Sharing Responsibilities: Applicability of PCI DSS Requirements for Merchants and MNSPs

Presenter:
Sam Pfanstiel
Director, Security Consulting Services
ControlScan
Agenda

• Housekeeping
• Presenters
• About Conexxus
• Presentation
• Q & A
This webinar is being recorded and will be made available in approximately 15 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck
- Survey Link – Presentation provided at end

Participants
- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact arussell@conexxus.org for questions regarding a certificate of webinar attendance.

Email: info@conexxus.org
Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Moderator

Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speakers

Sam Pfanstiel
MBA, CISSP, CISM, CISA, QSA, QSA(P2PE), QPA
SME, Data Security Committee
Director, Security Consulting Services; ControlScan
spfanstiel@controlsan.com
About Conexxus

• We are an independent, non-profit, member driven technology organization
• We set standards…
  – Data exchange
  – Security
  – Mobile commerce
• We provide vision
  – Identify emerging tech/trends
• We advocate for our industry
  – Technology is policy
<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 24, 2019</td>
<td><strong>Who’s Watching Your Network? What you should know about Managed Detection &amp; Response (MDR)</strong></td>
<td>Mark Carl, Tom Callahan</td>
<td>ControlScan</td>
</tr>
<tr>
<td>March 21, 2019</td>
<td>Proactive Defense in Depth</td>
<td>Brett Stewart, DeWayne Mangan, Mark Palmer</td>
<td>Acumera</td>
</tr>
<tr>
<td>June 27, 2019</td>
<td>Web Payment Aspirations</td>
<td>Ian Jacobs</td>
<td>W3C</td>
</tr>
<tr>
<td>July 25, 2019</td>
<td>Skimming</td>
<td>Linda Toth, Paige Anderson, Caleb Burke</td>
<td>Conexxus, NACS, CITGO</td>
</tr>
<tr>
<td>August 8, 2019</td>
<td>Application Security 101</td>
<td>Denis Sheridan</td>
<td>Synopsys</td>
</tr>
</tbody>
</table>
# 2019-2020 Conexxus Webinar Schedule

<table>
<thead>
<tr>
<th>Month/Date</th>
<th>Webinar Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 29, 2019</td>
<td>Don't Get Phished!! Train Your Employees To Avoid Ransomware</td>
<td>Geoffrey Vaughan Ed Adams</td>
<td>Security Innovation</td>
</tr>
<tr>
<td>September 26, 2019</td>
<td>Using Data Science to Proactively Manage the Connected C-Store</td>
<td>Ashwin Swamy Thomas Duncan</td>
<td>Omega ATC Omega ATC</td>
</tr>
<tr>
<td>October 24, 2019</td>
<td>Easy PCI—How to Make PCI &amp; Attestation Easier</td>
<td>Ajith Edakandi</td>
<td>Hughes</td>
</tr>
<tr>
<td>November 14, 2019</td>
<td>Impending Consumer Privacy Laws</td>
<td>Alan Thiemann Paige Anderson</td>
<td>Conexxus NACS</td>
</tr>
<tr>
<td>November 21, 2019</td>
<td>Applicability of PCI DSS requirements for Merchants and MNSPs</td>
<td>Sam Pfanstiel</td>
<td>ControlScan</td>
</tr>
<tr>
<td>December 5, 2019</td>
<td>EMV</td>
<td>Brian Russell Linda Toth TBD</td>
<td>Verifone Conexxus Visa</td>
</tr>
<tr>
<td>December 12, 2019</td>
<td>EMV</td>
<td>Gray Taylor Dispenser Manufacturers</td>
<td>Conexxus TBD</td>
</tr>
</tbody>
</table>
2020 Conexxus Annual Conference

April 26 – April 30, 2020
Loews Ventana Canyon
Tucson, AZ

More about Sponsorship Opportunities & Registration:
www.Conexxus.org

Conexxus thanks our 2019 Annual Diamond Sponsors!
Sharing Responsibilities: Applicability of PCI DSS Requirements for Merchants and MNSPs

Presenter:
Sam Pfanstiel
Director, Security Consulting Services
ControlScan
Overview

Conexxus: Sharing Responsibilities: Applicability of PCI DSS Requirements for Merchants and MNSPs
Payment Card Industry Data Security Standard

