Introduction to PCI Compliance
Who is HALOCK Security Labs?

- Established in 1996
- Focused 100% on security since 1999
- One of less than 5 QSA approved companies based in Chicago
- All Partners and Directors are QSAs
- Completed 75+ Compliance Engagements in 2009
- Certified Ethical Hackers (CEH) and Authorized Training Center for Ethical Hacking
- Project Management Office and Certified Project Management Professionals (PMPs)
Overview of the PCI Standards

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data

MANUFACTURERS
PCI PTS
PIN Transaction Security

SW DEVELOPERS
PCI PA-DSS
Payment Application Data Security Standard

MERCHANTS & PROCESSORS
PCI-DSS
Data Security Standard

PCI SECURITY & COMPLIANCE

Ecosystem of retail payment devices, applications, infrastructure and users
<table>
<thead>
<tr>
<th>Phase</th>
<th>Compliance Mandate</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications</td>
<td>1/1/08</td>
</tr>
<tr>
<td>2</td>
<td>VNPs and agents must only certify new payment applications to their platforms that are PA-DSS-compliant</td>
<td>7/1/08</td>
</tr>
</tbody>
</table>
| 3     | Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PA-DSS-compliant applications  
Level 3: Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.  
Level 4: Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year. | 10/1/08        |
| 4     | VNPs and agents must decertify all vulnerable payment applications                                                                                                                                                    | 10/1/09        |
| 5     | **Acquirers must ensure their merchants, VNPs and agents use only PA-DSS compliant applications**                                                                                                                  | 7/1/10         |
What is the PCI SSC?

- Payment Card Industry Security Standards Council (SSC)
- The SSC is an independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis
- Founding multi-national acceptance brand members:
  - American Express
  - Discover Financial
  - JCB
  - MasterCard Worldwide
  - Visa, Inc.
What is a Qualified Security Assessor (QSA)?

- Only certified QSAs are approved by the PCI Security Standards Council to provide PCI guidance and validation.
- Only about 5 QSA companies are based in Chicago, and HALOCK is one of those companies.
- Only 800 QSA individuals in all of North America (average of about 16 per state).
- Assist merchants and service providers in getting compliant and validating that compliance.
What are the Business Drivers behind PCI?

- Avoid potential breach fines or Non-Compliance fees
- Achieve Safe Harbor\(^1\) status - consequences waived
- Maintain ability to continue process credit cards
- Avoid cost of data breach
- Recognize organizational benefits
- Reduce Risk - “Hacking” has become a profitable line of business for organized crime

\(^1\) Safe Harbor status: Per Visa, Safe Harbor Status requires that “a member, merchant, or service provider must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation.”
Credit Cards are Being Sold on the Internet

Golden Dump

About  News  Prices  Rules  Contacts

487533546
goldendump@rambler.ru

GOLD NEWS

24 Feb 2009, 5:56 PM
Good news: Gold dumps are available!
New batch of fresh USA Visa Gold dumps is available now.
Read more >>>

1 Feb 2009, 11:56 PM
Global site update!
Today we opened some new parts of our site. We have added a new page where you can find all news, promotions and other fresh information.
Read more >>>

PRICES

Prices on 17 Mar 2009

- USA classic: $22
- USA gold/plat/bus: $40
- USA sign/corp/world: $44
- Canada classic: $50
- Canada gold/plat/bus: $65
- Euro classic: $120
- Euro gold/platinum: $160
- Discover: $30
- Amex grit/opt/gold/plat: $25
- Amex corp/centurion: $50

HISTORY

Hi everyone!
My name is Pita Baidy and I am the credit card dumps seller. Our team skims dumps all over the world and sells them to you.

Every few days we have a lot of fresh credit card dumps AA and AAA quality. We have usa/eu/canada/asia/latin etc. dumps.

We occupy leading positions in this business. I hope you have
PCI Non-Compliance Fines are Increasing Rapidly

- Fines are escalating overall
- These fines are also being applied increasingly to Level 2, 3 and 4 merchants.
State Laws Mandating PCI DSS Compliance

- Laws in effect
  - Nevada
  - Minnesota
  - Washington

- Pending Legislation
  - Alabama
  - Iowa

- Several more will likely follow suite – As occurred post California SB1386
A Closer Look at the PCI Data Security Standard and Compliance Requirements
Who are the Players?

