Payment Security & Risks: Controls and Processes for Securing Payment Transactions

November, 2017
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

Speakers

Terry Mahoney
Partner
W. Capra Consulting Group
tmahoney@wcapra.com

Clint Cady
Director of Payments
W. Capra Consulting Group
ccady@wcapra.com

Sam Schieber
Payments Consultant
W. Capra Consulting Group
sschieber@wcapra.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
# 2017 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>July 27, 2017</td>
<td>Third Party Risk Management: How to Identify and Manage Data Security Risks from your Vendors</td>
<td>Sam Pfanstiel</td>
<td>Coalfire Systems</td>
</tr>
<tr>
<td>August 31, 2017</td>
<td>Using the NIST Cybersecurity Framework to Guide your Security Program</td>
<td>Chris Lietz</td>
<td>Coalfire Systems</td>
</tr>
<tr>
<td>September 28, 2017</td>
<td>Things &amp; Impact of Bring Your Own Device to the Workplace</td>
<td>Bradford Loewy Jeff Gibson</td>
<td>Dover Fueling ControlScan</td>
</tr>
<tr>
<td>December 19, 2017</td>
<td>How Much Can You Save with Electronic Data?</td>
<td>Donna Perkins Mark Holloway</td>
<td>E-Z Stop Foodmarts Hammer Williams</td>
</tr>
</tbody>
</table>
## 2018 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>January 2018</td>
<td>Securing and Penn Testing your Mobile Payment App</td>
<td>TBD</td>
<td>Citigal</td>
</tr>
<tr>
<td>February 2018</td>
<td>Unified threat management: What is it and why is it important?</td>
<td>Thomas Duncan</td>
<td>Omega</td>
</tr>
<tr>
<td>March 2018</td>
<td>Penetration Testing: How to Test What Matters Most</td>
<td>Sam Pfanstiel &amp; Coalfire Lab Personnel</td>
<td>Coalfire</td>
</tr>
<tr>
<td>May 2018</td>
<td>QIR Program Update</td>
<td>Chris Bucolo</td>
<td>ControlScan</td>
</tr>
</tbody>
</table>
2018 Conexxus Annual Conference
Loews Chicago O’Hare
Chicago, Illinois
April 29 – May 3, 2018
Evolution of Payment Risk Management

Minimal
- PCI Compliance
- AVS/CVV Checks
- Velocity Checking
- ID Verification

Moderate
- EMV
- Encryption
- Tokenization
- Transaction Scoring

Proactive
- Consortium-Based Fraud Detection
- Security First Design
- Intrusion Detection and Prevention
Topics to Cover

1. 3 Questions to Consider
2. Transaction Risk Management
3. Data Security
4. Operational Integrity & Network Security
3 Questions to Consider

<table>
<thead>
<tr>
<th>Transaction Risk Management</th>
<th>Should I accept the transaction?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td>How do I protect the transaction details?</td>
</tr>
<tr>
<td>Operational Integrity &amp; Network Security</td>
<td>How do I secure consumer data and protect my environment?</td>
</tr>
</tbody>
</table>
Should I Accept The Transaction?

Your decision to accept a transaction is your **first line of defense** in managing payments risk

**Channels**
- CP, CNP, or Both?
- Attended or Unattended Devices
- ECom/Mobile

**Goods**
- Digital Goods
- Groceries
- Fuel
- Big Ticket Items
- Gift Cards

**Location**
- High/Low Fraud Regions
- Local Fraud Trends

**Consumer Experience**
- Speed of Service
- Frictionless Experience

**Risk Tolerance**
- High/Low Risk
- Liability Coverage

Organizations **must** consider these factors when developing a framework for transaction acceptance
What Controls Have Payments Systems Used to Date?

