

PCI & Small Merchant Compliance: What Does the Future Hold?

Presenter: Chris Bucolo, ControlScan, Inc.

Agenda

- Housekeeping
- Presenters
- About Conexus
- 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

Speaker:

Chris Bucolo

Director, Strategic Partnerships & Market Strategy

ControlScan

cbucolo@controlscan.com

Moderator:

Kara Gunderson

Conexxus, Data Security Committee Chair

POS Manager, CITGO Petroleum

kgunder@citgo.com

Today's Speaker

- Conexus 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

About Conexus

- 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



2018 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 25, 2018	Attacking Fuel Mobile Payment Solutions	Denis Sheridan	Synopsys
February 22, 2018	PCI & Small Merchant Compliance	Chris Bucolo	ControlScan
March 22, 2018	Penetration Testing: How to Test What Matters Most	Sam Pfanstiel & Coalfire Lab Personnel	Coalfire
May 2018	QIR Program Update	Chris Bucolo	ControlScan
June 2018	TBD	TBD	TBD

2018 Conexus Annual Conference

April 29 – May 3, 2018
Loews Chicago O'Hare
Chicago, Illinois

More about Sponsorship Opportunities &
Registration:
www.Conexus.org



Conexus thanks our 2018 Annual Diamond Sponsors!

mSHIFT.
Relevant. Mobile. Solutions.

 **GILBARCO
VEEDER-ROOT**

Stuzo

Cybera
Simplify Security and Networks

**DIEBOLD
NIXDORF**

Session Summary

- The evolution of PCI:
 - Where it has been and where it is heading
 - New initiatives from the PCI Council and card brands
- A fresh perspective on scope and risk reduction:
 - P2PE, E2EE and tokenization solutions, and semi-integrated payments
- An inside look at the PCI Council Small Merchant Task Force
 - Goals for streamlining compliance and security
- Our top takeaways for Security and Compliance

Where it Started: The PCI Big Three

	PCI DSS	PA DSS	PTS (PED)
Overview	<ul style="list-style-type: none"> The Payment Card Industry DSS (PCI DSS) is a data security standard managed by the PCI SSC The standard was created to help organizations that accept card payments minimize exposure to a data breach 	<ul style="list-style-type: none"> The Payment Application DSS (PA-DSS) is a comprehensive set of requirements designed for payment application vendors The program is designed to drive out prohibited data storage and foster a more secure payments system. 	<ul style="list-style-type: none"> The PCI PIN Security Requirements are primarily focused on device characteristics impacting the security of PIN Entry Devices (PED) The PCI SSC manages the listing of approved PIN Transaction Security (PTS) Devices and the PCI PED security requirements
Applies To	<ul style="list-style-type: none"> Any business that accepts or processes payment cards 	<ul style="list-style-type: none"> Software vendors that develop commercial payment applications that store, process or transmit cardholder data as part of authorization or settlement Acquirers must ensure their merchants use only PA-DSS compliant applications (Visa) as applicable 	<ul style="list-style-type: none"> Vendors that manufacturer PIN-Entry Terminals Merchants who accept PIN-based transactions (integrated terminal or standalone PIN pad) <p>NOTE: These devices may also be referred to as PTS Points-of-Interaction (POI)</p>

Where PCI Stands Today

- A mature standard—no more 3 year cycles
- Updates based on breach experiences, service providers and remote access
- Software explosion and ecommerce concerns
- Addressing the explosion of consumer driven buying experiences
 - EMV
 - High growth of transactions on consumer devices

Current U.S. Breach Experiences

The Service Provider Factor

Service Provider Definition: Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity.

- This includes providers of services that control or could impact security of cardholder data.
- Examples include managed service providers for managed firewalls, IDS and other services, as well as hosting providers and other entities.

Note: Any third party with remote access into a merchant's cardholder data environment can impact security and will be viewed as a service provider.



The Broad Reach of Service Provider Breaches...



WHAT HAPPENED?

