Annual Trustwave PCI Self Assessment Questionnaire (SAQ) Educational Presentation

Understanding the Merchants Responsibilities for PCI Compliance
Agenda

• Discussion on Merchant Responsibilities
• Discussion on SAQ’s
• Discussion on New Expectations
• Question and Answer
Merchant Responsibilities
PCI Merchant Responsibilities

Know your payment card processing business and how you process credit cards
• Mail, Phone, Online, Over the Counter F2F, Secure fax
24/7 adherence to PCI DSS
• Read PCI DSS standards
• Keep cardholder data secure and confidential
• Limit physical access to terminals and data from terminals; need to know basis

Attend Trainings; includes all employees who have access to cardholder data or revenue
• Revenue Process (attendance once every two years)
• Security Awareness Education (SAE-annually)

Complete Annual SAQ to attest PCI Compliance
PCI DSS Standards

Payment Card Industry Security Standards

PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards globally govern all merchants and organizations that store, process or transmit this data, and include specific requirements for software developers and manufacturer of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI Standards Include:
- Payment Card Industry Security Standards
- PCI PTS
- P2PE
- PCI-SQ
- Payment Application Data Security Standard (PA-DSS)
- PCI DSS Data Security Standard
- PCI Security Standards & Compliance

PCI Data Security Standard for Merchants & Processors

The PCI DSS is the global data security standard that any business of any size must achieve in order to accept payment cards. It presents common sense steps that minor best practices.

<table>
<thead>
<tr>
<th>Goal</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a secure network</td>
<td>Establish and maintain a secure network.</td>
</tr>
<tr>
<td>2. Store cardholder data securely</td>
<td>Protect cardholder data from unauthorized access.</td>
</tr>
<tr>
<td>3. Maintain a secure network configuration</td>
<td>Protect cardholder data from unauthorized access.</td>
</tr>
<tr>
<td>4. Use strong encryption for cardholder data</td>
<td>Maintain a secure network configuration.</td>
</tr>
<tr>
<td>5. Regularly update anti-virus software and firewalls</td>
<td>Maintain a secure network configuration.</td>
</tr>
<tr>
<td>6. Test system and network security</td>
<td>Test system and network security.</td>
</tr>
<tr>
<td>7. Restrict access to cardholder data</td>
<td>Limit access to cardholder data.</td>
</tr>
<tr>
<td>8. Use strong access control measures</td>
<td>Limit access to cardholder data.</td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
<td>Limit access to cardholder data.</td>
</tr>
<tr>
<td>10. Maintain an information security policy</td>
<td>Maintain an information security policy.</td>
</tr>
</tbody>
</table>

Participating Organizations

- Merchants
- Banks
- Processors
- Developers
- Point-of-sale vendors

PCI SSC Founders

- Visa
- MasterCard
- American Express
- Discover
- JCB International
SELF ASSESSMENT QUESTIONNAIRE
Why do I have to complete the SAQ?

• Annual requirement for merchants that accept credit cards.
• Confirms that your department strives to keep cardholder data secure.
• Helps Treasury uncover possible weaknesses in processes that may violate PCI DSS.
Self Assessment Questionnaire

Most importantly you are attesting that your department is keeping your payment card processing environment secure by following the guidelines/policies set forth by the PCI Council and the IU Treasurers Office.
Self Assessment Questionnaire

Who should be completing the SAQ?

- Someone designated by Fiscal Officer
- Someone knowledgeable about the merchants processing environment
- Someone who has completed the SAE & Revenue Process Training
Which SAQ Should I Complete?

SAQ Description

A- Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.

B- Standalone, dial-out merchants with no electronic cardholder data storage, imprint only merchants with no electronic cardholder data storage.

C-VT- Merchants using only web-based virtual terminals, no electronic cardholder data storage. (No IU Merchants)

C- Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. (No IU Merchants)

D- All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment card brand as eligible to complete an SAQ.
Which SAQ Should I Complete?

