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

November, 2017

CONEXXUS
solve forward

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

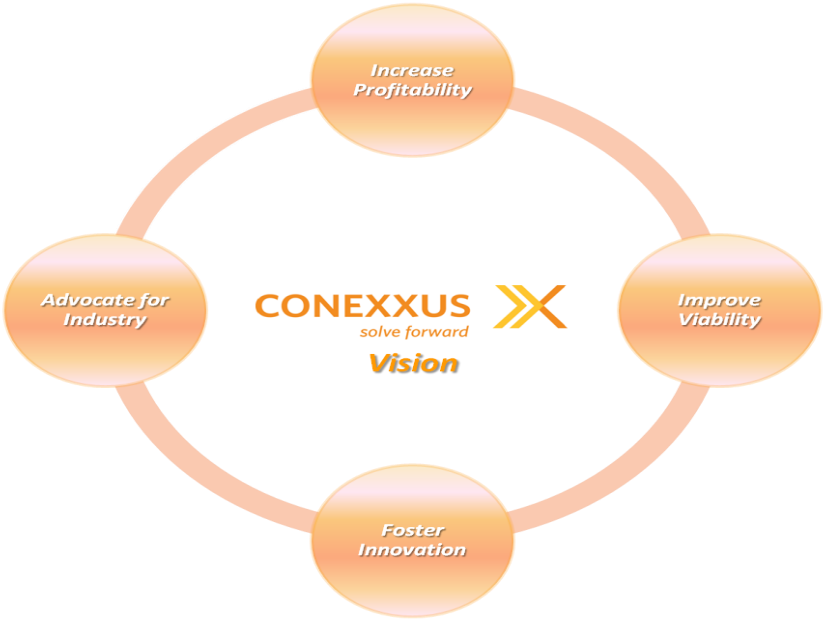
Terry Mahoney
Partner
W. Capra Consulting Group
tmahoney@wcapra.com

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*

Month/Date	Webinar Title	Speaker	Company
July 27, 2017	Third Party Risk Management: How to Identify and Manage Data Security Risks from your Vendors	Sam Pfanstiel	Coalfire Systems
August 31, 2017	Using the NIST Cybersecurity Framework to Guide your Security Program	Chris Lietz	Coalfire Systems
September 28, 2017	Things & Impact of Bring Your Own Device to the Workplace	Bradford Loewy Jeff Gibson	Dover Fueling ControlScan
November 28, 2017	Payment Security & Risks: Controls and Processes for Securing Payment Transaction	Terry Mahoney Clint Cady	W. Capra W. Capra
December 19, 2017	How Much Can You Save with Electronic Data?	Donna Perkins Mark Holloway	E-Z Stop Foodmarts Hammer Williams

CONEXXUS solve forward

2018 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
January 2018	Securing and Penn Testing your Mobile Payment App	TBD	Citigal
February 2018	Unified threat management: What is it and why is it important?	Thomas Duncan	Omega
March 2018	Penetration Testing: How to Test What Matters Most	Sam Pfanstiel & Coalfire Lab Personnel	Coalfire
May 2018	QIR Program Update	Chris Bucolo	ControlScan