The Sabre Hospitality Solutions SynXis Central Reservation System (SHS reservation system) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following an examination of forensic evidence, on June 6, 2017, Sabre began notifying certain customers and partners that use or interact with the SHS reservation system that an unauthorized party gained access to account credentials that permitted unauthorized access to payment card information, as well as certain reservation information, for a subset of hotel reservations processed through the SHS reservation system.



Remote Access Breach Formula

The screenshot displays the Central LogMeIn interface. The top navigation bar includes the 'Central LogMeIn' logo, a user profile icon, and 'Settings'. The left sidebar contains a navigation menu with categories like 'Computers', 'Deployment', 'Ad Hoc Support', 'Users', 'One2Many', 'Updates', 'Reports', 'Alerts', 'Configuration', 'Networks', and 'Backup'. The main content area is titled 'Computers' and features a search bar and a 'Show All Groups' dropdown. Below this, a list of computers is shown, including individual devices and a group named 'Pizza People'. Each computer entry includes its name, status (e.g., 'Offline for 11 days'), and a set of icons for navigation and actions.

Computer Name	Status	Actions
Britt's Bistro	Offline for 11 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Burger Villa	Offline for 11 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Coffee N More	Offline for 219 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Pizza People	Offline for 11 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Galactic Grocers	Offline for 11 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Pizza People Group (10 computers, 4 online)		
Back Waitress	Offline for 2 hours and 11 minutes	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Bar 1	Online	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Bar 2 (1)	Offline for 4 days and 21 hours	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Liquor	Offline for 979 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
PIZZA left	Offline for 981 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
PIZZA2(AP)	Online	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Register 2 (3)	Online	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Server (1)	Offline for 382 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
SERVER(AC)	Online	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties
Waitress (6)	Offline for 724 days	Main Menu, Dashboard, File Manager, Alerts, Updates, Note, Properties

The PCI Council & Card Brands' Response

PCI DSS Compliance

*“If you are a merchant that accepts payment cards, you are required to be compliant with the **Payment Card Industry Data Security Standard (PCI DSS)**.”*



- ✓ Must achieve compliance annually
- ✓ Must validate compliance (effective Jan. 31, 2017)
- ✓ Must use a QIR certified technician to install POS systems (effective Jan. 31, 2017)

Source: www.pcisecuritystandards.org

PCI SAQ v3.2: New Service Providers Reqs. Kick-in

+ As of February 1, 2018:

- **6.4.6** Material changes require that PCI DSS requirements be applied to all new or changed systems and networks, with updated documentation
- **8.3.1 Utilize multi-factor authentication for non-console administrative access to CDE, locally and remote** (this has already been in place for remote access)
- **10.8** A process must be in place for detecting and reporting a failure of critical systems, along with an action plan for responding
- **11.3.4.1 Penetration tests for network segmentation must now be completed every 6 months by a qualified internal or external resource**
- **12.4.1** Executive management must establish accountability for maintaining PCI DSS compliance and define the charter
- **12.11** Quarterly reviews must be performed and documented to ensure that personnel are following security policies and procedures

What is Multi-Factor Authentication?

- 3 factors cover:
 - *What you know* (e.g., password, PIN)
 - *Something you have* (e.g., card, phone)
 - *Something you are* (i.e., a factor unique to you that cannot be changed such as biometrics – fingers, heart rate, movement, etc.)



Penetration Testing Vs. Scanning

- Due to breach forensics, more Self-Assessment Questionnaires (SAQs) require scanning and penetration testing.
 - Increased requirements for service providers
 - Medical analogy: MRI vs. exploratory surgery



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.**

“Integrators and resellers play a key role in the payments ecosystem, as merchants depend on these service providers to install, configure, and/or maintain their validated applications.

“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.**”

- https://www.pcisecuritystandards.org/program_training_and_qualification/qualified_integrator_and_reseller_certification

Right for you if...

You're an integrator or reseller that **sells, installs, and/or services PA-DSS validated payment applications on behalf of software vendors or others.**

Visa Updates/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.
- 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.

