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

Chris Bucolo
Director, Strategic Partnerships and Market Strategy
ControlScan
cbucolo@controlscan.com

Todd Rosen
Sr. Director, Petro Sales Support and Service
Verifone
todd.rosen@verifone.com
Today’s Speaker

- Conexxus Data Security Standards Committee
- NAMA Data Security Standards Committee
- PCI Council Small Merchant Task Force
- Merchant Acquirers’ Committee (MAC) Education Committee
- Frequent speaker and writer

Chris Bucolo, PCIP
Director, Strategic Partnerships & Market Strategy
ControlScan
Today’s Speaker

• More than 20 years’ experience in the industry.
• Responsible for VASC (Verifone Authorized Service Contractors)
• Responsible all Field Support and Training
• Involvement with QIR since 2015

Todd Rosen
Sr. Director, Petro Sales
Support and Service
Verifone Petroleum
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: QIR Review & Updates. May 24, 2018
## 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>May 24, 2018</td>
<td>QIR Program Update</td>
<td>Chris Bucolo</td>
<td>ControlScan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Todd Rosen</td>
<td>Verifone</td>
</tr>
<tr>
<td>June 21, 2018</td>
<td>Can We Leverage Data Science to Improve Retail Data Security?</td>
<td>Thomas Duncan</td>
<td>Omega ATC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ashwin Swamy</td>
<td>Omega ATC</td>
</tr>
<tr>
<td>July 26, 2018</td>
<td>Roadmap to a Vulnerability Disclosure Program</td>
<td>Joe Basirico</td>
<td>Security Innovation</td>
</tr>
<tr>
<td>August 23, 2018</td>
<td>Moving Toward Outdoor EMV</td>
<td>Linda Toth</td>
<td>Conexxus</td>
</tr>
<tr>
<td>September 2018</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>November 2018</td>
<td>Building a Scalable Security Engineering Team</td>
<td>Joe Basirico</td>
<td>Security Innovation</td>
</tr>
</tbody>
</table>
NACS Show
October 7-10, 2018
Las Vegas, NV

Conexxus thanks our 2018 Annual Diamond Sponsors!
Session Summary

• QIR Background & Evolution
• Review of Updated QIR program
• Why QIR Matters-Breach case
• FAQs/Resources
• Interactive Q & A Session
What is PCI QIR?

Payment Card Industry (PCI)
Qualified Integrator & Reseller (QIR)

Offers QIR Professional Qualification – a qualification for technicians who carry out PA-DSS POS installations and/or upgrades on behalf of merchants

QIR professionals must demonstrate their knowledge of critical security controls that mitigate the most common causes of loss of Cardholder Data arising from installations

QIR professionals must possess a base level of knowledge and awareness of information technology, network security and architecture consistent with QIR Program requirements and payment technologies

Source: www.pcisecuritystandards.org
Where are we today?

“Since 2014, there are 21 Active Petro Companies with QIR Certified Technicians”

• Why so few Companies and Technicians?
  – Industry Adoption
  – Cost was too high
  – Lack of Marketing
  – No “buy in” from the POS Providers, Manufacturers and Service Providers
  – Unable to combine Training Programs in place

• Recommendation and Plan
  – Create a MFR panel that would cover the majority of the POS and Software providers in Petro
  – Mandate that new Technicians and Certifications from the POS Providers include QIR

Conexxus Webinar: QIR Review & Updates. May 24, 2018
Service Contractor Update

- North America Petroleum Service Authorized Service Contractors are made up of about 500 Companies across the United States.
- The Count of Technicians servicing the landscape of Convenience Store and Fueling Sites is approximately 3,000 Full time “Career” Technicians
- Verifone is the largest POS Provider to this market with a 85% share of “Authorized Technicians”
- Verifone provides POS Software across all Major Brands and Networks

Conexxus Webinar: QIR Review & Updates. May 24, 2018
Updated QIR Program: Review and Discussion
Qualified Integrators & Resellers (QIRs)

“Numerous breach investigations have shown that incorrect installation and/or maintenance of payment applications creates opportunities for merchant networks to be compromised.

“This program outlines guiding principles and procedures for the secure installation and maintenance of validated payment applications in a manner that supports PCI DSS compliance.”
Updated QIR Program - As of 3/14/2018

**STREAMLINED CERTIFICATION**
for integrators and resellers:
- Reduced Cost
- Shorter Course Time
- Individual Certification

**FOCUSED TRAINING**
on the 3 leading causes of payment data breaches:
- Weak Password Practices
- Insecure Remote Access
- Unpatched and Outdated Software

**MERCHANDS BENEFIT by:**
- Increased Pool of Integrators and Resellers Trained in Critical Security Controls

Source: https://blog.pcisecuritystandards.org/the-qir-program-is-changing-heres-what-you-need-to-know

Conexxus Webinar: QIR Review & Updates. May 24, 2018
Updated QIR Program - as of 3/14/2018

3 Payment Data Security Essentials SMBs Shouldn’t Ignore

Attacks on POS systems at U.S. brick-and-mortar businesses are on the rise, leading to costly payment data breaches. Here are three essential data security practices SMBs should adopt now to minimize the risk of being breached:

#1 point of entry for attacks against brick-and-mortar merchants is insecure remote access*

Limit remote access by third party vendors. Businesses should talk to their vendors to make sure remote access to their systems is only turned on when needed, and that multi-factor authentication is being used.

