



Top Five Data Security Trends Impacting Franchise Operators

Payment System Risk

September 29, 2009



Top Five Data Security Trends – Agenda



- Data Security Environment
- Compromise Overview and Attack Methods
- Top Five Data Security Trends
- Data Security Requirements and Prevention Methods
- Franchisee Training and Education
- What to Do if Compromised
- Questions



Data Security Environment

- Criminals continue to target merchants in the hospitality industry, specifically hotels and restaurants
- Franchise payment networks serve as the main vehicle for transmission of cardholder data between systems, commonly known to hackers
- Attack methods include intercepting cardholder data in transit through the use of packet sniffers, memory parsers and other malware
- Once intruders gain entry to steal cardholder data, identification of the incident is difficult to detect
- These threats underscore the urgency of maintaining compliance with **all** PCI DSS requirements

Common Compromise Vulnerabilities



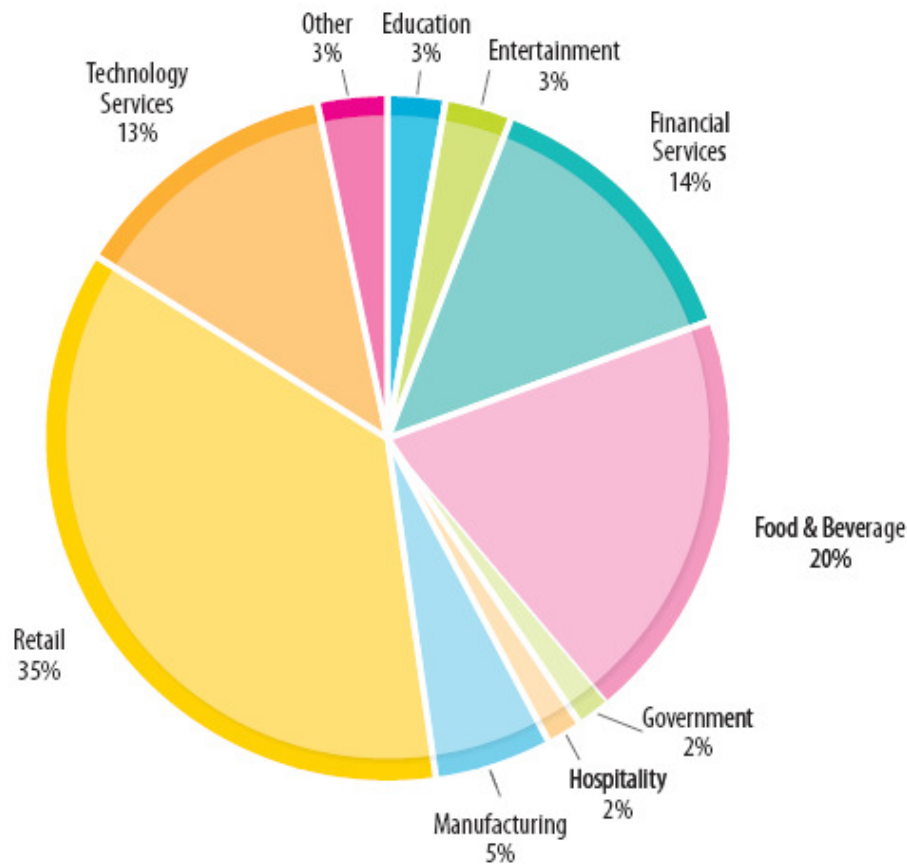
PCI DSS compliance should mitigate common vulnerabilities found to contribute to data breaches

PCI Data Security Standard	Common Compromise Vulnerabilities	
Build and Maintain a Secure Network	<ul style="list-style-type: none"> Failure to secure and monitor connected non-payment environment Improperly segmented networks Insufficient egress and ingress filtering and firewall monitoring Insecure database configuration Failure to update or change default passwords 	PREVENTION DETECTION
Protect Cardholder Data		
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> Unprotected systems vulnerable to SQL injection attacks Corporate websites targeted to gain access to network <ul style="list-style-type: none"> Malware installed to capture passwords and cardholder data 	
Implement Strong Access Control Measures	<ul style="list-style-type: none"> Failure to limit user access to critical system 	
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> No monitoring of privileged user access No implementation or monitoring of intrusion detection or anti-virus 	
Maintain an Information Security Policy		