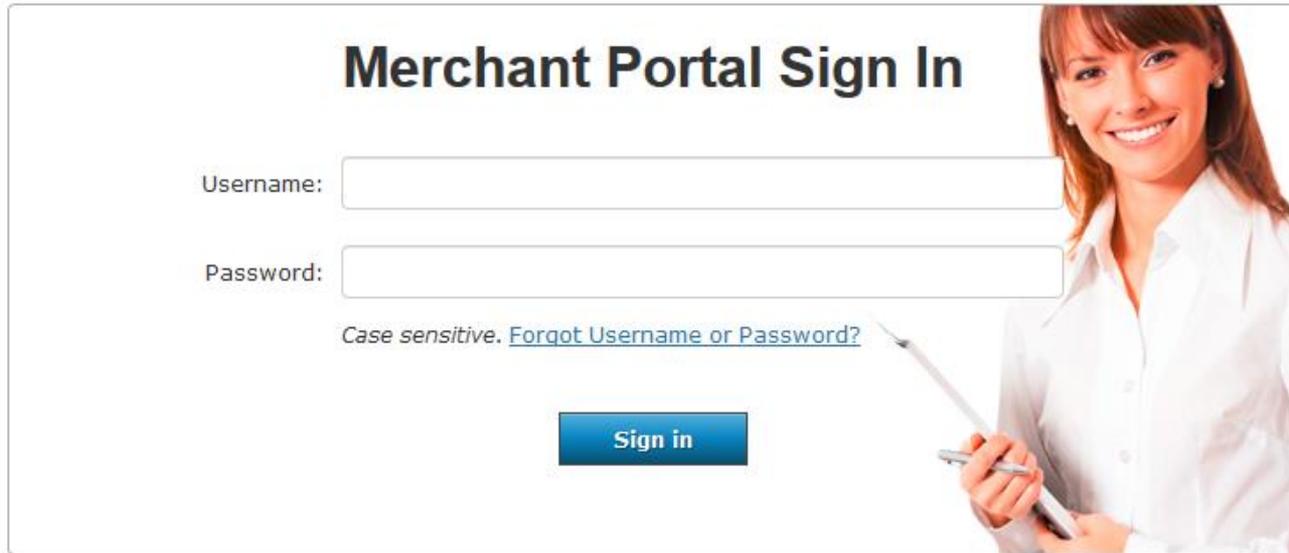
How to Mitigate The Remote Access Risk

- Always use two-factor authentication for remote access - Two factor authentication can be something you *have* (a device) as well as something you *know* (a password)
- Ensure proper firewalls rules are in place, only allowing remote access from known IP addresses
- If remote connectivity is required, **enable it only when needed** - Contact your POS vendor or integrator to take immediate steps to disable remote access when not in use
- Restrict access to only the service provider and only for established time periods
- Contact your POS Integrator and verify that a unique username and password exists for each of your remote management applications
- Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment
- Enable logging in remote management applications and examine the logs regularly for signs of unknown activity
- Do not use default or easily-guessed passwords
- Only use remote access applications that offer strong security controls
- Plan to migrate away from outdated or unsupported operating systems like Windows XP

What is The Best Approach?

Merchant Perspective

Enroll in a PCI program & Complete Online



Merchant Portal Sign In

Username:

Password:

Case sensitive. [Forgot Username or Password?](#)

A woman in a white shirt holding a clipboard and pen is positioned on the right side of the form, pointing towards the password field.

Get Pointed to the Correct SAQ!!

Select Your Processing Method

If you use more than one processing method, select your first processing method and you can add another when complete. This helps determine the Questionnaire that is appropriate for your business.