- SAQ’s are based on merchant numbers.
- Each merchant number has to have an SAQ completed.
- Some departments have multiple payment card acceptance methods each having its own merchant number:
  - **Online** = IU PAY Plus, VeriSign/PayPal, Specialty Systems (ticketing, dining, parking, etc.)
    - **Caution**: No merchant should be entering cardholder data into an online system for the cardholder (i.e. No IU Computer or Workstation).
  - **POS Stand Alone Terminals** = F2F, Mail, Phone, Secure Fax
    - **Caution**: Any mail-in, phone-in, secure fax cardholder data should be cross shredded after entered into terminal. Email and phone messages strictly prohibited. Secure Fax acceptable.
Self Assessment Questionnaire

THE BASICS

Expiration Date

How many SAQ’s

SAQ Type
### SAQ (A) & B Merchants

#### Section A. ELIGIBILITY

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions</td>
<td>[TWQ1923]</td>
<td>✔️</td>
<td>✔️</td>
<td>If you are using a 3rd party processor all credit card information is directly transacted on their site. If your department is entering cardholder data through your computers, <strong>STOP</strong>! Consult with Treasury you may be in violation of PCI DSS.</td>
</tr>
<tr>
<td>1</td>
<td>The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant</td>
<td>[TWQ1924]</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Merchant does not store any cardholder data in electronic format</td>
<td>[TWQ1926]</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Merchant retains only paper reports or receipts with cardholder data, and such documents are not received electronically</td>
<td>[TWQ1925]</td>
<td>✔️</td>
<td>❌</td>
<td></td>
</tr>
</tbody>
</table>
### SAQ A & (B) Merchants

Every merchant should be using a Treasury issued terminal. These terminals do not store cardholder data. The receipts that come out of them should be truncated and are not considered to be received electronically.

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>Merchant description</td>
<td>[TWG1693]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Merchant uses only standalone, dial-up terminals, and the standalone, dial-up terminals are not connected to the Internet or any other systems within the merchant environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Merchant does not store any cardholder data in electronic format.</td>
<td>[TWG1926]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Merchant retains only paper reports or receipts with cardholder data, and such documents are not received electronically</td>
<td>[TWG1926]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Section A. ELIGIBILITY

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:
### Section B. 3. STORED DATA PROTECTION

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>B-1</td>
<td>Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)? (SAQ #3.2)</td>
<td>✔️ [TWQ2123]</td>
<td>✔️ [TWQ2123]</td>
<td>✔️ [TWQ2123]</td>
</tr>
<tr>
<td>✔️</td>
<td>4</td>
<td>Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, contained in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.</td>
<td>✔️ [TWQ2130]</td>
<td>✔️ [TWQ2130]</td>
<td>✔️ [TWQ2130]</td>
</tr>
<tr>
<td>✔️</td>
<td>5</td>
<td>Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. (SAQ #3.2.2)</td>
<td>✔️ [TWQ2132]</td>
<td>✔️ [TWQ2132]</td>
<td>✔️ [TWQ2132]</td>
</tr>
<tr>
<td>✔️</td>
<td>6</td>
<td>Do not store the personal identification number (PIN) or the encrypted PIN block. (SAQ #3.2.3)</td>
<td>✔️ [TWQ2134]</td>
<td>✔️ [TWQ2134]</td>
<td>✔️ [TWQ2134]</td>
</tr>
<tr>
<td>✔️</td>
<td>B-6</td>
<td>Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)?</td>
<td>✔️ [TWQ2136]</td>
<td>✔️ [TWQ2136]</td>
<td>✔️ [TWQ2136]</td>
</tr>
</tbody>
</table>

This section is based on your POS terminal. A printout of terminal receipt and detail report should reveal the truncation of credit card and expiry date.
### SAQ A & (B) Merchants

#### Section C. 4. TRANSMITTED DATA PROTECTION

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>C-1</td>
<td>Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)? (SAQ #4.2)</td>
<td></td>
<td></td>
<td>TWQ2156</td>
</tr>
</tbody>
</table>

#### Section D. 7. ACCESS RESTRICTIONS

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>D-1</td>
<td>Is access to system components and cardholder data limited to only those individuals whose jobs require such access? (SAQ #7.1)</td>
<td></td>
<td></td>
<td>TWQ2200</td>
</tr>
</tbody>
</table>

#### Section E. 9. PHYSICAL ACCESS CONTROLS

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>E-1</td>
<td>Are all paper and electronic media that contain cardholder data physically secure? (SAQ #9.6)</td>
<td></td>
<td></td>
<td>TWQ2246</td>
</tr>
<tr>
<td></td>
<td>E-2</td>
<td>Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?(SAQ #9.7.a)</td>
<td></td>
<td></td>
<td>TWQ2248</td>
</tr>
</tbody>
</table>

