MAXIMIZE COMPLIANCE BENEFITS OF PAYMENT ENCRYPTION

Tim Winston, Principal, Payment Processors & P2PE
AGENDA

• Coalfire At A Glance
• Solutions to Remove Payment Data From Your Environment
  – Retail
  – E-Commerce
  – Tokenization
  – Mobile payments
  – EMV
• Bottom Line: Minimum Risk and Compliance
• Questions
COALFIRE AT A GLANCE
COALFIRE AT A GLANCE

Who is Coalfire?

• Thought-leader and go-to advisor in the fast-growing cybersecurity market
• More than 1,400 customers across a broad set of industry sectors
• More than 500 employees in 12 locations in North America and Europe
• Backed by The Carlyle Group and The Chertoff Group

What do we do?

• A sophisticated portfolio of cyber risk advisory and assessment services
• Industry-leading ethical hacking and technical testing services
• Cyber engineering services for designing, integrating, monitoring, and optimizing security systems
• Cloud-based CoalfireOne™ enterprise risk and compliance platform, used by more than 800 clients
TIM WINSTON

Education + Certifications

Mathematics, University of Washington

- Certified Information Systems Security Professional (CISSP) – 2000
- Certified Information Systems Auditor (CISA) – 2011
- Payment Card Industry (PCI) Qualified Security Assessor (QSA) – 2010
- PCI Point-To-Point Encryption QSA (P2PE QSA) – 2013
- Visa PIN Security Assessor - 2016
SOLUTIONS TO MINIMIZE PAYMENT DATA IN YOUR ENVIRONMENT
STRATEGIES TO MINIMIZE PAYMENT DATA

• Encryption
• Tokenization
• Outsourcing
## SOLUTIONS TO MINIMIZE PAYMENT DATA IN YOUR ENVIRONMENT

<table>
<thead>
<tr>
<th>Payment Channel</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail, Kiosk, &amp; Phone</td>
<td>Point-to-Point Encryption</td>
</tr>
<tr>
<td>Retail and Kiosk</td>
<td>Mobile Payments</td>
</tr>
<tr>
<td>Web Commerce</td>
<td>E-Commerce Outsourcing</td>
</tr>
<tr>
<td>Recurring Payments</td>
<td>Tokenization</td>
</tr>
<tr>
<td>Off-line Payments</td>
<td>EMV</td>
</tr>
</tbody>
</table>
IMMORTAL MERCHANT DSS RESPONSIBILITIES

• Training
• Physical security of terminals
• Follow payment vendor instructions
• Vendor compliance
• Policies, risk, and scope management
• Monitoring
• Incident response
DSS SCOPE MANAGEMENT

• Number of systems that store, process, and/or transmit PAN/SAD
• Number of DSS controls applicable to a system
RETAIL SOLUTIONS
POINT-TO-POINT ENCRYPTION
ENCRYPTION: THE POINT OF INTERACTION

Hardware or firmware encryption immediately on swipe, chip read, or entry
DECRYPTION: THE OTHER POINT

- Bank or other Acquirer
- Payment Gateway
- Payment Service Provider
KEY MANAGEMENT: THE IMITATION GAME

- Key injection
- Asymmetric keys
- Derived Keys
- Identity Based Encryption
COMPLIANCE EFFORT WITH P2PE (LISTED VERSUS NON-LISTED)

Are non-PCI listed encryption solutions just as secure as PCI P2PE Solutions?

• No – most are much better than non-encrypting solutions
• Assurance of minimal security – Non-Listed Encryption Solution Assessment or other third party testing
• More solutions available – especially market specific
• Acquirer must agree annually to the reduction of controls proposed by the QSA

PCI P2PE provides a pre-validated solution for merchants.

• Limited certified solutions list doubled this year
• Healthcare, Higher Education, and Public Sector are leading
• (+) P2PE SAQ for merchants, Significant reduction of controls
E-COMMERCE OUTSOURCING
IFRAME PAYMENT FLOW

1. Show merchant shopping cart
2. Show merchant web page (no payment function)
3. Handle response received
4. Show results page

CUSTOMER BROWSER

Customers → Checkout → Buy

PAYMENT SOLUTION PROVIDER

Show payment page in iFrame
Authorize transaction
Send transaction result

Card data submitted to Payment Solution Provider
DIRECT POST PAYMENT FLOW

1. **MERCHANT ECOMMERCE INFRASTRUCTURE**
   - Show merchant shopping cart
   - Show payment page
   - Handle response received
   - Show results page

2. **CUSTOMER BROWSER**
   - Customers
   - Checkout
   - Buy
   - Order Processed

3. **PAYMENT SOLUTION PROVIDER**
   - Authorize transaction
   - Send transaction result

The process flows as follows:
1. The merchant shows the shopping cart.
2. The customer proceeds to checkout and orders a product.
3. Card data is submitted to the payment solution provider via TLS.
4. The transaction is authorized, and the results are sent back via TLS.
JAVASCRIPT FORM PAYMENT FLOW

1. Show merchant shopping cart
2. Payment page requests JavaScript to create payment form
3. JavaScript Code
4. Payment page
5. Card data (submitted via JavaScript)
6. Send transaction result

CUSTOMER BROWSER

MERCHANT ECOMMERCE INFRASTRUCTURE

- HTML for page (incl. payment form)
- Handle response received
- Show results page
TOKENIZATION
TOKENIZATION FLOW

1. Application (for example, POS) sends PAN.
2. Tokenization system requests authentication.
3. Token Generation generates a token.
4. Token and PAN are sent to the Card data vault.
DE-TOKENIZATION FLOW
EMV PAYMENTS
EMV PAYMENT FLOW

Consumer may enter a PIN (Chip + PIN), a signature or no factor based on limits or in contactless mode.

- Contact Interface
- Contactless Interface
- NFC
- Secure Element
  - SIM Card
  - In Phone, Fab, microSD

EMV System
- EMV Security Stack - Crypto
- Offline Mode
  - Authorization / Limits
- Online Mode

Payment Network
MOBILE PAYMENTS

• Still no Mobile standard for payment applications
• PCI guidelines and taskforce
• P2PE Tokenization Service Provider Standard
• FSISAC/PPISC voluntary guidelines
• Conexxus mobile working group
MOBILE PAYMENTS

1. I've got a card: 4111 1111 1111 1234
2. Here, use this instead: 4123 **** **** 9876
3. User goes shopping at Merchant
4. I'm paying with: 4123 **** **** 9876
5. Can you process this for me? 4123 **** **** 9876 $50.00
6. Hey, is this valid? 4123 **** **** 9876
7. 4123 **** **** 9876 = 4111 1111 1111 1234
8. Yep, all good!
9. Yep, all good!
10. This purchase was made using: 4111 **** **** 1234
BOTTOM LINE

• Security concerns are ever changing
• Cyber Risk should guide your security plans
• Know your technology and security partners, don’t check the box
• There is no silver bullet – If you take credit cards you have PCI DSS Compliance responsibilities (but you can have a lot less!)
QUESTIONS?

Tim Winston
tim.winston@coalfire.com