 <p><input type="radio"/> ABC Secure Terminal Select this processing method if you utilize ABC Payments Secure Terminal to process credit card transactions. To learn more about how the ABC Secure Terminal can increase your security and decrease your PCI burden, click here.</p>	 <p><input type="radio"/> Payment Terminal Select this method if you use a standalone device, not connected to a computer, to read or key-in credit card information.</p>
 <p><input type="radio"/> Virtual Terminal Select this method if you use a web browser on a computer or mobile device to access a merchant services site for entering and authorizing credit card purchases. You should have a username and password and be able to access the site from any online computer.</p>	 <p><input type="radio"/> POS Terminal Select this method if you are using POS (Point of Sale) software installed on a computer or other system. Computers with POS software are often combined with devices such as cash registers, bar code readers, printers, optical scanners, and magnetic stripe readers. In addition, POS systems typically have functionality beyond just payment processing, such as inventory management, and are usually designed for a specific business sector (e.g.</p>
 <p><input type="radio"/> Shopping Cart Select this method if your customers enter their credit card information into a website to make online purchases, payments, or donations.</p>	 <p><input type="radio"/> Phone/Paper Select this method if you use a manual imprint machine or call a phone number and use the telephone key pad to submit credit card information to your processor.</p>
 <p><input type="radio"/> Smartphone/Tablet Select this method if you use an application on a smart phone or tablet to accept credit cards. You may also have a card reader connected to your device.</p>	 <p><input type="radio"/> Point to Point Encryption Select this method if you process cardholder data ONLY with a hardware payment terminal that is part of a PCI SSC Approved Point to Point Encryption Solution.</p>

Determine Which Security Offerings Match-up

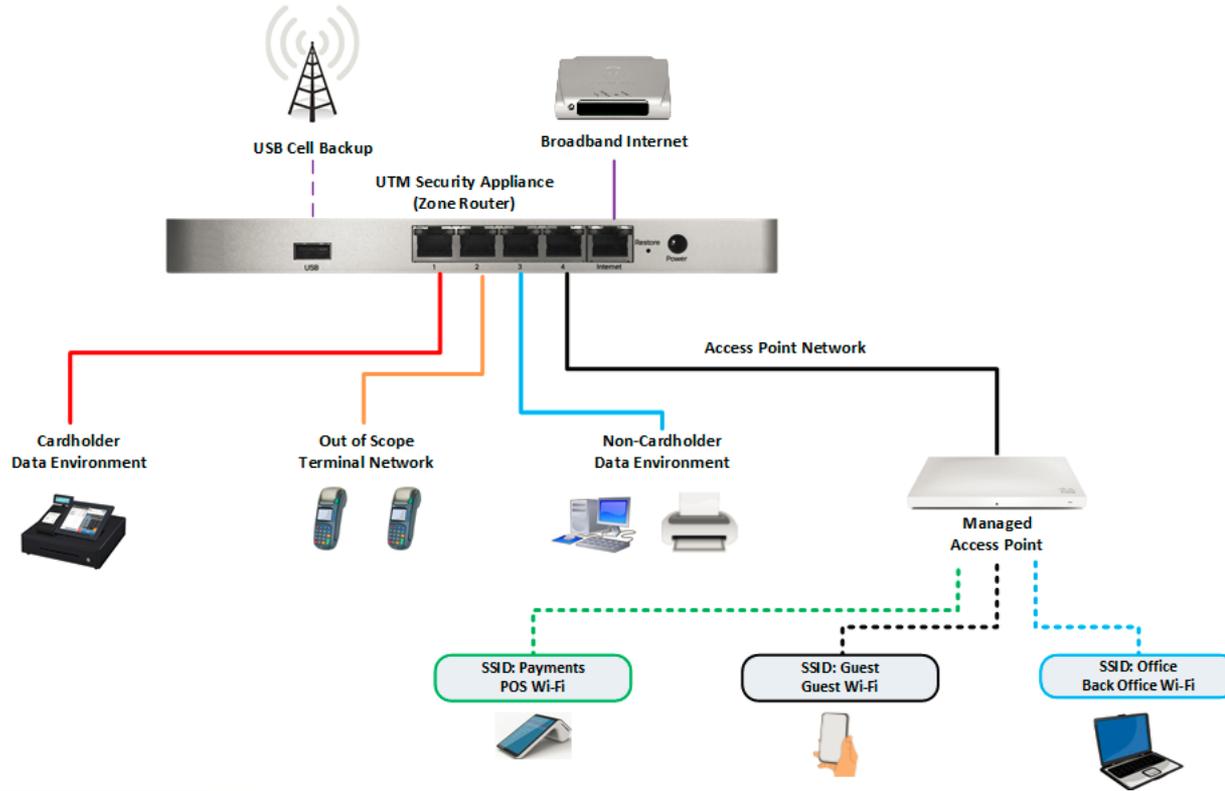
	Firewall UTM	Logging	FIM	Anti-Virus	Sec Aware Training	Internal Scanning	External Scanning
SAQ A							
SAQ A - EP	✓	✓	✓	✓	✓		✓
SAQ B					✓		
SAQ B - IP	✓				✓		
SAQ C	✓	✓	✓	✓	✓	✓	✓
SAQ C - VT	✓			✓	✓		
SAQ D - M	✓	✓	✓	✓	✓	✓	✓
SAQ D – SP	✓	✓	✓	✓	✓	✓	✓
SAQ P2PE					✓		

