



PCI Survivor's Guide Webinar

Gray Taylor – NACS

Marc Lucas – Coalfire Systems

March 3, 2010





Some of the opinions of the contributors expressed herein do not necessarily state or reflect those of the National Association of Convenience Stores. Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, shall not constitute or imply an endorsement, recommendation, or support by the National Association of Convenience Stores.

The National Association of Convenience Stores makes no warranty, express or implied, nor does it assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

. . . Or its consultants





Introductions

- Gray Taylor – Card Payments Consultant to NACS
gtaylor@nacsonline.com
+1 512 508 3469
- Rick Dakin – President/Co-Founder Coalfire Systems
 - one of the top 5 PCI audit firms
 - has audited hundreds of industry POS solutions
 - operates the NACS/PCATS “CIO Boot Camp”Rick.Dakin@Coalfiresystems.com
+1 303.554.6333 ext. 7001

Mark Lucas, CISSP, CISA, CGEIT, QSA, MCSD
Vice President, Managed Services

Mark.Lucas@Coalfiresystems.com

+1 206-352-6028, ext 7508





POLL QUESTION:

**HAVE YOU BEEN ASKED TO PROVE
PCI COMPLIANCE BY YOUR
PROCESSOR?**





POLL QUESTION:

**WHO'S WITH US ON THE CALL
TODAY?**



Case Study

TOO SMALL & REMOTE TO HACK



Mel's Diner – Broussard, LA

- Profile
 - 24-hour diner, processing 60 to 70 card transactions per day
 - Broussard: population 6,800
 - Upgraded POS in November 2007 and added Internet-based card processing
 - Used well-known system, installed & supported by professional systems VAR
- The Symptoms
 - April 2008 employee notices “mouse cursor moving by itself on screen”
 - VAR advises that system be immediately unplugged from Internet
 - VAR replaces system hard drives next day, puts system back online
- The Notice
 - May of 2008, Mel's is notified by Visa and MasterCard that compromised card accounts have been traced to their restaurant



Mel's Diner – Broussard, Louisiana

- Forensics
 - Visa and MasterCard request Mel's conduct forensic investigation and report back.
 - Mel's hires a forensic Qualified Security Assessor (QSA) to review compliance with SAQ
- The Hack (a final report has not been made public)
 - Installer had left access user ID and passwords in default state
 - No verification of internet firewalls conducted
 - System software version installed was not PCI PA DSS compliant
 - Hacker found the exposed internet connection through an automated "bot" that prowls the net 24/7
 - Once identified, the hacker entered the site and installed "key logger" malware
 - All data entry (keystrokes, magnetic card reads) was sent back to hacker
 - Hacker used available data analyzer to cull card data – 669 card accounts compromised



Mel's Diner – Broussard, LA

- The Damage

– Forensic investigation	\$19,000
– Amount of theft \$30,000 negotiated to:	\$20,000
– Fine from Visa	\$ 5,000
– Fine from MasterCard \$100,000 waived	<u>\$ -0-</u>

Total Cost to Mel's \$44,000

– Cost per compromised card	\$ 66
-----------------------------	-------

- Takeaway

- With automated hacking tools, you are never too small
- With internet connections, you are never too remote



