PCI compliance: v3.1
Key Considerations

Corbin Del Carlo
Director, National Leader PCI Services
October 5, 2015
Today’s Presenter

Corbin Del Carlo QSA, PA QSA
Director, National Leader PCI Services Practice
847.413.6319
Corbin.delcarlo@mcgladrey.com
Objectives

• How PCI compliance affects your industry and organization
• New requirements and changed requirements, that could drastically impact your compliance efforts
• Guidance on how to provide the highest level of security for confidential data while still implementing efficient payment card processes
• Impact of Chip cards on your organization
“The world isn’t run by weapons anymore, or energy, or money. It’s run by little ones and zeroes, little bits of data. It's all just electrons.”

Cosmo – Sneakers 1992
What drives PCI compliance?

- Hackers and large international organized crime syndicates
- Higher monthly fees for non-compliance
- The fallout of a data breach:
  - The fallout can be significant, including fines/penalties, termination of your ability to accept payment cards, lost customer confidence, legal costs, settlements and judgments, fraud losses, etc.
  - A breach could result in a cost of, on average, $200 per card number lost.
- Knowing what data you have and where it resides
Queenbee
Seller
Level 1

Vendor is on vacation, he will handle your order/s later.

Created January 22 2015
Logged September 3 2015

Description

Vendor is on vacation, he will handle your order/s later.
Fraud cycle

How do the Criminals Make Money?

- Cards Purchased online
- Cloned Cards Created
- Buy Stuff (gift cards, luxury items, anything with high resale)
- Keep goods or resell for cash
- Profit!

- craigslist
- eBay
- Pawn shop
How does this effect NFP industry

- Significant Reputational Risk
- Lots of recurring membership or donation payments which can require significant CHD storage
- Funding is difficult to obtain or allocate for internal projects
- Mobile payments at conferences or events
- Legacy Paper records
Differences between version 2 and 3.1

- Version 3.1 released in April, mandatory for all assessments after June 30, 2015
  - Version 3.0 mandatory since January 2015
- Total changes – 114 modified requirements
  - Clarifications – 92 changes
  - Additional guidance – 8 changes
  - Evolving requirement – 14 changes
- 16 new requirements – all fit into one of the above categories
- Most of the changes in version 3 were “clarifications” of the version 2 requirements (83%)
- These were already requirements
  - Wording just “codifies” the requirement
Clarifications that organizations struggle with

- E-Commerce Scoping whitepaper
  - Published in January 2013
  - Clarifies the scope of PCI DSS in relation to e-commerce apps
  - Most importantly pulls redirect systems into scope.
  - SAQ exceptions

- [http://bit.ly/1Lg1NXO](http://bit.ly/1Lg1NXO)

Images courtesy of PCI SSC Information Supplement – PCI DSS E-Commerce Guidelines
Clarifications that organizations struggle with (cont.)

- Requirement 3.4 Mixture of Hash and Truncation (tokens)
  - Additional controls are required if both the hashed and the truncated tokens are present in the same system
    - If the organization is using tokens, what are those tokens?
    - See Council’s token guidance
  - Requirement 6.4.1 separation environments
    - Prod and dev must be segregated by logical access controls
    - No developers are to have access to prod (change/write/update/modify)
Clarifications that organizations struggle with (cont.)

- Requirement 10.2.1 Audit access to CHD
  - Requirement that all individual user access to CHD must be logged and included in the audit trails
  - No shared accounts without some other control
- Requirement 10.6 daily log reviews
  - Clarified that log reviews should identify suspicious activity or anomalies
  - Allows risk management strategy to be applied to the logs reviewed
  - Actually a bit easier but almost (always) requires a SIEM
Significant new requirements (not all)

- **Scope of assessment**
  - Evidence that card holder data only resides in the card holder data environment.
    - Proof via Data flow documentation
    - Interviews with business process owners
    - Automated scans at perimeter points
    - Proof of data containment

3.1 *Assessor’s validation of scope accuracy*

Document how the assessor validated the accuracy of the PCI DSS scope for the assessment, including:

- The methods or processes (for example, tools, observations, feedback, scans, data flow analysis) used to identify and document all existences of cardholder data:

- The methods or processes (for example, tools, observations, feedback, scans, data flow analysis) used to verify that no cardholder data exists outside of the ODE scope defined for this assessment.