Merchant Benefits – Ease of PCI Compliance

Requirement 1: Install and maintain a firewall configuration to protect cardholder data	1.1, 1.2 and 1.3	Unified Threat Management Firewall	Unified Threat Management Firewall (UTM Firewall) provides continuous network monitoring and protection against outside threats, including intrusion detection and prevention. When in place, this solution can help you meet requirements 1.1, 1.2 and 1.3.
--	------------------	--	--

- By utilizing a UTM firewall, MSSP assumes responsibility for PCI requirements 1.1, 1.2, and 1.3 and the PCI DSS 12 steps for compliance.
- Additionally and when implemented in conjunction with the Web Based Self-Assessment Questionnaire (SAQ) solution, assumed sections of compliance are automatically pre-populated to decrease the amount of effort and time to self-attest.

Typical Firewall Design in Petroleum Store



Why Segmentation Matters

Examples of Network Segmentation Controls

VISA

From Flat Networks to Best Practices

Flat Network

- No subnetting
- Single domain
- No VLANs
- CDE located with core network



Low (Good)

- Understand network data flows
- CDE is separated by VLANs
- Use of access control lists
- Basic firewall rules



Medium (Better)

- Firewalls separate CDE from core network
- Firewall rules are reviewed audited regularly
- Granular control on users, assets, and traffic



High (Best)

- Separate login domain for CDE than core network
- Air gapped/ Completely segregated
- Alerts are regularly reviewed
- Two-factor authentication to log into CDE domain

Tampering and Skimming

- PCI DSS requirement 9 addresses physical security controls
- In the fuel retail environment, physical security pertains to the controls necessary to protect card data in its many forms – including manual imprints and other printed forms of cardholder data that may only occur during network outages.
- The unique environment in the petroleum world necessitates that attention be paid to both inside and outside assets, especially those involving payment devices. There is evidence that skimming and tampering attacks have gotten more sophisticated and, often have become more successful. (Source: Verizon DBIR-2016)



Work on The Human Element

- Passwords
- Remote access: human intervention is best
 - Caveat: If done right, the sword cuts both ways
- Social engineering – phishing is huge!!
- Be a skeptic even if people get ruffled sometimes (not customers of course 😊).

Where is PCI Heading?

Wasn't EMV Supposed to Fix All This?

- 50%-55% of merchant outlets use EMV
- EMV reduces fraud for card present transactions
- However, magnetic stripe data is alive and well on the dark web—RAM scraping
- EMV alone vs. EMV plus P2PE/E2EE!



Things To Look For

- Streamlined QIR program (March 2018)
 - Remote access/passwords/software updates
- More focus on software/equipment security
- More emphasis on ecommerce breach risk
- More emphasis on technology answers: P2PE
- New alternative to SAQs from Small Merchant Task Force

Call To Action in The Marketplace

Merchant: How can we streamline and simplify PCI?

Card Processor: How do you achieve strong security at the same time?

If done well: it is a win-win.