Issuers

Card Brands

Acquirers

Service Providers

Consumers

Merchants
How is PCI Enforced?

Card Brands

Card brands have contracts with banks requiring them to ensure their merchants are PCI compliant

Acquirers

Banks have contracts with merchants requiring them to stay PCI compliant

Merchants

Banks must sponsor Level 1 Service Providers and must then monitor their compliance status

Service Providers

Merchants have contracts with Service Providers requiring them to protect cardholder data

HALOCK Security Labs
Purpose Driven Security
Validation Requirements are based on Transaction Levels

### Merchant Levels

<table>
<thead>
<tr>
<th>MERCHANT LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 1              | Any merchant, regardless of acceptance channel, processing over 6,000,000 Visa transactions per year.  
  - Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. |
| 2              | Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 Visa transactions per year. |
| 3              | Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year. |
| 4              | Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1,000,000 Visa transactions per year. |

### Service Provider Levels

<table>
<thead>
<tr>
<th>SERVICE PROVIDER LEVEL</th>
<th>DESCRIPTION</th>
<th>POSTED ON VISA’S LIST OF COMPLIANT SERVICE PROVIDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VisaNet® processors and third party agents that store, process or transmit more than 300,000 Visa transactions annually.</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Any third party agent that stores, processes or transmits less than 300,000 Visa transactions annually.</td>
<td>No*</td>
</tr>
</tbody>
</table>

* Level 2 service providers may choose to validate as a Level 1 service provider in order to be listed on Visa’s list of compliant service providers.
### Your Level Defines the Form of your Validation

<table>
<thead>
<tr>
<th>Group</th>
<th>Level</th>
<th>Compliance Actions</th>
<th>Validation Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant</td>
<td>1</td>
<td>Required</td>
<td>On-Site Security Assessment Required Annualy</td>
</tr>
<tr>
<td></td>
<td>2 &amp; 3</td>
<td>Required</td>
<td>Self-Assessment Questionnaire Required Quarter Yearly</td>
</tr>
<tr>
<td></td>
<td>4**</td>
<td>Required</td>
<td>Network Scan* Required Quarter Yearly</td>
</tr>
<tr>
<td>Service Providers</td>
<td>1</td>
<td>Required</td>
<td>Required Annualy</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Required</td>
<td>Required Annualy</td>
</tr>
</tbody>
</table>

*Network scanning is applicable to any internet facing system. **Validation requirements are determined by the merchant’s acquirer.

- **Effective June 30, 2011,** Level 2 merchants doing a self-assessment will have to send staff to PCI SSC-offered merchant training programs and pass an annual accreditation program.
- Validation is NOT the same as Compliance.
- Validation – can be accomplished through filling out a questionnaire.
- Compliance – requires actually doing what you say you are doing.
- **Why does this matter?**
# What Can Be Stored?

## What the PCI Rules Say About Data Storage

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
<th>Rule 3.4 Applies¹</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name²</td>
<td>Yes</td>
<td>Yes²</td>
<td>No</td>
</tr>
<tr>
<td>Service Code²</td>
<td>Yes</td>
<td>Yes²</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date²</td>
<td>Yes</td>
<td>Yes²</td>
<td>No</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data³</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

¹Requires rendering the PAN unreadable through encryption, truncation, or other means.
²Must be protected if stored with PAN.
³Must not be stored after authorization, even if encrypted.

Source: PCI Security Standards Council
PCI Data Security Standard (DSS)