- How the results of the methods/processes were evaluated to verify that PCI DSS scope is appropriate.

- How the results of the methods/processes were documented (for example, the results may be a diagram or an inventory of cardholder data locations):

- Why the methods used for scope verification are considered by the assessor to be effective and accurate:

- Provide the name of the assessor who attests that the scope of the assessment has been verified to be accurate and appropriate.
Significant new requirements (cont.)

• Requirement 2.4 – Inventory of systems
  • Inventory was part of scoping before, not as a specific requirement
  • Inventory will have to be very detailed
    • Include all system components that touch or support CHD processes

Image courtesy of PCI SSC
Significant new requirements (cont.)

• Requirement 4.1
  • SSL no longer considered a Secure Protocol
  • TLS - must migrate to TLS 1.2 or have plan to do so by June 2016

• Requirement 5.1.2
  • Protect all systems against malware
  • Exception for systems that are not considered to be commonly affected by malicious software has been modified
    • Target Malware on POS
    • MacOS Safari Bugs
    • Android Malware
  • Must be evaluated periodically (annually)
Significant new requirements (cont.)

• Requirement 8.5.1
  • Service Provider requirement for unique authentication for remote access at each customer premise
    • As a merchant this will have to be part of your acknowledgement/agreement

• Requirement 8.6 – unique token authentication
  • If using authentication such as physical tokens, smart cards, certificates, etc., the devices must be uniquely assigned
  • Each must only identify one user
    • Validate audit trail, provide non-repudiation
Significant new requirements (cont.)

• Requirement 9.9 – protect capture devices
  • All devices that capture payment data (PIN PADs, Card swipes, CHIP readers, etc.) must have unique tamper proof stickers
    • Periodic review of all stickers to validate “not broken or equipment substituted”

• Requirement 11.3 – Pen-testing methodology
  • Methodology has to be documented and based on industry standard (such as NIST SP800-115) and include current threats and vulnerabilities
  • Has to include the CDE perimeter and critical devices
  • Has to validate any segmentation or scope reduction controls used to reduce the scope of the assessment
  • Retention of remediation documentation
  • http://bit.ly/1NrH5pt
Significant new requirements (cont.)

• Requirement 12.8.5 – Vendor Management
  • Merchant must maintain information of which PCI DSS requirements are managed by each servicer provider or by the entity
  • Responsibility matrix
  • MORE than just contractual language
  • Organization may need to determine if TPSP meets PCI DSS requirements, depending on services provided

• Requirement 12.9 – vendor acknowledgement
  • Service providers must provide and merchants must obtain written acknowledgement of responsibilities discussed in 12.8
Significant new requirements (cont.)

- Matrix example:

<table>
<thead>
<tr>
<th>PCI DSS Requirement</th>
<th>RESPONSIBILITY</th>
<th>SPECIFIC COVERAGE/SCOPE OF THE ENTITY RESPONSIBILITY</th>
<th>SPECIFIC COVERAGE/SCOPE OF THE TPSP RESPONSIBILITY</th>
<th>HOW AND WHEN THE TPSP WILL PROVIDE EVIDENCE OF COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Establish and implement firewall and router configuration standards that include the following:</td>
<td>TPSP ONLY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.</td>
<td>ENTITY ONLY</td>
<td></td>
<td></td>
<td></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>SHARED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3 Current diagram that shows all cardholder data flows across systems and networks.</td>
<td>TPSP ONLY</td>
<td></td>
<td></td>
<td></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>ENTITY ONLY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.5 Description of groups, roles and responsibilities for logical management of network components.</td>
<td>SHARED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.6 Documentation and business justification for use of all services, protocols and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols or ports include, but are not limited to, FTP, Telnet, POP3, IMAP and SNMP v1 and v2.</td>
<td>TPSP ONLY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.7 Requirement to review firewall and router rule sets at least every six months.</td>
<td>ENTITY ONLY</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SAQ CLARIFICATIONS
<table>
<thead>
<tr>
<th>SAQ</th>
<th>Description</th>
</tr>
</thead>
</table>
| A   | Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises.  
*Not applicable to face-to-face channels.* |
| A-EP* | E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn’t directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises.  
*Applicable only to e-commerce channels.* |
| B   | Merchants using only:  
  - Imprint machines with no electronic cardholder data storage; and/or  
  - Standalone, dial-out terminals with no electronic cardholder data storage.  
*Not applicable to e-commerce channels.* |
| B-IP* | Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.  
*Not applicable to e-commerce channels.* |
## SAQ v 3.1

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-VT</td>
<td>Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>P2PE-HW</td>
<td>Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>D</td>
<td><strong>SAQ D for Merchants:</strong> All merchants not included in descriptions for the above SAQ types.</td>
</tr>
<tr>
<td></td>
<td><strong>SAQ D for Service Providers:</strong> All service providers defined by a payment brand as eligible to complete a SAQ.</td>
</tr>
</tbody>
</table>

* New for PCI DSS v3.0
THE FUTURE OF PCI – HOW TO REDUCE RISK
EMV – Chip and PIN

• EMV - Europay, MasterCard and Visa
• October 1, 2015 date for having EMV (Chip) implemented
• Only Chip and Signature in USA
• Liability of loss shifts to lower technology
• Minimal PCI DSS impact
  • Consider:
  • Chip does not change PAN transmission
  • Are they going directly from POS to processor and not entering the network?
  • Card Not Present (eComm, Mail In, Phone, Fax) not impacted
• What are the costs to implement updated PINPAD/POS?
• Business perspective to update
EMV – Chip and Signature

- Confirm issuer and processor are ready for accepting Chip and signature
- Global Operations
  - Implement global, if you have not already done so
  - Implement in US
- P2PE – Point-to-Point Encryption – consider EMV as part of this solution
- Multiple initiatives:
  - Some organizations are in process of implementing as part of POS upgrade tasks
  - Some organizations are waiting to upgrade until it is time to replace POS devices
  - Some organizations are waiting to see if the date is pushed back for EMV solutions
  - EMV will move forward as a result of high rate of breaches. US does 24% of global card transactions and is currently the target of 70% of fraud activity.
P2PE

- P2PE ensures sensitive credit and debit card data is protected from first card swipe, while in transit to the payment processor where it is securely decrypted.
- Consider P2PE along with EMV as part of your solution.
Tokenization

• The process of replacing a credit card number with a unique set of numbers that have no bearing on the original data.
Mobile payments

• Mobile solutions are ok, if they meet PCI requirements
• PCI Council Mobile Guidance Published
• Additional guidance includes:
  • Securing Mobile Device
    • Physical
    • Logical
    • Malware controls
  • Securing the Payment Acceptance Solution
    • Prevent local storage of PAN
    • Merchant validation
    • Secure Receipts
• Risks:
  • Loss of mobile device could mean loss of payment information (physical security)
  • Capturing transmission of information
  • Securing the OS and checking for virus/malware
Mobile (cont.)

- Square solution or other type of external, approved reader or PED device
- PA-DSS application that connects through mobile solution
- P2PE solutions
- Many trying to provide the market with a solution
  - Telecoms
  - Merchants
  - Processors
  - Software providers

Questions?

My contact Info:

Corbin Del Carlo QSA, PA QSA, CISSP, CISA, CRISC
Director, National Leader PCI Services Practice
847.413.6319
Corbin.delcarlo@mcgladrey.com