Authentication
Verification
Authorization
Authentication

The process in which the payment credential being used is checked for authenticity

Cash

Check for presence of anti-counterfeiting design elements in currency

Check

Validate MICR data encoded in check
Reference routing number against the financial institution listed

Card

Pre EMV: Check physical card for brand logos/hologram
Post EMV: Validate the card’s cryptogram

ACH

Perform a test deposit (pre-notes, micro-deposit) to ensure account is active
Validate account in real time using credential based access to customer’s bank

Conexxus: Payment Security & Risks: Controls and Processes for Securing Payment Transactions
Verification

The ability to verify that the individual initiating the transaction is the account owner or an authorized user

- **Cash**: N/A
- **Check**: Validate customer’s identify against another form of identification. Utilize electronic check acceptance/verification services.
- **Card**: Support of PIN entry where available. Utilize CVV, AVS, and 3DS for CNP. transactions.
- **ACH**: Validate customer’s access credentials when using a stored payment method online. Implement multi-factor authentication.
Authorization

The ability to validate the **availability of funds** and **transfer** them to the counterparty in the transaction

**Cash**

N/A

**Card**

Online Authorization to verify the availability of the customer’s funds in real time

**Check**

Funding made available by customer’s bank via overdraft loan
Re-presentation of the check by the merchant

**ACH**

Guarantee of funding (up to a certain dollar threshold) provided by some ACH processing providers
What Methods Can I Use?

An effective payments acceptance model should leverage both internal procedures and technology to mitigate the impact of fraudulent transactions.

### Procedures
- Cashier Training
- CVV/AVS Checks
- CVM Limits
- ID Verification
- Purchase Restrictions

### Technology
- EMV
- 3D Secure
- Real Time Transaction Scoring
- Account Monitoring
- Device Fingerprinting
- Customer History
- Consortium-Based Fraud Monitoring

Today, Procedural Methods are Favored, but Developments in Real-Time Monitoring Solutions are Advancing Quickly.

**1-3 Years**
- Tomorrow Comprehensive, Real-Time Approach

**Immediate**
- Today Advanced Merchant-Driven Approach
Challenges When Implementing

A successful design and implementation must avoid the following pitfalls

- Overly Restrictive Rules/Criteria = False Declines
- Increased Friction During Checkout = Customer Frustration
- Failure to Continuously Monitor and Update Scoring Rules/Criteria = Reduced Effectiveness Against Fraud Over Time
While there are many available solutions, a merchant’s architecture helps to define what will be the most effective.
Network Security – Future Risks

IoT Devices  Consumer WiFi  Business WiFi
### Network Security – IDS/IPS

<table>
<thead>
<tr>
<th>Intrusion Detection System (IDS)</th>
<th>Intrusion Prevention System (IPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detects</strong> – Identifies security threats</td>
<td><strong>Detects, Captures, and Reports</strong></td>
</tr>
<tr>
<td><strong>Captures</strong> – Logs information about incidents into SIEM solutions or centralized logging servers</td>
<td><strong>Blocks</strong> – Stops malicious traffic</td>
</tr>
<tr>
<td><strong>Reports</strong> – Summarizes monitored events and provide details on events of interest</td>
<td>• Terminates network connection or user session</td>
</tr>
<tr>
<td></td>
<td>• Blocks access to the target</td>
</tr>
<tr>
<td></td>
<td>• Reconfigures security controls</td>
</tr>
<tr>
<td></td>
<td>• Removes malicious content</td>
</tr>
<tr>
<td></td>
<td>• Applies patches</td>
</tr>
<tr>
<td></td>
<td>• Computationally intensive real time analysis</td>
</tr>
</tbody>
</table>
Software Defined Networking

Allows network administrators to **programmatically manage** network behavior dynamically via open interfaces and **provide abstraction** of lower-level functionality.
Defense in Depth

Encryption protects data from being observed and can be implemented at multiple layers

- **The Transport Layer using VPNs or other encrypted connections**: This prevents the data from being observed while moving across that connection, however data is still in clear text at any network node that is performing decryption/encryption

- **The Software Layer, typically with SSL/TLS**: This protects clear text data and provides an added layer of security on encrypted transport connections

- Security best practice is “Defense in Depth” - encrypt at multiple levels in case one gets compromised
Beyond Availability:
Protecting customer conversion, operations, and your brand by ensuring that critical systems are available **AND** performing within expected metrics.
Building Reliable Operations

Reliable Operations

- Monitoring, Alerting, & Controls
- Response Plans and Procedures
- Training & Continuous Improvement