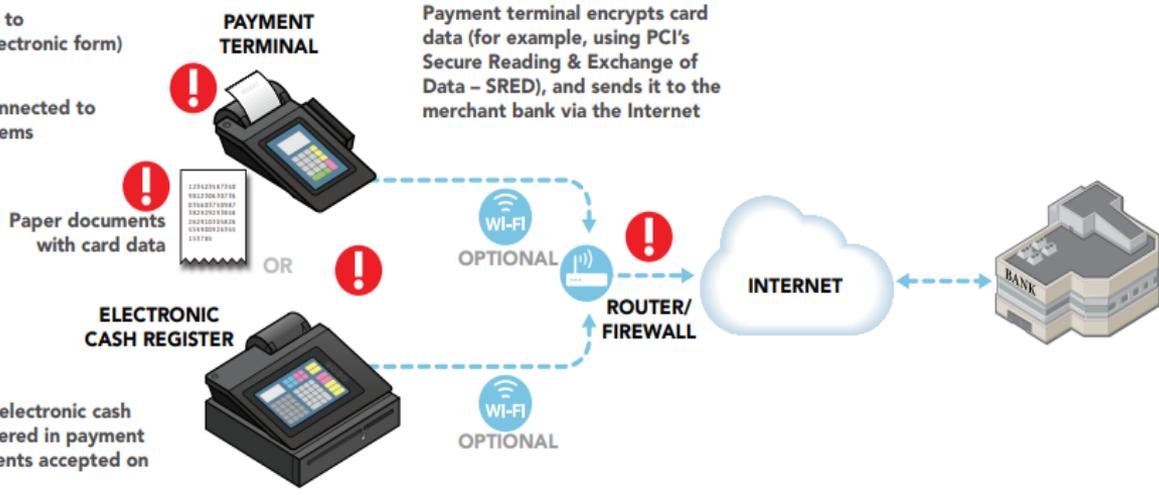
- Our View: Authentic Compliance + Strong Security = Winning Risk management Strategy
- The number 1 need is to find a few “trusted advisors.”



Semi-Integrated Models

Merchant has no access to unencrypted data (in electronic form)

No other equipment connected to merchant payment systems

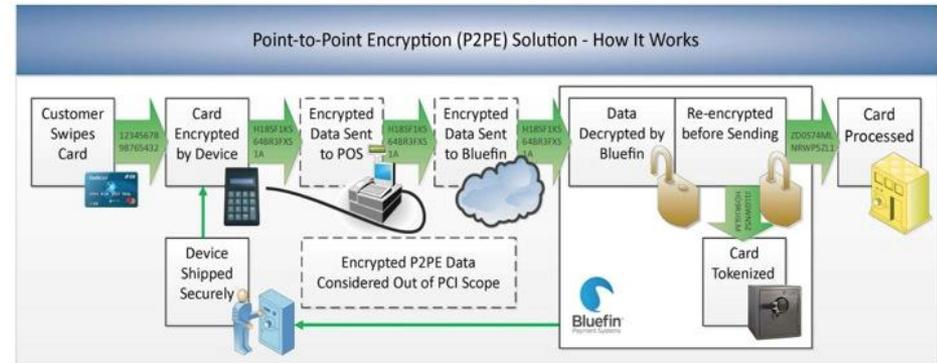


For this scenario, risks to card data are present at ! above. Risks explained on next page.

Source: www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf

P2PE Vs. E2EE

- Point-To-Point Encryption:
 - Ideal from a security and scope reduction standpoint
 - Costly
 - You have less control—no light bulb changes—all rewiring
- End-To-End Encryption:
 - The Council now has an official program for assessments
 - Can be very effective if well designed
 - Allows for more control and flexibility in many cases

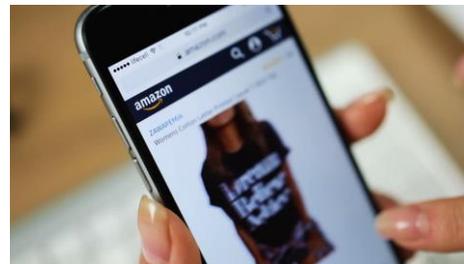


Mobile & Software Development Explosion

The PCI Council & Card Brands understand that consumer facing applications (heavily mobile focused) necessitate guidance on security:

- New guidance issued on Software based PIN entry on Consumer devices (COTS)
- Created an evaluation methodology-attended environment
- New security standards issued for EMV 3-D secure (3DS) protocol
 - Enhanced authentication to help prevent unauthorized card-not-present transactions from both web browsers and mobile applications.