Do controls include the following:

<table>
<thead>
<tr>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Is the media classified so it can be identified as confidential?(SAQ #9.7.1)</td>
<td></td>
<td></td>
<td>TWQ2250</td>
</tr>
</tbody>
</table>

P P P should be written using the sections of the SAQ as the outline. Give detail descriptions for each section of how your department handles and/or maintains the information referenced in each question.
This section is asking how you control the physical access to cardholder data, how is it transmitted, secured, and destroyed after it is no longer needed.
This section contains questions that pertain to your department and to Treasury functions. Your PPP should include what you do in your department in regards to these security questions. Treasury is available to consult with you concerning this section and the writing of your PPP’s.
SAQ A & B Merchants

These next four questions in particular relate to the functions that Treasury maintains and we will add the documentation to each merchant’s Virtual Binder.

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>25</td>
<td>A list of service providers is maintained. (SAQ #12.8.1) (TW2333)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>26</td>
<td>A written agreement is maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. (SAQ #12.8.2) (TW2335)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>27</td>
<td>There is an established process for engaging service providers, including proper due diligence prior to engagement. (SAQ #12.8.3) (TW2337)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>28</td>
<td>A program is maintained to monitor service providers’ PCI DSS compliance status. (SAQ #12.8.4) (TW2339)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>CA.1</td>
<td>PCI DSS Self-Assessment Questionnaire was completed according to the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>CA.2</td>
<td>All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment. (TW21918)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Section G. CONFIRMATION AND ACKNOWLEDGEMENT

<table>
<thead>
<tr>
<th>Status</th>
<th>Item</th>
<th>Question</th>
<th>Your Response</th>
<th>Best Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>CA.3</td>
<td>I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times. (TWQ1000)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>CA.4</td>
<td>No evidence of magnetic stripe (i.e., track) data*, CAV2, CVC2, CID, or CVV2 data**, or PIN data*** storage subsequent to transaction authorization was found on ANY systems reviewed during this assessment. (TWQ1021)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>CA.5</td>
<td>I have confirmed with my POS vendor that my POS system does not store sensitive authentication data after authorization. (TWQ1022)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>CA.6</td>
<td>Signature of Executive Officer (please provide full name) (TWQ1001)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✔️</td>
<td>CA.7</td>
<td>Title of Executive Officer (TWQ1002)</td>
<td>Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This final section is your attestation that you understand what you just completed, that it is a full assessment of your payment card environment, and that you have read the PCI DSS. Whomever completes the SAQ will sign it.
Compliance Certificate

PCI DSS Certificate of Compliance

Awarded To:
Treasury web Testing (IU PAY)

PCI Level: 4
Classification: Merchant
Expiration Date: Oct 11, 2011

Trustwave Engagement Information
Self-Assessment Questionnaire: Pass
Data Completed: Oct 13, 2011
Version Completed: PCI DSS Form A
Client SAQ Attestation: Kim L. Stuart
Title: Senior Mgr. Treasury Ops.

Certificate Number: 4F71-D742-42EE-0359

Client Authorization: 
Print Name: 
Sign Name: 

Trustwave

Immediate Security & Investigation
Compliance Certificate

PRINT
• Print certificate after completion of SAQ

SIGN
• Sign and date certificate
• Signatures required: person completing SAQ & Fiscal Officer

FORWARD
• Forward to Treasury Operations Office
• Treasurers Office signs certificate to verify SAQ completion
# SAQ D Merchants

## The Sections of SAQ D

<table>
<thead>
<tr>
<th>A) Firewall Configuration</th>
<th>H) Account Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>B) Systems Settings</td>
<td>I) Physical Access Controls</td>
</tr>
<tr>
<td>C) Stored Data Protection</td>
<td>J) Access Tracking</td>
</tr>
<tr>
<td>D) Transmitted Data Protection</td>
<td>K) Monitoring &amp; Testing</td>
</tr>
<tr>
<td>E) Anti-Virus Protection</td>
<td>L) Security Policies &amp; Procedures</td>
</tr>
<tr>
<td>F) Application &amp; Systems Security</td>
<td>M) Hosting Providers</td>
</tr>
<tr>
<td>G) Access Restrictions</td>
<td>N) Confirmation &amp; Acknowledgement</td>
</tr>
</tbody>
</table>
PCI Vulnerability Scans

