PCI DSS Awareness Session- Ecommerce Merchants

Satyendra K. Sahu
Associate Director- PCI Compliance
AGENDA

- PCI DSS 3.0 Overview
- Understanding the Scope
- Merchant PCI Level & SAQ Selection
- Understanding the Scope - Architectures
- PCI DSS Compliance Roadmap & Approach
- Recommendations & Best Practices
- Misconceptions
PCI DSS 3.0: OVERVIEW

- A single set of worldwide requirements for CARD HOLDER DATA protection across the entire industry.
- Single standard for Payment Card data security
  - Based on industry best practice & credit card incident history
  - Backed by all major card schemes (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.)
- Control Requirements are Mandatory to comply
Protection of Cardholder Payment Data

Ecosystem of payment devices, applications, infrastructure and users
ROLES & RESPONSIBILITIES

- Conduct internal bank PCI Certification
- Report merchant compliance to Card Brands
- Enforce PCI
- Promote Adoption
  - Sanctions
  - Rewards
- Comply with PCI
- Use compliant service providers
- Secure cardholder data
- Maintain the DSS
- Certify QSA’s & ASV’s
- Verify compliance through onsite assessment
- Quarterly vulnerability scans
- Render opinions to merchant bank on compensating controls

Owned and maintained by the PCI Security Standards Council

Promoted and enforced by the card brands

Administered by acquiring banks

Interpreted by Qualified Security Assessors (QSA’s)

Observed by merchants

Assessed by merchants or QSA’s and by Approved Scan Vendors (ASV’s)
**CARD HOLDER DATA**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Render Stored Data Unreadable per PCI DSS requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Holder Data</td>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cardholder Name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Service Code</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Expiration Date</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Sensitive Authentication Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Track Data</td>
<td>No</td>
<td></td>
<td>Cannot store per PCI DSS Requirement 3.2</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2/CID</td>
<td>No</td>
<td></td>
<td>Cannot store per PCI DSS Requirement 3.2</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>No</td>
<td></td>
<td>Cannot store per PCI DSS Requirement 3.2</td>
</tr>
</tbody>
</table>

- Sensitive authentication data must not be stored after authorization (even if encrypted).
- Track Data: Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere
- CAV2/CVC2/CVV2/CID: The three- or four-digit value printed on the front or back of a payment card
- PIN/PIN Block: Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message
<table>
<thead>
<tr>
<th>Level / Tier</th>
<th>Merchant Criteria</th>
<th>Validation Requirements</th>
</tr>
</thead>
</table>
| 1          | Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region | - Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or Internal Auditor if signed by officer of the company  
- The internal auditor is highly recommended to obtain the PCI SSC Internal Security Assessor ("ISA") certification  
- Quarterly network scan by Approved Scan Vendor ("ASV")  
- Attestation of Compliance Form |
| 2          | Merchants processing 1 million to 6 million Visa transactions annually (all channels) | - Annual Self-Assessment Questionnaire ("SAQ")  
- Quarterly network scan by ASV  
- Attestation of Compliance Form |
| 3          | Merchants processing 20,000 to 1 million Visa e-commerce transactions annually    | - Annual SAQ  
- Quarterly network scan by ASV  
- Attestation of Compliance Form |
| 4          | Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually | - Annual SAQ recommended  
- Quarterly network scan by ASV if applicable  
- Compliance validation requirements set by merchant bank |

https://www.visa-asia.com/merchants/stayingsecuremerchants/accountsecurity.shtml#
<table>
<thead>
<tr>
<th>Level / Tier</th>
<th>Merchant Criteria</th>
<th>Validation Requirements</th>
</tr>
</thead>
</table>
| Level 1     | • Any merchant that has suffered a hack or an attack that resulted in an account data compromise  
• Any merchant having more than six million total combined MasterCard and Maestro transactions annually  
• Any merchant meeting the Level 1 criteria of Visa  
• Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system | • Annual Onsite Assessment  
• Quarterly Network Scan conducted by an ASV |
| Level 2     | • Any merchant with more than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually  
• Any merchant meeting the Level 2 criteria of Visa | • Annual Self-Assessment  
• Onsite Assessment at Merchant Discretion  
• Quarterly Network Scan conducted by an ASV |
| Level 3     | • Any merchant with more than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually  
• Any merchant meeting the Level 3 criteria of Visa | • Annual Self-Assessment  
• Quarterly Network Scan conducted by an ASV |
| Level 4     | • All other merchants | • Annual Self-Assessment  
• Quarterly Network Scan conducted by an ASV |