Source: PCI Security Standards Council, LLC.



PCI Council Small Merchant Task Force

Why Focus on SMBs?

Small businesses globally are a prime target for cybercriminals.

DON'T LEAVE YOUR BUSINESS OPEN TO ATTACK

When your payment card data is breached, the fallout can strike quickly. Your customers lose trust in your ability to protect their personal information. They take their business elsewhere. There are potential financial penalties and damages from lawsuits, and your business may lose the ability to accept payment cards. A survey of 1,015 small and medium businesses found 60% of those breached close in six months. (NCSA)



Computer equipment and software out of the box often come with default (preset) passwords such as "password" or "admin," which are commonly known by hackers and are a frequent source of small merchant breaches.



PCI Small Merchant Task Force

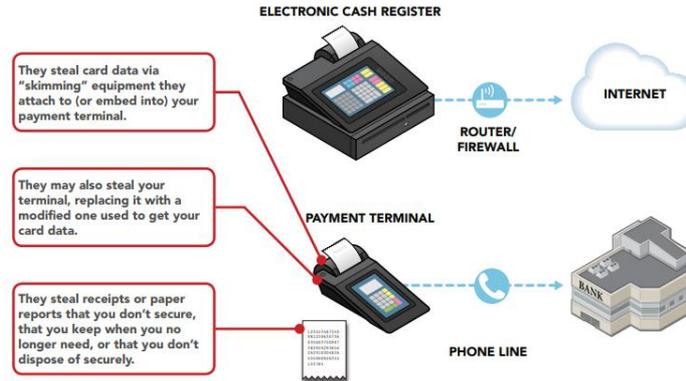
- Building on past work to create simpler ways of understanding security concepts
- Initial release: good work but not married to SAQ process
- First efforts to truly look at risk of how you process—and suggested ways to mitigate it
- **Current effort will release SAQ alternative: “Data Security Essentials” for low-to-medium risk scenarios (April 2018)**
 - Consolidation of concepts into fewer questions
 - Every effort made to simplify-with more explanation as back-up
 - Risk focus

PCI Small Merchant Task Force

Lower Risk Scenario

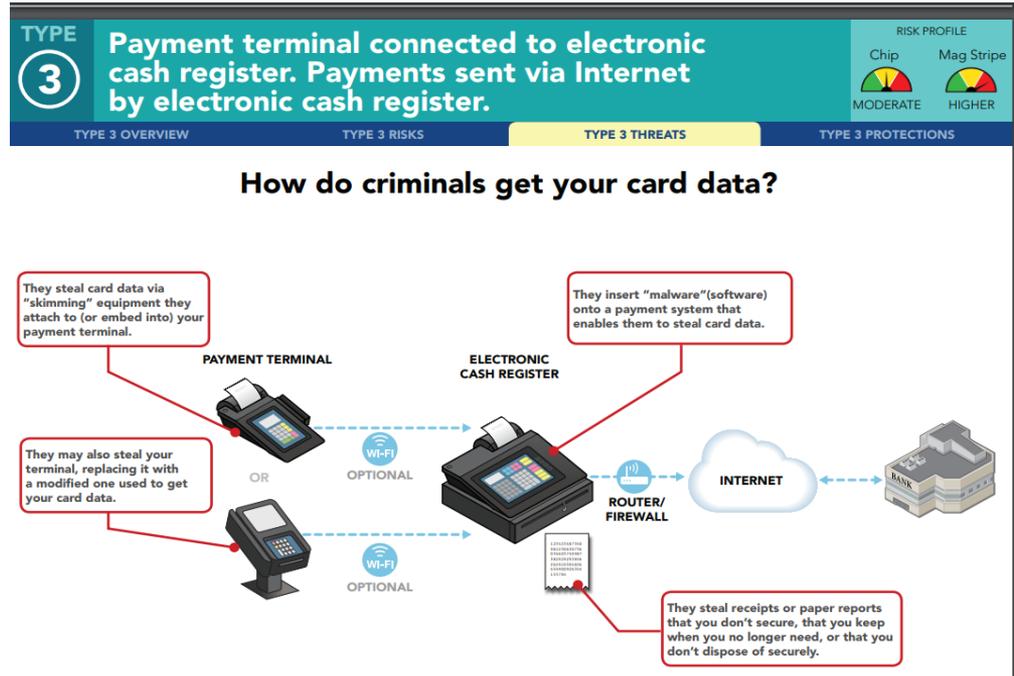
TYPE ②	Dial-up payment terminal and Internet-connected electronic cash register. Payments sent via phone line.	RISK PROFILE	
		Chip LOWER	Mag Stripe LOWER
TYPE 2 OVERVIEW	TYPE 2 RISKS	TYPE 2 THREATS	TYPE 2 PROTECTIONS

