



# **PCI DSS: A Briefing for the Restaurant Industry**

**Diana Greenhaw  
Payment System Risk & Compliance  
Visa U.S.A.**

**July 20, 2007**

# 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 Payment Card Industry (PCI) Data Security Standard (DSS) is growing but less than optimal
- Industry-wide coordination is increasing with the establishment of the PCI Security Standards Council (SSC)
- Legislators and regulators have become involved; there are a number of state laws as well as pending legislative initiatives
- Consumer confidence is impacted by data compromises

# What is the Likelihood of a Breach?



## Compromise Trends

- Visa has seen a notable increase in compromise activity for 2007
- 83% of compromises identified since 2005 are Level 4 merchants
- Brick and mortar compromises involving full track data account for the majority of exposed accounts
- Food services industry accounts for a majority of compromise events
- Majority of compromise incidents involve use of vulnerable payment applications
- Franchises commonly targeted
- Unsecured remote access applications contribute to compromises

# PCI DSS



## PCI DSS is based on fundamental data security practices

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

# Visa's Cardholder Information Security **VISA** Program (CISP)

## Visa's Security Initiatives for 2007

- Foster communication and collaboration with key stakeholders to improve overall payment system security
- Eliminate prohibited data retention, including track, CVV2 and PIN data

***“Don't store it, if you don't need it!”***

- Drive merchant, processor and agent compliance with the PCI DSS
- Support small merchant awareness and use of secure payment applications



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

# Payment Application Best Practices



## Milestones in the adoption of secure payment applications

- Visa launched PABP in 2005 to eliminate storage of prohibited data and facilitate PCI DSS compliance
- List of validated payment applications published monthly since January 2006
  - As of June 2007, 162 products across 86 vendors independently validated by a Qualified Security Assessor (QSA)
- Visa organized and hosted a PABP Vendor Conference December 2006
  - Over 100 product vendors attended
- List of vulnerable payment applications published February 2007
- Elevate PABP to an industry standard through PCI SSC



# Where is the Risk?



**As large merchants achieve PCI DSS compliance, risk of compromises migrating to smaller merchants (June 30, 2007)**

<b>CISP Category</b> (Visa transactions / year)	<b>Estimated Population Size</b>	<b>Estimated % of Visa Transactions</b>	<b>PCI DSS Compliance</b>	<b>Initial Validation in Progress / Remediating</b>
<b>Level 1 Merchant</b> (> 6M)	327 (230)	50% (48%)	39% (46%)	50% (54%)
<b>Level 2 Merchant *</b> (1 – 6M)	920	13%	33%	42%
<b>Level 3 Merchant</b> (e-commerce only 20,000 – 1M)	2,410	< 5%	52%	22%
<b>Level 4 Merchant</b> (< 1M)	~ 6,000,000	32%	Low	N/A
<b>VisaNet Processor</b> (Direct Connection)	76	100%	88%	12%
<b>Agent</b> (Downstream)	451	N/A	65%	13%

\* Level 2 redefined in July 2006 and merchants identified in late 2006.

# Top 5 Data Security Vulnerabilities



Based on merchant compromises, Visa has found the following common vulnerabilities:



1. Storage of prohibited data (e.g., full track, CVV2, PIN blocks)
2. Un-patched systems
3. Vendor default settings and passwords (e.g., unsecured wireless)
4. Poorly coded web-facing applications resulting in SQL injection
5. Unnecessary and vulnerable services on servers

# Three Step Approach for Merchants



## 1) Eliminate prohibited cardholder data

- Full magnetic stripe data (i.e., track 1, track 2), CVV2, and PIN blocks must not be retained subsequent to transaction authorization
- Do not use known vulnerable payment applications
- Use PABP-validated applications listed at [www.visa.com/cisp](http://www.visa.com/cisp)

## 2) Protect cardholder data using secure payment applications

- Minimize data storage storing only account number, expiration date, name and service code where business needs exist
- If you don't need it, don't store it!
- Protect data that must be retained by rendering it unreadable

## 3) Secure the environment according to the PCI DSS

- Validate PCI DSS compliance on systems where cardholder data is stored, processed or transmitted
- Utilize compliant agents listed at [www.visa.com/cisp](http://www.visa.com/cisp)



# Reference Tools

## PCI Security Standards Council (PCI SSC)

- Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaire
- Security Scanning Procedures
- Qualified Security Assessor List
- Approved Scan Vendor List
- Glossary of Terms

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

## Visa CISP

- Archive of Data Security Alerts, bulletins and webinars
- What To Do If Compromised guide
- Qualified CISP Incident Response Assessor List
- List of CISP-Compliant Service Providers
- Payment Application Best Practices
- List of Validated Payment Applications

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