Verizon Business 2008 Study



Industry Demographic → Risk vs. Reward . . . Cyber criminals are targeting Retail and Food & Beverage industries which are least resistant to compromise and account for more than half of all cases



- Financial Services, typically well protected in comparison to other industries, account for 14% of breaches
- Technology Services (i.e., software firms, data warehousing companies, telecommunication providers, etc.) account for 13% of breaches

Source: Verizon Business 2008 Data Breach Investigations Report

Compromise Overview and Attack Method



»» Forensic intelligence reveal weak security posture of compromised corporate franchisors' and franchisees' payment processing environment

- **Flat Networks**
 - No segmentation of network functionality
- **Default or Weak Passwords**
 - Commonly found on Point of Sale (“POS”) or other critical payment systems
 - Created or managed by POS Vendor/Resellers or Business Administrators
- **Remote Desktop Services**
 - Weak passwords allowing ‘administrative’ level access to systems
 - Left in an ‘always on’ capacity for convenience
- **No Monitoring of Network Traffic (Inbound and Outbound)**
 - Firewall rules outdated and unmonitored
- **Payment Processing Systems Being Used to Surf the Web**
 - Systems must be dedicated to only process payment transactions

Compromise Overview and Attack Method



(cont'd)

- **Brute Force on Weak Log-in Credentials**
 - Point of Sale (“POS”)
 - Remote Desktop Services
 - Local/Domain Administrative Accounts
- **Using Selected Internal Computers as Malware Repositories**
- **Sending Traffic in Some Cases over Legitimate Ports Using Traffic Converters**
- **Target and Infiltrate ‘Trusted’ Locations**
 - Infiltrate one network and freely move about an additional network
- **Malware**
 - Allows hacker to propagate using compromised administrative accounts, network shares, etc
- **Memory Parsing**



Compromise Overview and Attack Method

- **What is a memory parser?**
 - Most are legitimate tools used to assist administrators with debugging efforts
 - Work in conjunction with memory dumpers.
 - Parse (or search and extract) data matching a given set of parsing parameters
 - Some parsers can map system processes and include the ability to search for RSA keys and certificates in the different mappings of a process dump
- **Perpetrated by hackers**
 - Hackers are using the parser on Point of Sale (“POS”) systems running Windows
 - Extract full magnetic stripe data from POS data stored in temporary or volatile memory (“RAM”)
 - There is evidence to suggest that parsers are being “tailored” to parse memory of POS systems

Compromise Overview and Attack Method

Memory Parsing (Cont'd)

- **Capabilities**

- Use standard ports, such as File Transfer Protocol (“FTP”) to upload captured full magnetic stripe data to the hacker’s server; Other ports are being used
- Binary is executed remotely using Sysinternal’s PsExec software
- Instances observed where binary is obfuscated in order to circumvent anti-virus and intrusion detection system

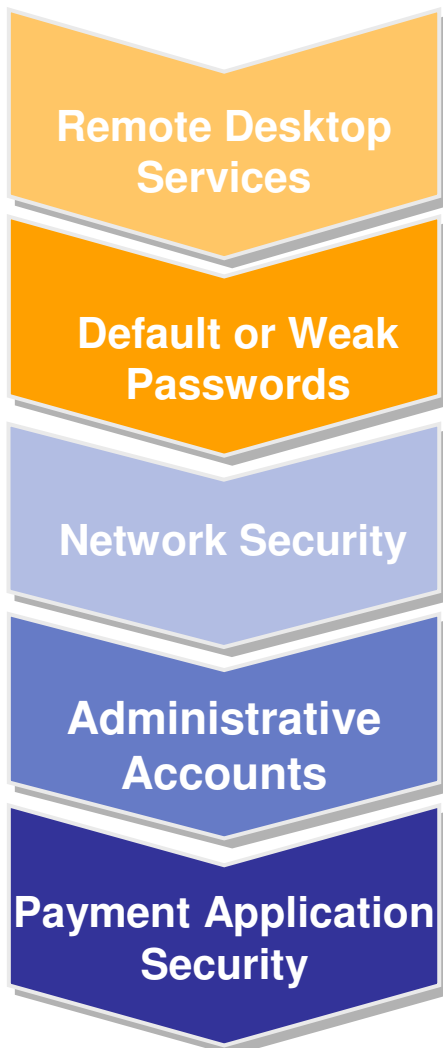
Franchise Payment System Security Practices