2018 Conexxus Annual Conference

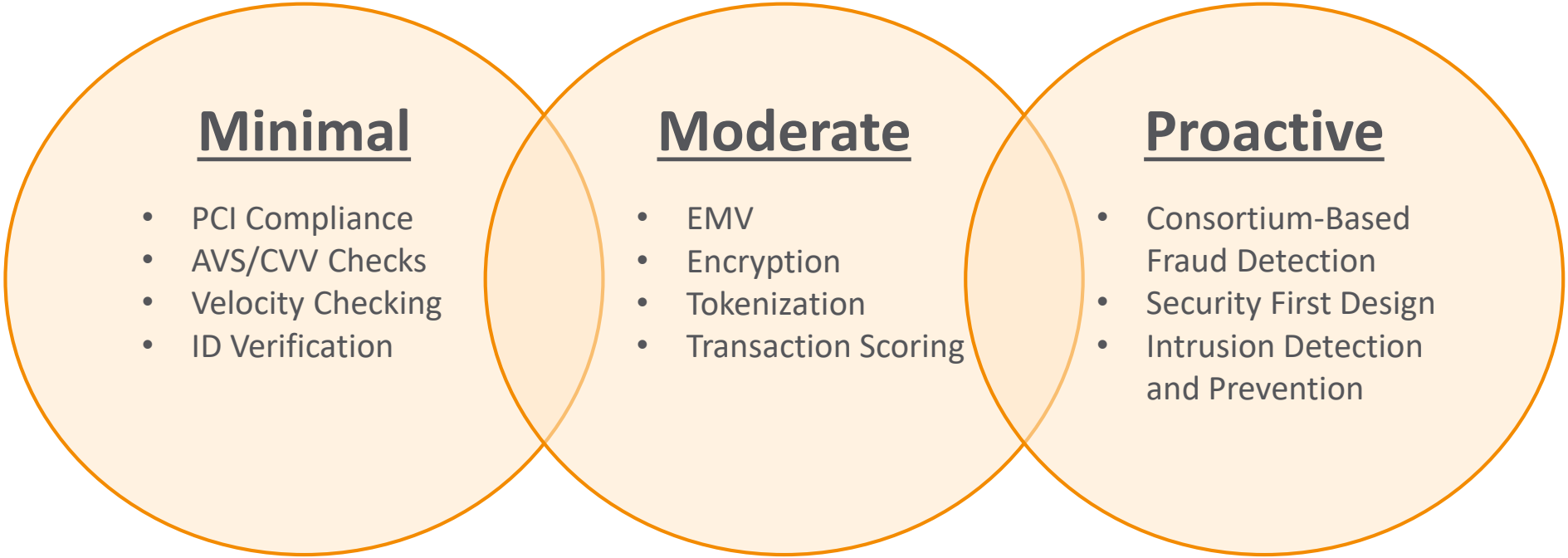
Loews Chicago O'Hare

Chicago, Illinois

April 29 – May 3, 2018

CONEXXUS solve forward

Evolution of Payment Risk Management



CONEXXUS solve forward

Topics to Cover

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

3 Questions to Consider

Transaction Risk Management

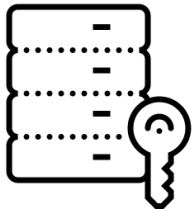
Should I accept the transaction?

Data Security

How do I protect the transaction details?

Operational Integrity & Network Security

How do I secure consumer data and protect my environment?



CONEXXUS solve forward

Should I Accept The Transaction?

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

Channels	Goods	Location	Consumer Experience	Risk Tolerance
• CP, CNP, or Both? • Attended or Unattended Devices • ECom/Mobile	• Digital Goods • Groceries • Fuel • Big Ticket Items • Gift Cards	• High/Low Fraud Regions • Local Fraud Trends	• Speed of Service • Frictionless Experience	• 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?

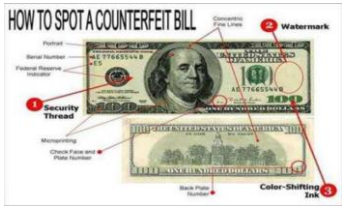
CONEXXUS
solve forward

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

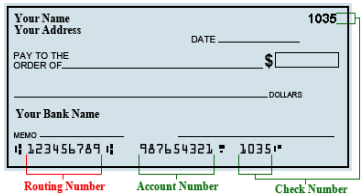


Card

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

Check

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



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

Verification

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

Cash

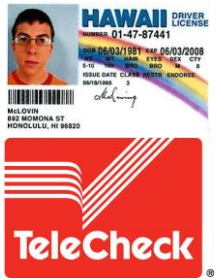
N/A

Card

Support of PIN entry where available
Utilize CVV, AVS, and 3DS for CNP. transactions

Check

Validate customer's identify against another form of identification
Utilize electronic check acceptance/verification services



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-presentment 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*

