

**NFIB**

The Voice of Small Business.®

**VISA**



# Visa / NFIB Data Security Best Practices for Small Business

Payment System Security Compliance

July 30, 2008

# National Federation of Independent Business (“NFIB”)

**NFIB**  
The Voice of Small Business.®

- America's leading small business association
  - Mission is to promote and protect our members' right to own, operate and grow their business
- Benefits of NFIB membership
  - A voice in Washington, D.C. and all 50 state capitals
  - Discounts on valuable business products and services
  - Helpful legal resources (1-800 employment hotline)
  - Practical business information and toolkits
  - Print and e-mail publications plus networking opportunities
- Visit [NFIB.com](http://NFIB.com) to join and sign up for our FREE e-mail newsletters
  - Or, call 1-800-NFIB-NOW

# Agenda



- Security Environment
- Compromise Trends
- Payment Card Industry Data Security Standard (“PCI DSS”)
- Small Merchant Security Best Practices
- Questions?

# Security Environment



## Increasing industry, regulatory and legislative focus on security due to high profile data compromises

- Criminals are targeting full track data, Card Verification Value 2 (“CVV2”) and PINs in data compromises
- Merchant compliance with the PCI DSS is growing among large merchants
- Industry-wide coordination is increasing with the establishment of the PCI Security Standards Council (“SSC”)
- Legislators and regulators have become involved and there are a number of state laws pending
- Consumer confidence is impacted by data compromises

# Security Environment



- **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



# Card Compromise Trends



## Notable increase in cardholder compromises over past years

- Recent compromises are evenly split between card present (brick-and-mortar) and e-commerce
- Vast majority of compromised accounts consist of track data
- Large (Level 1) merchant and processor breaches account for majority of compromised accounts, **yet small (Level 4) merchants account for over 85% of compromise events**
- Restaurants, brick-and-mortar retailers and universities have been the most common targets

# Card Compromise Trends



- The growing threat of network packet sniffers and other malware are playing a significant role in recent compromises
- This further reinforces the criticality of the Top 5 most common vulnerabilities contributing to system breaches:
  1. Use of vulnerable payment applications
    - Prohibited data (e.g., full track, CVV2, PIN blocks) storage in logs and other system files
  2. Unpatched systems / lack of antivirus protection
  3. Unsecured remote access
    - Vendor or employee remote access
  4. Vendor default settings and passwords
    - Unsecured wireless settings
  5. Poorly coded web-facing applications resulting in SQL injection

# How Hackers Break In



## Identify and exploit technical vulnerabilities:

- Scan for vulnerabilities in the network, systems and payment applications and attack them
- Use hacker tools freely available on the Internet
- Trial and Error
  - Hackers have unlimited amounts of time and resources
- Publish and Share
  - Hackers often find issues and then publish their techniques on the Internet (chat rooms, foreign language hacker forums, etc.)

# Industry Collaboration



- PCI Security Standards Council (“SSC”), launched in September 2006, is a global forum for the ongoing development and enhancement of security standards for account data protection
- Security standards managed by the council include the PCI Data Security Standard (“DSS”), Payment Application Data Security Standard (“PA-DSS”) and PIN Entry Device (“PED”) program
- Visa, Amex, Discover, JCB and MasterCard are founding members
- Payment card industry stakeholders are invited to join as Participating Organizations and can be elected to an Advisory Board
  - Participating organizations are invited to attend community meetings, comment on DSS revisions and future security standards and participate in implementation "best practice" discussions



## PCI DSS is based on fundamental data security practices

<b>Build and Maintain a Secure Network</b>	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
<b>Protect Cardholder Data</b>	<ol style="list-style-type: none"><li>3. Protect stored data</li><li>4. Encrypt transmission of cardholder data and sensitive information across public networks</li></ol>
<b>Maintain a Vulnerability Management Program</b>	<ol style="list-style-type: none"><li>5. Use and regularly update anti-virus software</li><li>6. Develop and maintain secure systems and applications</li></ol>
<b>Implement Strong Access Control Measures</b>	<ol style="list-style-type: none"><li>7. Restrict access to data by business need-to-know</li><li>8. Assign a unique ID to each person with computer access</li><li>9. Restrict physical access to cardholder data</li></ol>
<b>Regularly Monitor and Test Networks</b>	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes</li></ol>
<b>Maintain an Information Security Policy</b>	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security</li></ol>