Franchise Data Security Action Plan

- Minimize risk to the payment system by eradicating storage of prohibited card data and promoting security education
- Serve as industry resource to franchise corporations for development of messaging to address PCI DSS within their franchise communities
- Require franchisors to secure corporate networks and franchisees to use compliant payment applications and eliminate use of vulnerable payment applications
- Partner with Visa's Cyber Security and Investigation team to identify emerging fraud trends and exploits and convey these threats to industry stakeholders
- Promote "Franchise Payment System Security Practices" through bulletins, webinars and PCI training opportunities

Top Five Data Security Trends Impacting Franchise Operators



- Many franchise businesses use remote desktop services to disseminate business downloads, conduct sales polls or service Point of Sale (POS) systems
- PCI DSS Requirement 8.3: Incorporate two-factor authentication for remote access

- Franchise businesses that use default settings to access payment networks are in **violation** of PCI DSS and are more susceptible to data compromise
- PCI DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Hackers have successfully gained unauthorized access to franchise cardholder data networks through commonly known network vulnerabilities
- PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data

- Secure all local and domain administrative accounts to help ensure unauthorized software cannot be installed on ANY systems
- PCI DSS Requirement 8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components

- Franchise businesses must ensure payment applications do not retain sensitive authorization data and are implemented properly
- PA-DSS was developed to aid vendors in development of secure payment applications that adhere to PCI DSS



Top Five Data Security Trends Impacting Franchise Operators

Remote Desktop Services :

- Update remote access products to latest version
- Change vendor supplied default settings
 - Off the shelf software such as remote management applications are packaged from vendors with original default (or blank) passwords
 - Hackers learn POS vendor support account credentials to gain access via remote desktop services to access payment infrastructures
 - Ensure accounts that have remote desktop (including terminal services) capabilities take advantage of complex and frequently changed passwords
 - Implement two-factor authentication
- Configure the remote management application to allow connections only from specific (known) IP / MAC addresses
- Franchises should turn on modem only when needed for downloads from the franchisor or vendor and turn off the modem immediately after downloads are complete
 - Third parties may argue against this practice, however this is your right as a customer and franchise owner

Top Five Data Security Trends Impacting Franchise Operators



Default and Weak Passwords :

- New hardware devices and software generally arrive from vendors configured with default settings for ease of installation and management
 - Default settings must be changed prior to deployment into the production environment
 - Use strong authentication or complex passwords for logins
- Examples of devices and software that use default settings include the following:
 - Routers, switches, servers, wireless access points, shopping carts, point of sale (“POS”) software, Web servers, and database software
- Many compromises have occurred when franchise businesses permit third parties (e.g., vendors) to access POS systems remotely
 - Hackers can subsequently access systems using default settings
 - Mandate vendors accessing your system remotely change default settings in remote access software

Top Five Data Security Trends Impacting Franchise Operators



Network Security :

- Franchises with IP based POS systems or broadband connection should install and maintain a stateful hardware firewall
 - Disabling a firewall may leave network prone to internet attacks, potential compromise and possible system failure
 - Proper firewall rules configuration and management of network devices is critical to preventing unauthorized access
- Enable firewall logging and maintain firewall logs for at least one year with 90 days available immediately for analysis
 - Audit trails (e.g., logging) assist with reconstructing system events and help to identify suspicious network activity
- Implement strong access controls
 - Identify data flows for cardholder information in and out of the network
 - Restrict inbound and outbound traffic on known ports to only that which is necessary for the cardholder data environment