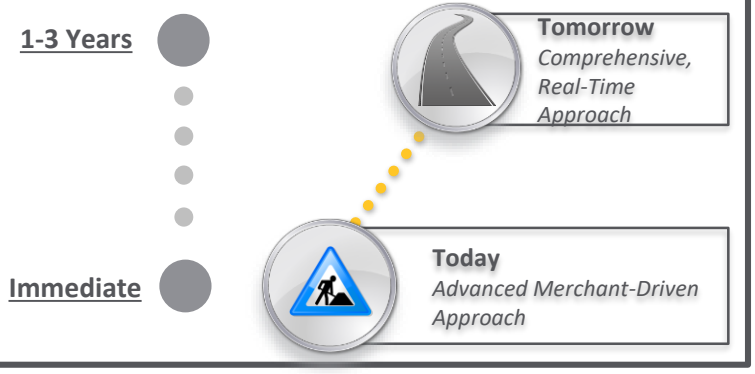
Procedures

- 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

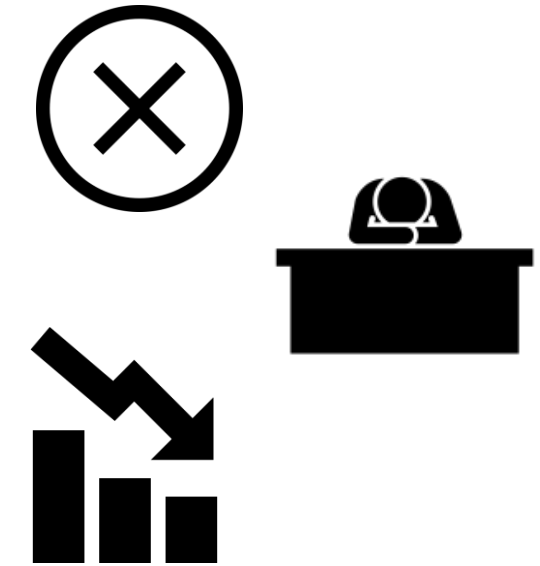


CONEXXUS solve forward

Challenges When Implementing

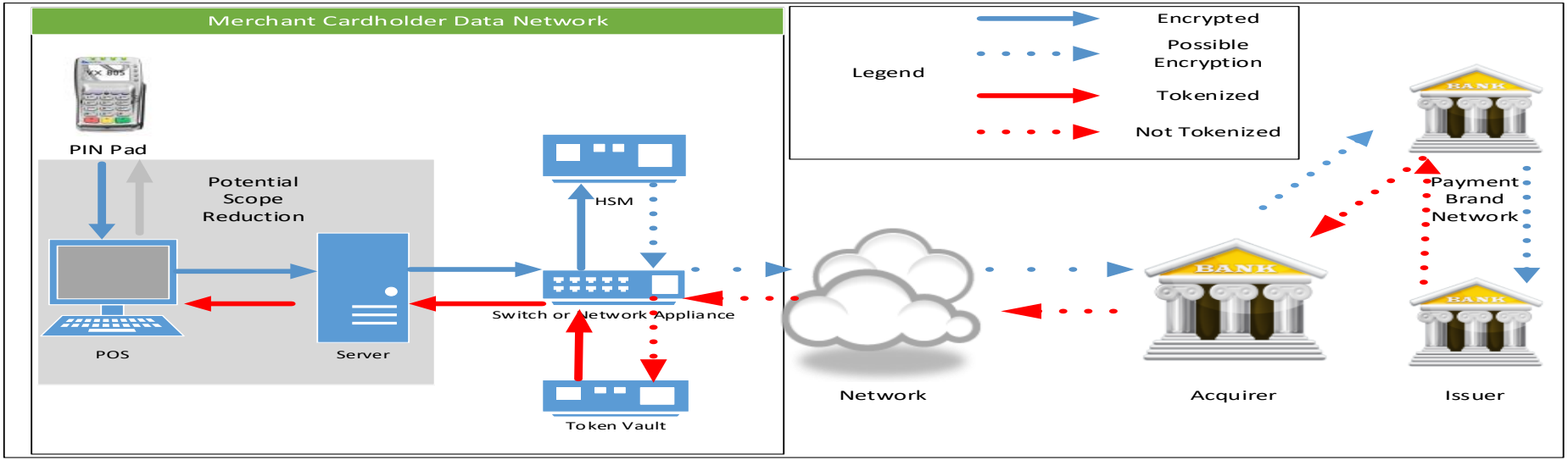
*A successful design and implementation **must avoid** the following pitfalls*

- **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**



Protecting Transactions

*Retailers are protecting transactions through the **encryption and tokenization of data***



While there are many available solutions, a merchant's architecture helps to define what will be the most effective

CONEXXUS solve forward

Network Security – Future Risks

IoT Devices

Consumer WiFI

Business WiFI

CONEXXUS solve forward

Network Security – IDS/IPS

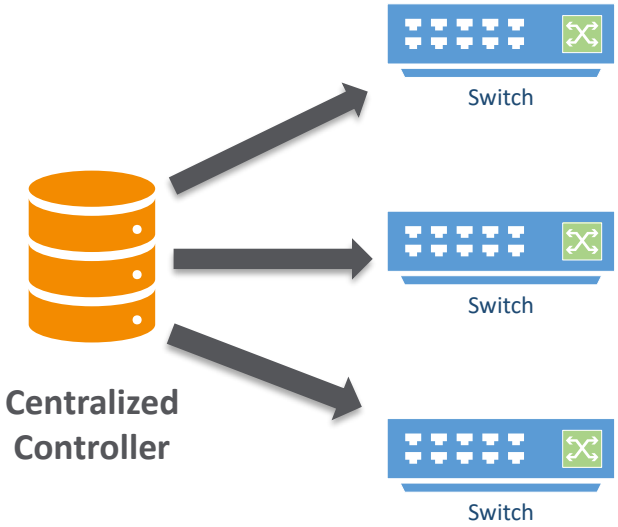
Intrusion Detection System (IDS)

- **Detects** – Identifies security threats
- **Captures** – Logs information about incidents into SIEM solutions or centralized logging servers
- **Reports** – Summarizes monitored events and provide details on events of interest