PCI DSS
PCI Data Security Standard

• 251 Requirements in v3.2.1
  – Not counting service provider requirements and appendices
  – Apply to merchant that operates the card present environment
• All are “required” for all merchants
• Some payment configurations may render some controls “not applicable” (e.g., SAQ eligibility)
PCI DSS Document Repository

- https://www.pcisecuritystandards.org/document_library
- Requirements and Security Assessment Procedures 3.2.1 (link)
- Third-party Security Assurance guidance (link)
- SAQs (Self-Assessment Questionnaires)
Third-Party Service Providers

TPSP
TPSPs: Types

Store/process CHD
• Call center
• E-commerce service
• Loyalty host
• Processors
• Gateways

Secure CHD
• Media destruction
• Tokenization
• Encryption service / KIF
• POS vendor, integrators, resellers

Securing CDE
• Data centers
• Managed infrastructure
• Managed network
• Monitoring/alerting

Incidental access to CHD or CDE
• IT support
• Software developers
• Maintenance services
• Product Delivery
TPSPs and PCI DSS

• Vendor Risk Management & PCI Requirements
  – Disseminate Information Security Policy (12.1)
  – Risk Assessment (12.2)
  – List (12.8.1)
  – Written agreement that acknowledges PCI responsibility (12.8.2)
  – Due Diligence (12.8.3)

• Compliance Responsibilities
  – Monitor compliance (12.8.4)
  – Maintain list of PCI DSS requirements (12.8.5)

• Change Notification

• Incident Response (12.8.3, 12.10)
ASSESSMENT
Assessments: Documents

- List of TPSPs with description
- TPSP control responsibilities
  - Responsibility Matrix
- Attestation of Compliance (AOC)
  - ROC (optional: May be partial or redacted)
- Other Evidence
  - Agreements/templates
  - Risk assessment
Assessment: Environmental Scope

- People – TPSP contractors or roles
- Process – TPSP services
- Technology – TPSP systems
- In Scope
  - CDE
  - Security Affecting Systems
  - Connected-to Systems
- Segmentation
- Applicable Product / Service / Delivery model (see AOC)
### Assessment: Environmental Scope

**List of Service Providers**

<table>
<thead>
<tr>
<th>TPSP Name</th>
<th>Description of Service Provided (12.8.1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Vendor</td>
<td>Place a detailed description here of the service that the TPSP is providing. This is a requirement under PCI DSS requirement 12.8.1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PCI DSS Scope Impact</th>
<th>People (Outsourcing)</th>
<th>Processes (Services)</th>
<th>Technology (Systems)</th>
<th>In Scope for PCI DSS?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>List TPSP people or roles (e.g., contractors) that have access to CHD, to the CDE, or whose roles impact the security of the CDE.</td>
<td>List TPSP processes (e.g., services) that store, process, transmit, or impact security of CHD.</td>
<td>List TPSP technologies that store, process, transmit, or impact security of CHD.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Sample list template available for download at [https://www.controlscan.com/TPSP-Management](https://www.controlscan.com/TPSP-Management)
Assessment: Control Scope

• Is Function providing Security Control?
• Did they meet it, or deem it N/A
• How are you monitoring that TPSP is meeting control (12.8.4)?
• Is Responsibility Matrix provided? If not, you must create (12.8.5)

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.8.4 Maintain a program to monitor service providers’ PCI DSS compliance status at least annually.</td>
</tr>
<tr>
<td>12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.</td>
</tr>
</tbody>
</table>
Attestation of Compliance

AOC
AOC: Part 2e

- Read the description

<table>
<thead>
<tr>
<th>Part 2e. Description of Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide a <strong>high-level</strong> description of the environment covered by this assessment. For example:</td>
</tr>
<tr>
<td>- Connections into and out of the cardholder data environment (CDE).</td>
</tr>
<tr>
<td>- Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.</td>
</tr>
</tbody>
</table>

ACME Service Provider Inc. provides data center services for its clients, and the physical security of said data center. However, it doesn’t manage the network configuration of the client’s routing devices, doesn’t manage the logical security services or log monitoring, and certainly doesn’t manage the storage of cardholder data.
AOC: Part 2a

- View service names and types
AOC: Part 2g

- Every N/A must be noted
- What is N/A for the TPSP may not be N/A for the merchant
- It is the merchant’s responsibility to compare these controls against PCI DSS

