMPROMISED

- Take compromised system off the network
- If you must rebuild system, take a forensic image prior to rebuild
- Review firewall configuration and disable any unnecessary inbound and outbound traffic
- Pair down ACLs, ports and services between PCI and non-PCI environment
- Create strict ACLs segmenting public facing systems and backend database systems that house payment data (e.g., DMZ)
- Change all passwords on the network including applications and local accounts
- Review all access to the payment processing environment and terminate connectivity

Source: “What To Do If Compromised” – www.visa.com/cisp

WHAT TO DO IF COMPROMISED [CONTINUED]

- Notify your acquiring bank
- Contact local law enforcement or the U.S. Secret Service
- For more information, please refer to the Visa publication *What To Do If Compromised*, available at www.visa.com/cisp under the "If Compromised" section
- Contact Visa Fraud Control and Investigations at usfraudcontrol@visa.com or (650) 432-2978, option 4



Source: "What To Do If Compromised" – www.visa.com/cisp

APPENDIX

RESOURCES

Visa's Data Security Program

- Data Security Alerts, Bulletins and Webinars
- Data Security Best Practices
- Data Security Press Releases and Third Party Media Articles
- Global Registry of Service Providers – PCI DSS Validated Entities
- Technology Innovation Program
- PIN Security and Key Management Program
- What To Do If Compromised manual
- Responding to a Data Breach guidelines
- Comments to cisp@visa.com
- www.visa.com/cisp

RESOURCES

PCI Security Standards Council

- PCI Data Security Standard (DSS)
- Payment Application Data Security Standard (PA-DSS)
- PCI PIN Transaction Security (PTS)
- PCI Point-to-Point Encryption (P2PE)
- PCI DSS Applicability in an EMV Environment
- PCI DSS Tokenization Guidelines
- Self-Assessment Questionnaires (SAQ A, B, C, VC-VT, D, P2PE-HW)
- Qualified Security Assessor (QSA) List
- Approved Scan Vendor (ASV) List
- PCI Forensic Investigator (PFI) List
- FAQ Database
- www.pcisecuritystandards.org

QUESTIONS?