* Remote Access Technology Best Practices

80% of hacking attacks could be prevented by strengthening passwords and installing software patches*

Install software updates or “patches”. Vendors regularly issue patches to fix software vulnerabilities. Businesses should apply these security patches to their systems as soon as they receive them.

* 2017 Verizon Data Breach Investigations Report

81% of hacking-related breaches leveraged either stolen and/or weak passwords*

Use strong passwords and change default ones. Computer equipment and software out of the box (including POS terminals) often come with default passwords such as “password” or “admin”. Businesses should change them to something hard to guess, update them regularly and never share them.

* 2017 Verizon Data Breach Investigations Report
Visa Clarifications on QIR

QIR Requirements **Do Not Apply to:**

- Vendors that support ancillary applications integrated into the POS systems, but which are **properly segmented from the payment processing operations**.

- Vendors providing **simple plug-and-play devices** for merchants which will not allow remote access into the POS environment. (Example: Counter-top credit card terminals)

- An acquirer or their affiliated business unit.

  → As a best practice, an acquirer may choose to complete the QIR certification in order to be included on the PCI SSC’s list of QIR companies, making it easy for merchants to identify their secure provider.

Source: Visa Bulletin-August 2016

Conexxus Webinar: QIR Review & Updates. May 24, 2018
Why QIR Matters-Breach Case

• Some large hospitality breaches involve multiple reseller companies across the USA. Because of Geography, the organization mandates a specific POS system that may have a different reseller in each major metro area.

• For some franchisees they may not know which local POS support company is better than the other.

• In this case, corporate had remote access to every store to gather nightly sales statistics and other data. 3 major US banks identified a large amount of fraudulent activity and demanded a PFI be conducted.
A Nationwide breach

**QIR**

- The QIR companies had a different password per each client location for their use, but unfortunately the attacker had corporate’s account.

- The QIR had outbound firewall rules that prevented the malware from exfiltrating data.

- The attacker then tried other malware tools but system patching prevented some of the older tools from working.

**Non-QIR**

- The attacker was able to exfiltrate data, but also installed a secondary remote control tool for later use (his backup plan).

- Logging was not preserved for a year so the franchisee could not argue the duration (months) of their breach.

- Because of their liability, this integrator “lawyered up” and would not assist in the PFI investigation.

Information provided by: Conexxus Webinar: QIR Review & Updates. May 24, 2018
A QIR has these traits over non-QIRs

• QIRs are usually more active in the industry. They network with other similar organizations. They stay in touch with new technology that may keep business costs down, but also prevent breaches.

• QIRs realize that security cannot be solely the job of the retailer. It’s difficult (these days) for a tech support organization to support a system and not be involved in its security.

• QIRs have often been through training that helps them understand “how to identify and respond” to data breach scenarios.

• QIRs are aware that the initial setup of a system is often where things go terribly wrong.
New QIR Program
Frequently Asked Questions

What are primary changes?
• Shorter course
• Individual level certification
• Lower cost/annual re-up
• Expanded to include non PA-DSS listed applications

What is new training course focused on? The Big Three
• Password strength
• Software patching
• Insecure remote access

What are the new fees? $100 per person (annual)
Updated QIR Program: Merchant Benefits
Merchant Benefits of Using QIR

- Proper installation & following PA-DSS Implementation Guide
- Understanding importance of properly securing POS
- Instills consistent knowledge of securing cardholder data
- Technician/QIR check-list for POS installation
- Installation technician name and sign-off for future reference
PCI Resources

- Website: [www.pcissc.org](http://www.pcissc.org)
- FAQs: [https://www.pcisecuritystandards.org/documents/QIR-Program-Update-FAQs.pdf](https://www.pcisecuritystandards.org/documents/QIR-Program-Update-FAQs.pdf)
Q & A
Helpful Resources

- Website: [www.conexxus.org](http://www.conexxus.org)
- Email: [info@conexxus.org](mailto:info@conexxus.org)
- LinkedIn Profile: [Conexxus.org](http://www.conexxus.org)
- Follow us on Twitter: [@Conexxusonline](https://twitter.com/Conexxusonline)
- NACS/Conexxus WeCare© Program: [www.conexxus.org/wecare](http://www.conexxus.org/wecare)