Top Five Data Security Trends Impacting Franchise Operators

Administrative Accounts :

- Secure all local and domain administrative accounts to help ensure unauthorized software cannot be installed on ANY system
- Identify any systems that store, process or transmit account data
- Administrative credentials (system-local/domain and application) should be complex and frequently changed
- Implement 'least' privilege necessary for system and application accounts
- Conduct regular audits of application, domain and local system administrator accounts
- Check for 'backdoor' accounts (sometimes created by employee domain administrators)
 - 'Backdoors' may also be created by hackers for unauthorized access

Top Five Data Security Trends Impacting Franchise Operators



Payment Application Data Security Standard (PA-DSS) :

- Vet POS applications with both the PCI SSC's and Visa's list of validated payment applications
 - Lists available at www.pcisecuritystandards.org/security_standards/vpa and www.visa.com/cisp
- Confer with franchisor, payment application vendor (or reseller / integrator) to ensure software does not store prohibited data (e.g., magnetic-stripe, CVV2 or PIN data)
 - Require reseller/integrator follow vendor implementation guide that adheres to PCI DSS
- Partner with merchant bank to obtain a list of *vulnerable* payment applications
 - If payment application deficiencies are identified, franchise business should **immediately** upgrade to a compliant version
 - In addition to upgrading the application, any historical storage of prohibited data must be securely wiped from all systems immediately!

Additional Data Security Prevention Steps



Ensure the following solutions exist, are monitored and updated on a regular basis

- Implement two-factor authentication, for remote access
- Utilize host / application / network based Intrusion Detection Systems (“IDS”) and Intrusion Prevention Systems (“IPS”)
- Ensure antivirus, anti-spyware and anti-malware software are up-to-date
- Implement file integrity monitoring to detect and alert security personnel of unauthorized file changes
- Examine systems and networks for newly added hardware devices
- Periodically reboot POS systems to clear volatile memory
- Include in overall security configuration, patch and password management
- Perform application penetration tests for combating known vulnerabilities (including SQL injection, Cross-site scripting, etc.)

Franchisee Communication and Training



- Create or refine Standing Operating Procedures (SOPs)
 - Operational guide provides directives inherent to franchise businesses
 - Franchisors should amend these procedures to include cardholder data security practices using PCI DSS as a model
- Franchises businesses are strongly encourage to visit reputable security reference sites like www.visa.com/cisp
 - The Visa website has an array of practical security and compliance information
 - Includes data security alerts, webinar presentations and bulletins
- Consider attending data security training
 - PCI Security Standards Council (SSC) holds global two-day PCI Standards Training seminars
 - To preview the 2009 PCI SSC Standards Training Schedule visit: <https://www.pcisecuritystandards.org/education/training>

What To Do If Compromised



- If you detect a suspected or confirmed security breach, notify your merchant bank, franchisor and Visa **immediately**
- For more information, please refer to:
 - Visa’s *What To Do If Compromised*, available at www.visa.com/cisp under the “If Compromised” section
 - Visa’s *Responding to a Data Breach — Communications Guidelines for Merchants*, available at www.visa.com/cisp under the “Tools & FAQ” section
- You can also contact Visa Fraud Control and Investigations at usfraudcontrol@visa.com or (650) 432-2978



Reference Tools

PCI Security Standards Council (PCI SSC)

- Data Security Standard
- Security Audit Procedures
- PCI Data Security Standards
- PCI POS PIN-Entry Device Security Requirements
- PCI EPP PIN-Entry Device Security Requirements
- PCI Approved PIN Entry Devices List
- Payment Application Data Security Standards
- List of Validated Payment Applications
- Glossary of Terms

www.pcisecuritystandards.org

Visa CISP

- Archive of Data Security Alerts, Bulletins and Webinars
- What To Do If Compromised and Responding to a Data Breach guides
- Qualified Incident Response Assessor List
- Global List of Validated Service Providers
- PCI PIN Security Requirements
- PCI PIN Entry Device Testing and Approval Program Guide

www.visa.com/cisp

www.visa.com/pin



Questions?