SELECTING YOUR SUITABLE SAQ

SAQ SELECTION INSTRUCTIONS

- To determine the applicable SAQs, follow the path(s) for EACH channel.
- If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- Merchants must meet all eligibility criteria for any applicable SAQ.
No matter which option a merchant may choose, there are several key considerations to keep in mind regarding the security of cardholder data, including:

- **No option completely removes a merchant’s PCI DSS responsibilities**
  - Regardless of the extent of outsourcing to third parties, the merchant retains responsibility for ensuring that payment card data is protected.
  - Connections and redirections between the merchant and the third party can be compromised and;
  - The merchant should monitor its systems to ensure that no unexpected changes have occurred and that the integrity of the connection/redirection is maintained.

- **E-commerce payment applications such as shopping carts**
  - Should be validated according to PA-DSS, and
  - Confirmed to be included on PCI SSC’s list of Validated Payment Applications.
  - For in-house developed e-commerce applications, PA-DSS should be used as a best practice during development.
COMMON E-COMMERCE IMPLEMENTATIONS

- **Merchant Managed (Self Served)**
  - Proprietary/custom developed shopping cart/payment application
  - Commercial shopping cart/payment application
  - The merchant should monitor its systems to ensure that no unexpected changes have occurred and that the integrity of the connection/redirection is maintained.

- **Hybrid Architecture (Shared Architecture)**
  - Third-party embedded application programming interfaces (APIs) with Direct Post
  - An inline frame (or “iFrame”) that allows a payment form hosted by a third party to be embedded within the merchant’s page(s)
  - Third-party hosted payment page which redirects the consumer to a page on an entirely different domain for payment entry

- **Completely Outsourced**
  - Merchant website, along with payment page is hosted and managed by approved service provider
MERCHAND MANAGED PAYMENT ENVIRONMENT

- For proprietary or custom-developed e-commerce implementations (also called “bespoke”)
  - The application code for the merchant’s shopping cart/payment application has either been developed by the merchant internally or
  - Custom-developed by a third party as part of the overall development of the website.

- Merchant PCI Scope
  - Ensuring secure development of merchant-developed software
  - Confirming PA-DSS validation of third-party payment applications
  - Having written agreements with any third parties and ensuring that cardholder data (CHD) is protected in accordance with PCI DSS.
MERCHANT MANAGED PAYMENT ENVIRONMENT

- **Merchant-managed Commercial Shopping Cart/Payment Applications**
  - Similar to the previous case (Proprietary/Custom Developed), except that the payment functionality is delivered through commercially available software used in the merchant’s site (the “payment application”). Such payment applications are developed and licensed for commercial use.

- **Merchant PCI Scope**
  - Ensuring secure development of merchant-developed software
  - Confirming PA-DSS validation of third-party payment applications
  - Having written agreements with any third parties and ensuring that cardholder data (CHD) is protected in accordance with PCI DSS.
HYBRID ARCHITECTURE (WEB REDIRECTION)

- E-commerce implementations the merchant’s customer is redirected to the payment page on the e-commerce payment processor’s site to enter payment card data.
- Once payment is processed, acknowledgement is sent back to the merchant’s web application.

- **Merchant PCI Scope**
  - Managing website and servers (if self-hosted), including applicable PCI DSS requirements
  - Applicable PCI DSS requirements for managing third parties, (e.g., Requirement 12.8)
  - Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS.
  - Securing the web page(s) containing the redirection code and/or function(s).