- Monthly
- Log Results
- Complete Scan Attestation
Trustwave Scan Report Attestation of Compliance

Scan Customer Information
- Company: Trustwave
- Contact: Ranji Abraham
- Title: Email: abraham@indiana.edu
- Telephone: 
- City: State/Province: IN
- Zip: Country: US
- URL: 

Approved Scanning Vendor Information
- Contact: Trustwave Support
- Email: support@trustwave.com
- Telephone: 1-800-363-1621 (US Toll Free) or +1-312-267-3212 (US Toll) or +44 (0) 845 456 9613 (UK Toll Free)
- Business Address: 70 West Madison St., Ste 1050
- City: Chicago
- State/Province: Illinois
- Zip: 60602
- Country: USA
- URL: www.trustwave.com

Scan Status:
- Compliance Status: Passed
- Number of unique components scanned: 2
- Number of identified failing vulnerabilities: 0
- Number of components not scanned by TrustKeeper because the customer confirmed they were out of scope: 0
- Date scan completed: Jul 13, 2011
- Scan expiration date (3 months from date scan completed): Oct 13, 2011

Scan Customer Attestation
RPS Dining Services - Server A attests that: "This scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. RPS Dining Services - Server A also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of the PCI DSS. This scan does not represent RPS Dining Services - Server A's overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements."

Signature
Name: Title: Date:

ASV Attestation
This scan and report were prepared and conducted by Trustwave under certificate number 3702-01-05, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Trustwave attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scanning practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active Interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process.

Confidential Information This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of Trustwave and RPS Dining Services - Server A.
Copyright 2010 Trustwave, All Rights Reserved.
Trustwave Scan Report Attestation of Compliance
**Trustwave Scan Report Attestation of Compliance**

![Trustwave Scan Report](image_url)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Vulnerabilities Noted per IP address</th>
<th>Severity Level</th>
<th>CVSS Score</th>
<th>Compliance Status</th>
<th>Repeated Vulnerabilities (Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability)</th>
</tr>
</thead>
<tbody>
<tr>
<td>140.182.33.38</td>
<td>Windows Terminal Services</td>
<td>1</td>
<td></td>
<td>Pass</td>
<td></td>
</tr>
</tbody>
</table>

**Part 3b. Special Notes by IP Address**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Note</th>
<th>Item Noted</th>
<th>Scan customer's declaration that software is implemented securely (see next column if not implemented securely)</th>
<th>Scan customer's description of actions taken to either 1) remove the software or 2) implement security controls to secure the software</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Special Notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Confidential Information: This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of Trustwave and RFS Dining Services - Server A.*
New Expectations
Interconnected PCI Relationship

Equals a PCI Compliant Environment
PCI Compliance Coordinator

Responsibilities

➢ Complete annual SAQ
➢ Maintain Virtual Binder
➢ Primary Contact for PCI
➢ Maintain, update, all employee training which includes:
  Security Awareness Education (SAE)
  Revenue Process Training

Qualifications

✓ Prefer full-time employee
✓ Trained
  SAE & Revenue Process
Virtual PCI Binder

- SharePoint Environment – all documents will be virtual

- Binder Contents:
  - Departments PCI policies and procedures
  - PCI Compliance Certificate-Treasury adds
  - Signed Merchant Agreement-Treasury adds
  - Copy of Terminal receipt
  - Copy of applications, brochures, paper forms requesting credit card info
  - 3rd Party Service Provider Info-Treasury adds
  - Employee List of trainings completed
  - Equipment spec sheets-Treasury adds
  - Visio diagrams
  - Firewall rules
  - IP addresses
  - Gateways used
  - Vulnerability Scan dates & results

SAQ D-Additional contents
Site Visitations

Treasury will conduct periodic site visits to validate ongoing adherence with PCI DSS which will consist of:

- Comparison of Virtual Binder to daily environmental processes and activities.
- Review all aspects of your revenue processes, credit card, cash and checks.