Intrusion Prevention System (IPS)

- **Detects, Captures, and Reports**
- **Blocks** – Stops malicious traffic
  - Terminates network connection or user session
  - Blocks access to the target
  - Reconfigures security controls
  - Removes malicious content
  - Applies patches
- Computationally intensive real time analysis

Software Defined Networking



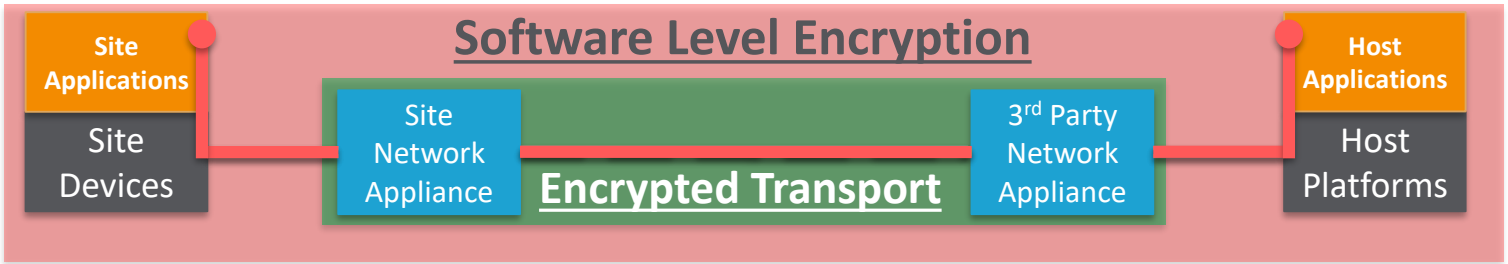
Allows network administrators to **programmatically manage** network behavior dynamically via open interfaces and **provide abstraction** of lower-level functionality

CONEXXUS solve forward

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



CONEXXUS solve forward

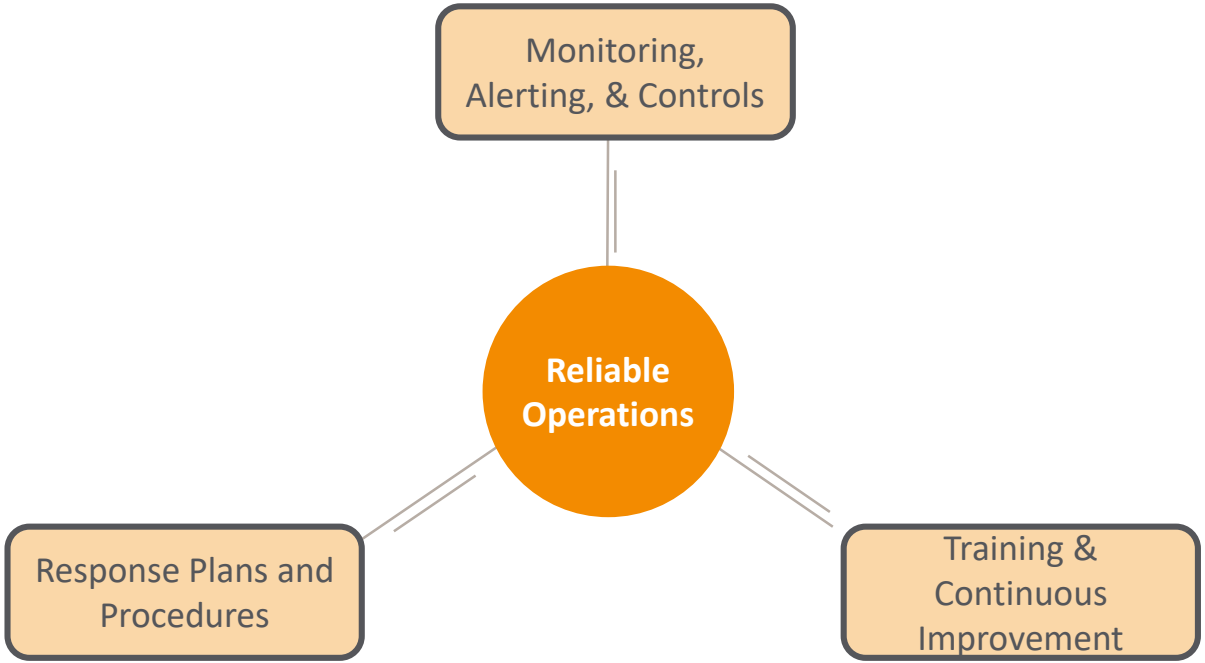
Operational Integrity

Beyond Availability:

Protecting customer conversion, operations, and your brand by ensuring that critical systems are available **AND** performing within expected metrics

CONEXXUS solve forward

Building Reliable Operations



CONEXXUS solve forward