How Stores Comply with Updated PCI Version

Presenters:
Kimberly Ford
Tabitha Greiner
Dr. Branden R. Williams
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
Kimberly Ford
Manager, IS
Valero Marketing & Supply

Speakers
Tabitha Greiner
CSO
Acumera, Inc

Dr. Branden R. Williams
Director, Cyber Security
Union Bank
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&lt;br&gt;Kimberly Ford&lt;br&gt;Branden Williams</td>
<td>Acumera&lt;br&gt;Valero&lt;br&gt;Union Bank</td>
</tr>
<tr>
<td>March 16 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&lt;br&gt;Jeff Gibson</td>
<td>Wayne Fueling&lt;br&gt;EchoSat</td>
</tr>
<tr>
<td>May 2017</td>
<td>Customer Engagement Technologies to Enhance Sales and Profitability</td>
<td>Ed Collupy&lt;br&gt;Gray Taylor&lt;br&gt;Lesley Saitta</td>
<td>W. Capra&lt;br&gt;Conexxus&lt;br&gt;Impact 21</td>
</tr>
</tbody>
</table>

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

- Fundamentals of PCI Compliance
- The realities of achieving and maintaining compliance
- Strategies and technologies to better secure CHD and ease complexities
Who does the PCI DSS apply to?

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data.
Who does the PCI DSS apply to?

Service Providers (definition): Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.
## Key Players

<table>
<thead>
<tr>
<th>PCI Security Standards Council (SSC)</th>
<th>Payment Brands/Banks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards Body</td>
<td>Enforcement and Tracking</td>
</tr>
<tr>
<td>Education and Certifications</td>
<td>Penalties, Fees, and Deadlines</td>
</tr>
<tr>
<td>Documentation, Guidance, FAQs</td>
<td>Data Compromises</td>
</tr>
</tbody>
</table>
# PCI DSS Key Dates

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2016</td>
</tr>
<tr>
<td>Retirement of 3.1</td>
<td>October 31, 2016</td>
</tr>
<tr>
<td>Best Practices - Requirements</td>
<td>January 31, 2018</td>
</tr>
<tr>
<td>SSL/Early TLS</td>
<td>June 30, 2018*</td>
</tr>
</tbody>
</table>
Observations

- Incremental Updates – Expect More?
- SSL Date Updates
- Multi-factor – New Guidance Released
- Small Merchant Guide
PCI DSS 3.2 – New Requirements

ALL
- 6.4.6 Ensuring continuous compliance
- 8.3.1 Multi-factor for admin

Service Providers
- 3.5.1, 10.8, 10.8.1, 11.3.4.1, 12.4.1, 12.11, 12.11.1
Compliance vs. Validation
Compliance vs. Validation - Breaches
Brand Relationships

If you have a relationship with an oil brand:

- Make sure you understand your contractual requirements in regards to PCI Compliance
- Ask them if they have any PCI related programs or recommendations
- Some oil brands have recommended vendors, some have required vendors, some directly resell
Realities – Achieving Compliance

Efforts to Comply

– $$$ for hardware, software, services
– Human capital
– On-going costs/Continuous compliance
Realities – Maintaining Compliance

Maintaining compliance is even harder

Verizon 2015 PCI Compliance Report
Memorable Quote

“We are but one change control away from non-compliance.”
Strategies

• Outsourcing

• Devalue Data

• Simplification
Technologies - Tokenization

Use Tokens instead of PAN

– Scope, architect, and implement properly
– Remove PAN data
– All ops done on token
– Scope reduced to Terminal
Technologies - Encryption

Point to Point Encryption (P2PE) Defined
Technologies - Mobile

ApplePay, SamsungPay, AndroidPay
- Similar to EMV, but possibly cheaper interchange!
- Requires equipment upgrade

Conexxus Mobile Standard
- Mobile Application on Consumer Device
- Service Provider handles CHD
March 16, 2017 @ 12:00PM Eastern: SIEM Presentation