Visa Level 4 Merchant Requirements
PCI DSS Validation &
QIR Technician Requirements
Effective January 31, 2017

Presenter:
Stewart Fey
Qualified Security Assessor
LBMC Security
Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A
Housekeeping

This webinar is being recorded and will be made available in approximately 30 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

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

Speaker

Stewart Fey, CISSP, CISA, QSA
Qualified Security Assessor
LBMC Security
sfey@lbmc.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
# Conexxus Webinar Schedule

<table>
<thead>
<tr>
<th>Month</th>
<th>Subject</th>
<th>Speaker(s)</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2017</td>
<td>How Stores Comply with Updated PCI Version</td>
<td>Tabitha Greiner, Kimberly Ford, Branden Williams</td>
<td>Acumera Valero DBA, CISSP, CISM</td>
</tr>
<tr>
<td>March 2017</td>
<td>SIEM Presentation</td>
<td>Matt Bradley</td>
<td>EchoSat</td>
</tr>
<tr>
<td>April 2017</td>
<td>Internet of Things &amp; Impact of Bring Your Own Device to the Workplace</td>
<td>Bradford Lowey, Jeff Gibson</td>
<td>Wayne Fueling EchoSat</td>
</tr>
<tr>
<td>May 2017</td>
<td>Customer Engagement Technologies to Enhance Sales and Profitability</td>
<td>Ed Collupy, Gray Taylor, Lesley Saitta</td>
<td>W. Capra Conexxus Impact 21</td>
</tr>
</tbody>
</table>

If you have a suggestion for a webinar, please contact Conexxus at info@conexxus.org.
2017 Conexxus Annual Conference
Loews Annapolis Hotel
Annapolis, Maryland
April 23 – 27, 2017
Agenda

• What is PCI Compliance?
• New Visa Requirements effective (Jan 31)
  – PCI QIR Program Overview
  – Visa new requirements to use PCI QIRs
  – How small merchants can comply
  – Enforcement and Penalties
  – PCI Validation Requirements for small merchants
  – VISA TIP program Overview
  – Benefits of using P2PE and Chip Readers
• PCI 3.2 Update
• Q&A
What is PCI?

• Commonly called PCI DSS – Stands for: “Payment Card Industry Data Security Standard”

• Industry security rules set by the major card brands to protect credit card information
Who Are the PCI Players?

• **The Payment Brands**
  – American Express, Discover, JCB, MasterCard, and VISA
  – Define compliance programs and enforcement
  – Assess fines & penalties

• **PCI Security Standards Council**
  – Maintain the PCI DSS standard
  – Gatekeepers for Qualified Security Assessor (QSA) and other PCI certifications
Who Are the PCI Players (con’t)?

• **Acquirers (Merchant Bank)**
  – Processes merchant payment card transactions
  – Responsible for merchant compliance with PCI DSS

• **Oil Brands**
  – Have contractual relationship with C-Store franchisees
  – Direct relationship with acquirers/POS vendors
Who Are the PCI Players (con’t)?

- **Merchants (C-Store Operators) & Service Providers**
  - Accept Credit Cards
  - Store/Process/Transmit Card Data
  - Must Comply with PCI Rules
What Does PCI Protect?

Protected Cardholder Data

1. The Full Contents of the Magnetic Stripe
2. The Credit Card Number
   - Also known as the PAN or Primary Account Number
3. Cardholder Name
4. The Card Security Code (aka: CVV2, CVC2 or CID)
5. The Expiration Date

PCI DSS allows the retention of certain parts of Cardholder Data, but not other parts.
PCI Data Security Standards Overview

- The PCI Data Security Standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect credit card data.

- The standard is divided into 12 requirements outlining different aspects of security best practices.

- The standard requires compliance with approximately 330 individual security validation procedures.
  - 100% compliance required to pass
  - Compensating controls can be utilized when necessary and appropriate
Who Has to Comply With PCI DSS?

- All merchants and service providers who store, transmit, or process credit cards must comply with all requirements.
  - A merchant cannot outsource its PCI DSS responsibility
  - Merchants CAN outsource operational responsibility for maintaining security controls

- The card brands have outlined various reporting levels based on volume of card transactions.
  - Acquirer will determine a merchant’s reporting level and reporting obligations
  - Merchant may have more than one acquirer (merchant ID)
What's The PCI QIR Program?
PCI QIR Program Overview

• QIR stands for - Qualified Integrators and Resellers

• The QIR Program simplifies the process for identifying and engaging integrators and resellers qualified to help merchants install POS applications and terminals securely.
New Requirements!

• As of January 31, 2017 - All Level 4 merchants must use a PCI certified QIR for POS app and terminal installs, integrations, and maintenance.

• As of January 31, 2017- All level 4 merchants must annually validate PCI DSS compliance or participate in the TIP program.
Who Does This Apply To?

• Level 4 Merchants in the US and Canada
  – Generally small merchants
  – Process less than 20,000 VISA or MC e-commerce transactions
  – Process up to 1 million VISA transactions

Your bank/acquirer/oil brand will inform you of your level
How Can A Small Merchant Comply?

• Only hire QIR companies listed on the PCI SSC website https://www.pcisecuritystandards.org

(Note: Merchants are not required to use a QIR if they do the work in-house)
What Happens If I’m Not In Compliance?

• Subject to non-compliance fines (up to your acquirer)

• **Good News!** – VISA will not enforce compliance against individual merchants
Level 4 Merchants Must Annually Validate PCI Compliance (New)

Every year:
- Complete a self assessment questionnaire (SAQ)
- Submit an attestation of Compliance (AOC)

Every Quarter:
- Conduct a quarterly external vulnerability scan by an approved scan vendor (ASV)
Do I Have to Validate PCI Compliance?

• Short answer – Yes

• VISA’s TIP Program excludes a merchant from annual compliance requirements
How Does An Organization Prove Compliance?

That depends on your reporting level...

Shown from least painful to most painful:
• Self Assessment Questionnaire (SAQ)
  – 11 different versions based on type of processing
• Results from an Approved Scanning Vendor (ASV)
• Qualified Security Assessor (QSA) Report on Compliance (RoC)

“SAQ-D” most likely applies to C-Store franchisees
Where Do I Start?

• Your Acquirer/Bank/Oil Brand will tell you what you must do

• PCI Council’s Website – Small Business Section
  https://www.pcisecuritystandards.org
What is VISA’s TIP Program?

- Technology Innovation Program (TIP)
  - Encourages merchants to pursue EMV and P2PE solutions
Qualifying for TIP

• 75% of all transaction originate via EMV capable card readers or a validated P2PE solution

• Confirm sensitive authentication data is not stored after card authorization

https://usa.visa.com/support/small-business/security-compliance.html
PCI Security 101 – P2PE
PCI Security 101 - EMV

"OVER 1,500,000,000"
PCI DSS Version 3.2

• PCI updates its requirements every 3 years (regularly).

• Starting Nov 1st 2016 everyone must be using the new requirements in version 3.2.

• Several "big impact” changes.
Multi-factor Authentication

• All admin type access must use multi-factor authentication
Merchant / Service Provider Relationship

• You can’t totally outsource PCI Compliance…

• Service Provider as part of its compliance process must identify the PCI Controls it is providing on behalf of a Merchant (and vise versa)
February 2017 @ 12:00 Eastern: How Stores Comply with Updated PCI Version