* Card Verification Code or Value/Card Security Code (CAV2, CVC2, CVV2, CID)
HYBRID ARCHITECTURE (DIRECT POST)

- the merchant hosts a web application using third-party APIs that redirect the payment data from the consumer’s browser directly to the e-commerce payment processor.
- The e-commerce payment processor accepts the payment card data from the consumer and passes a confirmation code (ID number, token, etc.) back to the merchant’s web application.

- **Merchant PCI Scope**
  - Managing website and servers (if self-hosted), including applicable PCI DSS requirements
  - If website/server hosting is outsourced, applicable PCI DSS requirements for management of third parties (e.g., Requirement 12.8)
  - Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS
  - Securing the web page(s) containing API code and/or function(s).
HYBRID ARCHITECTURE (iFRAME)

- Inline frames or “iFrames” allow a web page to be embedded within another web page.
- A common e-commerce implementation is to accept card payments via an e-commerce payment processor’s hosted web pages.
- The merchant’s web application then embeds the e-commerce payment processor’s web payment page as an inline frame so that it appears as part of the merchant’s page.
- When data is entered into the payment page, it is posted directly to the e-commerce payment processor’s web application server instead of the merchant’s.
- This iFrame host is transmitting and processing (and possibly storing) cardholder data, and both service providers in this scenario can affect the security of the transaction. In this implementation, the merchant should consider both third parties—the intermediate party hosting the iFrame and the third-party processor who provides the iFrame—to be service providers for the merchant, and the merchant should monitor the PCI DSS compliance of both third parties.

- Merchant PCI Scope
  - Managing website and servers (if self-hosted), including applicable PCI DSS requirements
  - If website/server hosting is outsourced, applicable PCI DSS requirements for management of third parties (e.g., Requirement 12.8)
  - Having written agreements with any third parties and ensuring that they protect cardholder data on behalf of the merchant, in accordance with PCI DSS
  - Securing the web page(s) containing the iFrame code.
Many merchants are interested in managing their PCI DSS responsibility by outsourcing all cardholder data storage, processing, and transmission to a third party hosting provider or e-commerce payment processor.

- Merchants may elect to use a solution provided and hosted by a third party, which is wholly under the control and responsibility of the third party.
- This type of solution could consist of an e-commerce application, hosted servers, and hosted infrastructure, which are all provided and managed by the third party.
- A web interface is provided for the merchant to access the third-party site, and to manage the e-commerce store and customers.

**Merchant PCI Scope**

- Applicable PCI DSS requirements for managing third parties, (e.g., Requirement 12.8)
- Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS
- Ensuring that the outsourced/hosted environment receives a passing score from an appropriate ASV scan on a quarterly basis.
SECURITY CONSIDERATIONS: HYBRID MODELS

As mentioned above, for each of these shared-management implementations, there is a security risk for the merchant since weaknesses on the merchant’s website can lead to compromises of payment card data during the transaction process.

- **Direct-post API Approach**: With the direct-post API approach, the merchant is still responsible for the web page that is presented to the consumer, and the merchant hosts the fields on the payment page that accept the data—only the cardholder data is posted directly from the consumer to the service provider. Since the payment pages are hosted by the merchant, the payment pages are only as secure as the merchant’s website, and a compromise of the merchant’s system could lead to a compromise of payment card data.

- **iFrame Approach**: With the iFrame approach, the iFrame must be configured and managed to prevent it from being modified to send cardholder data to an alternate and unauthorized source.

- **Hosted-payment Page (Redirection) Approach**: With hosted payment pages, a compromise of the merchant’s server could lead to redirection of communications intended for the e-commerce payment processor, allowing payment card data to be intercepted and stolen as transactions occur.
ASSESSMENT METHODOLOGY & APPROACH

- Conduct PCI DSS Self Assessment
- Perform ASV Scans
- Perform Penetration Testing (If applicable)
- Attest SAQ/AOC (ISA, Authorized Personnel, QSA)
- Submit the SAQ/AOC to PSP and / or Bank

NOTE: Below phases and chronology is a best practice and depends on Merchant’s PCI Scope
RECOMMENDATIONS & BEST PRACTICES