12 High Level Requirements – Seems so Innocent!

<table>
<thead>
<tr>
<th>Build and Maintain a Secure Network</th>
<th>Implement Strong Access Control Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 1:</strong> Install and maintain a firewall configuration to protect data</td>
<td><strong>Requirement 7:</strong> Restrict access to data by business need-to-know</td>
</tr>
<tr>
<td><strong>Requirement 2:</strong> Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td><strong>Requirement 8:</strong> Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td><strong>Requirement 3:</strong> Protect stored data</td>
<td><strong>Requirement 9:</strong> Restrict physical access to cardholder data</td>
</tr>
<tr>
<td><strong>Requirement 4:</strong> Encrypt transmission of cardholder data and sensitive information across public networks</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protect Cardholder Data</th>
<th>Regularly Monitor and Test Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 3:</strong> Protect stored data</td>
<td><strong>Requirement 10:</strong> Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td><strong>Requirement 4:</strong> Encrypt transmission of cardholder data and sensitive information across public networks</td>
<td><strong>Requirement 11:</strong> Regularly test security systems and processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maintain a Vulnerability Management Program</th>
<th>Maintain an Information Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 5:</strong> Use and regularly update anti-virus software</td>
<td><strong>Requirement 12:</strong> Maintain a policy that addresses information security</td>
</tr>
<tr>
<td><strong>Requirement 6:</strong> Develop and maintain secure systems and applications</td>
<td></td>
</tr>
</tbody>
</table>

- 12 High Level Requirements = 200+ Sub Requirements
- The 225 PCI DSS Requirements *can* create an overwhelming project – but it is achievable
PCI is an “All or Nothing” Standard

• A single requirement not being met = Non-Compliance
A Simplified Approach to PCI Compliance
The PCI Program

Year 1

- PCI DSS Gap Assessment or Discovery
- PCI 11.3 and 6.6 Penetration Test (Initial)
- PCI DSS Onsite Assessment & Report on Compliance (Draft)
- PCI 11.3 and 6.6 Penetration Test (Validation)
- PCI DSS Onsite Assessment & Report on Compliance (Final)

Ongoing PCI Counseling and Advisory Services

Year 2 and Beyond

- PCI DSS Mid Year Change Review or Gap Assessment
- PCI 11.3 and 6.6 Penetration Test (Initial)
- PCI DSS Onsite Assessment & Report on Compliance (Draft)
- PCI 11.3 and 6.6 Penetration Test (Validation)
- PCI DSS Onsite Assessment & Report on Compliance (Final)

Ongoing PCI Counseling and Advisory Services
Summary - The Challenge

• The Industry has mandated PCI Compliance with fines for non-compliance

• PCI Compliance translates to “Fortune 100 level of effort” to small and medium (SMB) merchants

• SMB merchants are overwhelmed by the level of effort to achieve PCI Compliance and find themselves frustrated!
Reducing the Scope of the PCI Project

- Larger PCI QSA companies have taken the utility approach to compliance – applying these 225 requirements to all software applications, systems, databases and network devices

- The small and medium businesses are overwhelmed by this level of work

- The Hallock approach focuses on reducing the project scope:
  - Strategic Network Segmentation
  - Outsourcing as much of the cardholder data as possible
  - Evaluating Tokenization Solutions
  - Handholding on an as-needed basis to help customers reduce the scope (vs. putting 2 - 4 consultants on site full time)
Sample Network Diagram (showing revised architecture): Strategically Grouping Cardholder Data in Unique Segments
Primary Guiding Principle for Cardholder Data

If you don’t absolutely need to store it, DON’T!
What Can Be Stored?

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
<th>Rule 3.4 Applies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Yes</td>
<td>Yes&lt;sup&gt;2&lt;/sup&gt;</td>
<td>No</td>
</tr>
<tr>
<td>Service Code&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Yes</td>
<td>Yes&lt;sup&gt;2&lt;/sup&gt;</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Yes</td>
<td>Yes&lt;sup&gt;2&lt;/sup&gt;</td>
<td>No</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data&lt;sup&gt;3&lt;/sup&gt;</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>No</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<sup>1</sup>Requires rendering the PAN unreadable through encryption, truncation, or other means.

<sup>2</sup>Must be protected if stored with PAN.

<sup>3</sup>Must not be stored after authorization, even if encrypted.

Source: PCI Security Standards Council

Purpose Driven Security
We ALL Have a Part to Play in Protecting Cardholder Data

- Attend regular security awareness training
- Read and understand your organization’s security policies
  - Ask questions if you are unclear regarding what is expected of you
- Never share your password with anyone!
- Always make sure your PC is locked before leaving your desk
  - (i.e. password-protected screen saver)
- Keep your desk clear of any sensitive materials
- Always properly dispose of paper records with cardholder data, using cross-cut shredders or approved shredding bins
- Don’t allow unauthorized individuals to follow you into protected areas (“tail-gating”)
Thank You!

www.halock.com