Conexxus: Sharing Responsibilities: Applicability of PCI DSS Requirements for Merchants and MNSPs
### AOC: Part 2f

- **PA-DSS software services: confirm QIR**

<table>
<thead>
<tr>
<th>Part 2f. Third-Party Service Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your company have a relationship with a Qualified Integrator &amp; Reseller (QIR) for the purpose of the services being validated?</td>
</tr>
</tbody>
</table>

**If Yes:**

<table>
<thead>
<tr>
<th>Name of QIR Company:</th>
<th>Best Ever Integrator and Reseller</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIR Individual Name:</td>
<td>Ira Sellers</td>
</tr>
<tr>
<td>Description of services provided by QIR:</td>
<td>Best Ever performs the installation of all PA-DSS software on behalf of ACME Service Provider, Inc.</td>
</tr>
</tbody>
</table>
AOC: Part 3

• Is AOC compliant?

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 1/1/2019.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (check one):

☑ Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby [Merchant Company Name] has demonstrated full compliance with the PCI DSS.

☐ Non-Compliant: Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby [Merchant Company Name] has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance: __________

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. Check with your acquirer or the payment brand(s) before completing Part 4.

☐ Compliant but with Legal exceptions: One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

If checked, complete the following:

<table>
<thead>
<tr>
<th>Affected Requirement</th>
<th>Details of how legal constraint prevents requirement being met</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Responsibility Matrix

• May or may not be provided by TPSP
  – Not required
  – AOC Part 2g provides sufficient information to inform conversation

• In lieu of responsibility matrix:
  – TPSP agreement must specify (12.8.2)
  – Controls maintained by Merchant (12.8.5)
## Responsibility Matrix

### PCI DSS v3.2.1 TPSP Responsibility Matrix

<table>
<thead>
<tr>
<th>Requirement</th>
<th>TPSP Name</th>
<th>Applicable? (e.g., based on ISG eligibility)</th>
<th>TPSP Only</th>
<th>Entity Only</th>
<th>Shared</th>
<th>Specific coverage/ scope of entity responsibility</th>
<th>Specific coverage/ scope of TPSP responsibility</th>
<th>How and when TPSP will provide evidence of compliance to entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 1: Install and maintain a firewall configuration to protect cardholder data</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
</tr>
<tr>
<td>1.1 Establish and implement firewall and router configuration standards that include the following:</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
<td>[Details]</td>
</tr>
<tr>
<td>1.1.1 Formal process for approving and testing all network connections and changes to the firewall and router configurations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.1.3 Current diagram that shows all cardholder data flows across systems and networks</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.1.5 Description of groups, roles, and responsibilities for management of network components</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.1.7 Requirement to review firewall and router rule sets at least every six months</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Note:</strong> An untrusted network is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1.2.2 Secure and synchronize router configuration files.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Sample responsibility matrix available for download at [https://www.controlscan.com/TPSP-Management](https://www.controlscan.com/TPSP-Management)
Managed Network Service Providers

MNSP
MNSP – Remote Access

Conexxus: Sharing Responsibilities: Applicability of PCI DSS Requirements for Merchants and MNSPs
MNSP – CHD Flow
MNSP PCI DSS Responsibilities

• 1 – Firewalls
  (both hosted and on-premises)
• 8.1, 8.3, 8.5 – Managing vendor IDs and remote access to environment
Possible MNSP Responsibilities

• 4 – Encryption for CHD communications from site to processor
• 6 – Custom application for conversion of cardholder data to the payment host
• 10 – May perform logging and monitoring
• 11 – May perform external and internal network testing
SHARED Responsibilities

MNSP and merchant each...

- 2 – Securely configure respective systems
- 4 – Encrypt CHD on respective networks
- 5 – Have antimalware on applicable systems
- 6 – Have secure software (e.g., PA-DSS)
- 10 – Track and monitor respective systems
Merchant Responsibilities

• 1.4 – Personal firewalls
• 3 – Protect cardholder data
• 7 – Access control responsibilities
• 9 – Physical security
• 11 – Testing
• 12 – Risk management and infosec policies
• 12.8.9 – One-time support password
• Website: www.conexxus.org
• Email: info@conexxus.org
• LinkedIn Profile: Conexxus.org
• Follow us on Twitter: @Conexxusonline
DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.