# Visa Merchant Compliance Validation



Level	Validation Action	Scope	Validated By
<b>1</b>	<ul style="list-style-type: none"> <li>Annual On-site Security Audit</li> </ul>	<ul style="list-style-type: none"> <li>Authorization and Settlement Systems</li> </ul>	<ul style="list-style-type: none"> <li>Qualified Security Assessor or Internal Audit if signed by Officer of the company</li> </ul>
	<ul style="list-style-type: none"> <li>Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>Internet Facing Perimeter Systems</li> </ul>	<ul style="list-style-type: none"> <li>Approved Scan Vendor</li> </ul>
<b>2 and 3</b>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> </ul>	<ul style="list-style-type: none"> <li>Any system storing, processing, or transmitting Visa cardholder data</li> </ul>	<ul style="list-style-type: none"> <li>Merchant</li> </ul>
	<ul style="list-style-type: none"> <li>Quarterly Network Scan</li> </ul>	<ul style="list-style-type: none"> <li>Internet Facing Perimeter Systems</li> </ul>	<ul style="list-style-type: none"> <li>Approved Scan Vendor</li> </ul>
<b>4</b>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire Recommended</li> </ul>	<ul style="list-style-type: none"> <li>Any system storing, processing, or transmitting Visa cardholder data</li> </ul>	<ul style="list-style-type: none"> <li>Merchant</li> </ul>
	<ul style="list-style-type: none"> <li>Network Scan Recommended</li> </ul>	<ul style="list-style-type: none"> <li>Internet Facing Perimeter Systems</li> </ul>	<ul style="list-style-type: none"> <li>Approved Scan Vendor</li> </ul>

# PCI DSS New Self-Assessment Questionnaires (“SAQ”)



- Released February 6, 2008
- New SAQ Documents
  - SAQ Instructions and Guidelines
    - Guidance on choosing the correct SAQ
  - Navigating PCI DSS – Understanding the Intent of the Requirements
- New SAQs
  - SAQ A - 11 Questions + Attestation
  - SAQ B - 21 Questions + Attestation
  - SAQ C - 38 Questions + Attestation
  - SAQ D - 226 Questions + Attestation
- Located at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

# PCI DSS New SAQ



SAQ Validation Type	Description	SAQ
1	Card-Not-Present (e-commerce or MO / TO) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand alone dial-out terminal merchants, no electronic cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A, B or C above) and <b>all</b> service providers defined by a payment brand as SAQ-eligible	D

# Level 4 Small Merchant Initiatives



## Executing a plan to address small merchants in the U.S.

- Level 4 merchants account for more than 85% of all compromises identified since 2005, but less than 5% of potentially exposed accounts
  - Most small merchant compromises involve vulnerable payment applications
- Outreach to all active acquirers to promote small merchant security
- Education and awareness campaign including a webinar series, regular data security alerts and bulletins
- Publish list of vulnerable payment applications quarterly and promote use of PA-DSS validated applications
- 100% of 231 acquirers provided Visa with Level 4 compliance plans
  - Updated progress reports due from acquirers by June 30, 2008

# Payment Application Security



## Drive the adoption of secure payment applications that do not store prohibited data

- Visa PABP published in 2005
  - Provide vendors guidance to develop products that facilitate PCI DSS compliance
  - Minimize compromises caused by insecure payment applications with emphasis on track data storage
- List of validated payment applications published monthly since January 2006
  - 348 products across 157 vendors independently validated by a Qualified Security Assessor
  - List of validated applications published on [www.visa.com/cisp](http://www.visa.com/cisp)
- List of vulnerable payment applications published quarterly since February 2007
- PABP adopted by PCI SSC as an industry standard, Payment Application Data Security Standard (“PA-DSS”) in April 2008



[www.visa.com/pabp](http://www.visa.com/pabp)

# Payment Application Mandates



Visa plans to aggressively drive the adoption of secure payment applications in the U.S. marketplace

Phase	Compliance Mandate	Effective Date
I.	Newly boarded merchants must not use known vulnerable payment application and VNP and agents must not certify known vulnerable payment applications	1/1/08
II.	VNP and agents must certify only PA-DSS compliant payment applications to their platforms	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or utilize PA-DSS compliant payment applications*	10/1/08
IV.	VNP and agents must decertify all known vulnerable payment applications**	10/1/09
V.	Acquirers must ensure their merchants, VNP and agents use PA-DSS compliant payment applications	7/1/10***

\* In-house use only developed applications and stand-alone POS terminals are not applicable

\*\* VisaNet Processors and agents must decertify vulnerable payment applications within 12 months of identification

\*\*\*Date is aligned with TDES mandate for all POS PEDs to support TDES and be Visa-Approved / Lab-Evaluated