- Know the Location of all Your Cardholder Data
- If You Don’t Need It, Don’t Store It
- Limit display of Cardholder Data
- Evaluate Risks Associated with the Selected E-commerce Technology
- Address Risks Associated with Outsourcing to Third-party Service Providers
- ASV Scanning of Web-hosted Environments
- Best Practices for Payment Applications – PA DSS, OWASP, SANS
- Implement Security Training for all Staff
-Delegate Information Security responsibility to qualified staff

Information Security Resources:
- Payment Card Industry Security Standards Council (PCI SSC) (www.pcisecuritystandards.org)
- Open Web Application Security Project (OWASP) (www.owasp.org)
- The SysAdmin, Audit, Network, and Security (SANS) Institute (www.sans.org)
- The Center of Information Security (CIS) (www.cis.org)
- Information Systems Audit & Control (ISACA) (www.isaca.org)
COMMON MISUNDERSTANDINGS

1. I’m a small merchant, who only takes a handful of cards, so I don’t need PCI.... A common misunderstanding with the standard is that small merchants, handling a few 10’s of credit cards a day are exempt from compliance. If you are a merchant and you are set up to take credit cards, by any mechanism - then you need to be complaint

2. PCI only applies to E-commerce companies.... No, PCI applies to every company that stores, processes or transmits cardholder information. In fact anyone who takes card present transactions that involve POS devices are more at risk than E-Commerce solutions, quite often these types of transactions involve storage of track data (which is forbidden under PCI). Disclosure of this type of data will bring heavy fines and requests for compensation from the banks involved.

3. You only have to be compliant with the majority of criteria.... The pass mark for PCI is 100%, so if you fail even one of the criteria, you fail PCI. The standard is not really meant to be something to strive for; it is really a floor, a basis for further security measures. Failing to achieve even one of the requirements, is failing to meet a basic standard for handling cardholder information. All companies that routinely handle this type of data should be aiming to exceed the standard.
4. **As a Merchant, I did not sign anything, saying I would be complaint; therefore, I do not need to be...**

   The PCI standard forms part of the operating regulations that are the rules under which Merchants are allowed to operate merchant accounts. The regulations signed when the Merchant opens an account at the bank state that the VISA regulations have to be adhered to. Even if you have been in business for decades, PCI still applies, if you store, process or transmit credit cards.

5. **As a Merchant, I’m entitled to store any data....** Many Merchants believe that they own the customer and have a right to store all the data about that customer in order to help their business. Not only is this incorrect regarding PCI, it may also be a violation of State and Federal legislation regarding privacy.

6. **I can wait until my bank asks me to be compliant....** The dates for Merchants demonstrating compliance are long gone, and the Merchant is responsible for making sure they are in compliance. Waiting until the bank asks you could be very costly indeed.

7. **I only need to protect my credit card data, not ATM debit card related data....** Unfortunately, both are required. Many debit cards are dual-purpose “signature debit,” which can be used on debit and credit card networks. As such, they are covered under PCI and must be protected in the same way as credit cards.
8. **I can wait until my business grows....** Unfortunately, the PCI standard applies to all sizes of business and waiting could be costly. Should you be compromised and not be compliant the fines and the compensation sort by the banks (it costs between $50 and $90 to replace one card) could be substantial.

9. **I can just answer “yes” to all the criteria on the self-assessment....** The self-assessment is merely a mechanism for getting the information about the level of your compliance to your merchant bank or to Visa. The standard applies at all times. Just saying yes to the questions puts the merchant at great risk. If a compromise took place and it was obvious that the merchant was not and has never been compliant, the matter would be taken very seriously by VISA. The merchant would be risking the whole business by answering “yes” to the questions, when there is no basis in fact for that answer.

10. **As a merchant I’m not liable if a credit card is compromised....** Merchants are liable and not just for the credit card compromise, there are basically 4 scenarios where credit card data is compromised: Merchants can be liable not only for the compromise but also for subsequent damages from the issuing banks.
THANK YOU