How do criminals get your card data?



PCI Small Merchant Task Force

Higher Risk Scenario



Top Takeaways

- PCI is here to stay! 10 years and counting...
- For small businesses, PCI is the basis for security knowledge and action plans.
- Complying with PCI is typically not expensive for small businesses.
 - The alternatives are usually expensive: breach related costs/brand damage
- Typical vulnerabilities:
 - Remote Access*
 - Password Strength*
 - Software updating/patching*
 - *New QIR focus.
 - Firewalls with established rules to restrict traffic and manage risk
 - Physical fraud-skimmers, PIN pad overlays, etc.
 - The human element!!

The Big Three

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%

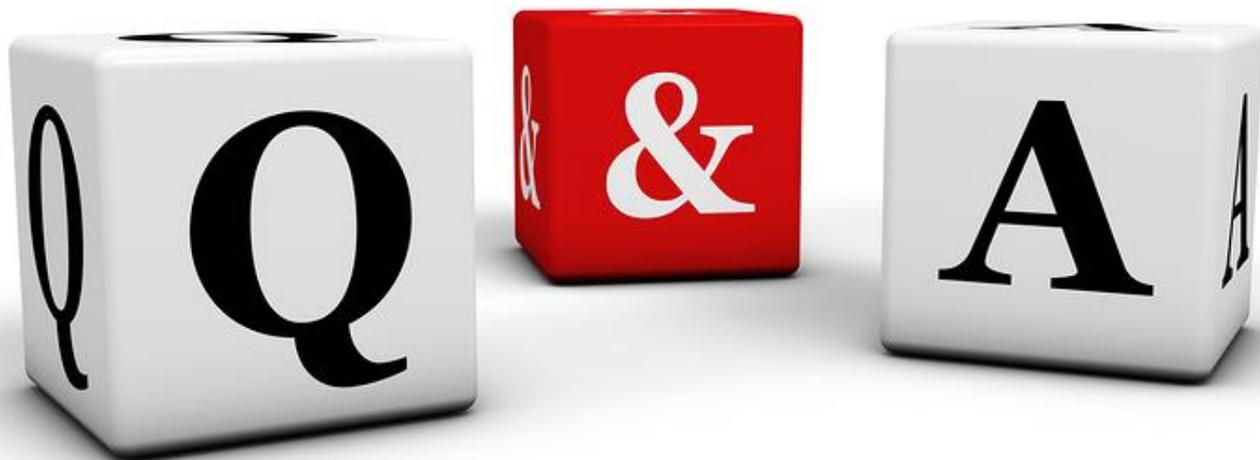
of hacking-related breaches leveraged either stolen and/or weak passwords*

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

For more information, download Payment Protection Resources for Small Merchants at:
PCISSC.org/SmallMerchant





Helpful Resources

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