# Level 4 Merchant Security Best Practices



## Understand PCI DSS Requirements:

- Use online resources
  - The PCI SSC website contains the standards and other supporting documentation (e.g. self-assessment questionnaires) – [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
  - The Visa website has an array of helpful security and compliance information – [www.visa.com/cisp](http://www.visa.com/cisp)
- Partner with your merchant bank
  - Utilize resources offered by your merchant bank such as alerts, bulletins and training
  - Understand the compliance validation required by your merchant bank

## Understand PCI PIN Security Requirements:

- The [www.visa.com/pin](http://www.visa.com/pin) website has an array of helpful PIN security and compliance information for Interlink accepting entities
- The PCI SSC website contains the Approved PIN Entry Devices list and other supporting documentation – [www.pcisecuritystandards.org/pin](http://www.pcisecuritystandards.org/pin)

# Level 4 Merchant Security Best Practices



## Adopt Payment Application Best Practices:

- Vet Point-Of-Sale (“POS”) applications with Visa’s list of validated payment applications
  - List available at [www.visa.com/pabp](http://www.visa.com/pabp)
- Confer with payment application vendors (or reseller / integrator) to ensure their software does not store prohibited data (e.g., magnetic-stripe, CVV2 or PIN data)
- Partner with merchant bank to obtain a list of *vulnerable* payment applications
  - If payment application deficiencies are identified, merchants should work with their acquirer to 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!

# Level 4 Merchant Security Best Practices



## Enforce Network Security Controls:

- Merchants 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
- Enable firewall logging and maintain firewall logs for at least 90 days (online)
  - Audit trails (e.g., logging) assist with reconstructing system events and help to identify suspicious network activity
- Implement strong access controls
  - Restrict inbound and outbound traffic on known ports to only that which is necessary for the cardholder data environment

# Level 4 Merchant Security Best Practices



## Secure Remote Management Applications:

- Change vendor supplied default settings
  - Off the shelf software such as remote management applications are packaged from vendors with original default (or blank) passwords
- Configure the remote management application to allow connections only from specific (known) IP / MAC addresses
- Merchants should consider activating the modem only when needed for downloads from the software vendor and deactivating the modem immediately after downloads are complete
  - If merchant business requires modem configuration in the “always-on” mode, the business should consult with the application vendor on secure configuration setting for “always-on” mode connections

# Call to Action



## **Cardholder data security is a shared responsibility and all participants must do their part to prevent fraud**

- Issuers must use available fraud prevention services and ensure their processors and agents are PCI DSS compliant
- Acquirers must ensure merchants and agents are PCI DSS compliant with key focus on prevention of track data storage
- Merchants must ensure they do not store track data, only store necessary cardholder data and confirm that they and their agents comply with PCI DSS
- Visa will execute presented strategy and work with members to ensure the safety and soundness of the payment system

# Upcoming Visa Trainings and Webinars



- PCI DSS Trainings – August 26 and 27
  - For more information regarding PCI DSS Training, email [cisp@visa.com](mailto:cisp@visa.com)
  
- PIN Security / Key Management Workshops – October 9
  - For more information regarding PIN Security and Key Management Workshops, email [pinusa@visa.com](mailto:pinusa@visa.com)

# Reference Tools



## PCI SSC

- PCI Data Security Standard
- PIN Entry Devices Program
- Payment Application Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaires
- Security Scanning Procedures
- Qualified Security Assessor List
- Approved Scan Vendor List
- Glossary of Terms

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

## Visa CISP

- Visa's Business Guide to Data Security
- Archive of Data Security Alerts, bulletins and webinars
- What To Do If Compromised guide
- Qualified CISP Incident Response Assessor List
- List of PCI DSS-Compliant Service Providers
- Payment Application Best Practices
- List of Validated Payment Applications
- PIN Security Best Practices

[www.visa.com/cisp](http://www.visa.com/cisp)

[www.visa.com/pin](http://www.visa.com/pin)

# Valuable Resources



- Visa CISP website at [www.visa.com/cisp](http://www.visa.com/cisp)
- Visa compliance inquiries emailed to [cisp@visa.com](mailto:cisp@visa.com)
- Visa Data Security Alerts, bulletins and webinars
- PCI DSS requirement questions can be submitted to the PCI Security Standards Council at [info@pcisecuritystandards.org](mailto:info@pcisecuritystandards.org)
- When in doubt, seek the assistance of a QSA company included in the PCI SSC's QSA list at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- POS application and other payment application questions can be directed to the application vendor / reseller

**NFIB**

The Voice of Small Business.®

**VISA**

[www.NFIB.com](http://www.NFIB.com)  
[www.visa.com](http://www.visa.com)