Data Security Environment

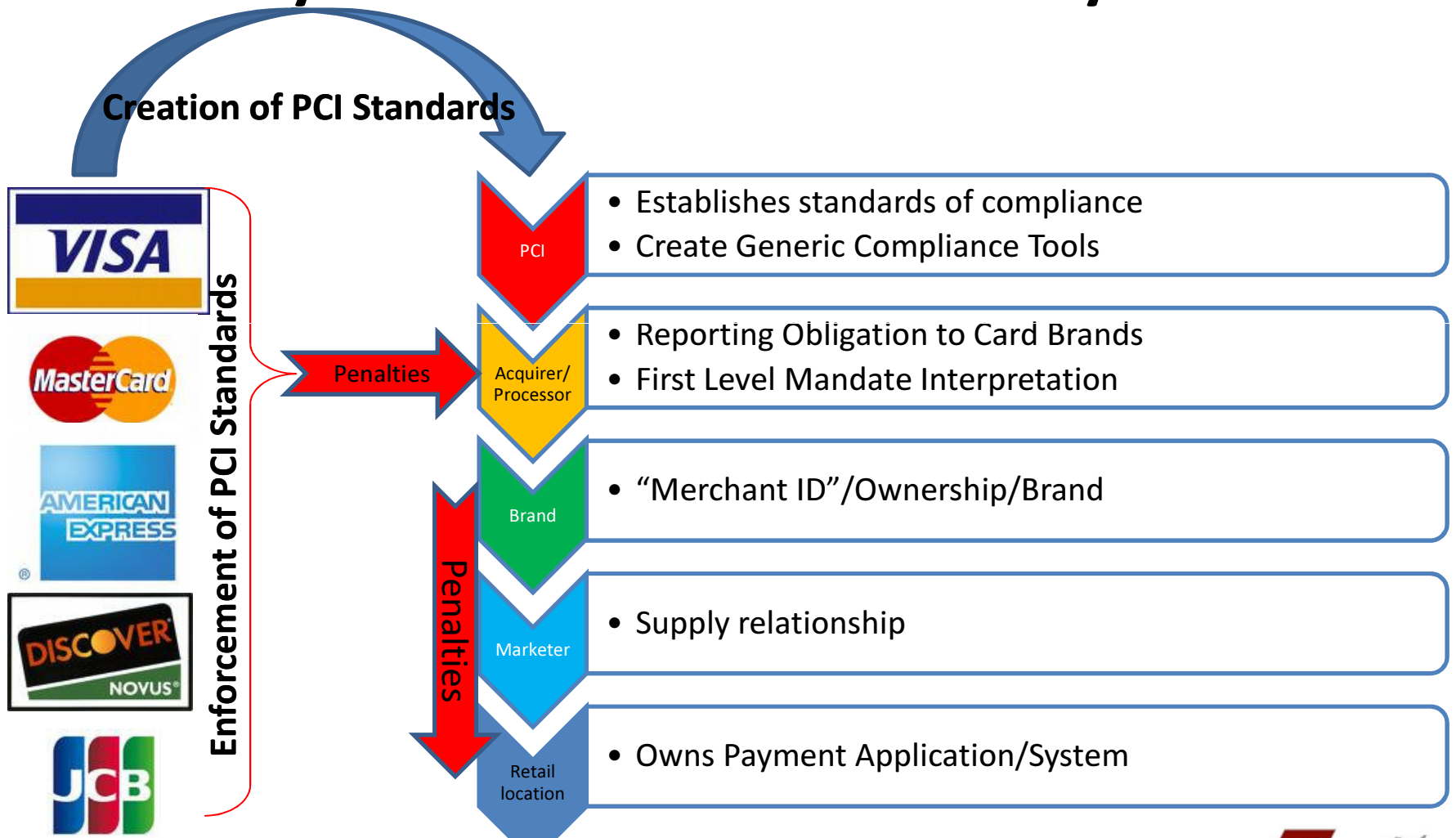
Increasing focus on data security by government and financial entities on the heels of several large breaches

- PCI DSS is focal point of card companies' efforts to improve security
 - Large retail has mostly adopted
 - Small retail – majority of US sales – has not adopted
- Consumer confidence in financial system is at risk
- Legislators and regulators have identified the threat and are working to require data security
 - States are creating patchwork of statutes targeting data security
 - Federal regulators are broadening their scope to include data security

PCI-DSS and Data Security Laws Apply To:

- You if you store, process or transmit payment cardholder data
- If you extend credit to individuals and DBA's
- If you capture two items of personal identification on ANY customer
- If you accept employment applications with personal information
- If you retain or handle employee health records

Today's Focus: Card Data Security & PCI DSS



Compliance is mandatory through the Merchant Agreement!



What is NACS' Position on PCI?

- NACS supports data security and understand the risks associated with handling sensitive cardholder data
 - Our industry is in the “risk business” - we do a good job at it!
 - However, PCI is flawed in several ways:
 1. It attempts to fix a decades old system architecture
 2. It assumes small retailers have IT expertise/resources
 3. It effectively transfers card business risk to retail
 4. It does not require card issuers to comply
 5. It is arbitrary in its application
 6. You are compliant until you are breached!
 - The best way to comply is to be data secure
 - You avoid other adversaries (FTC, State Law, Litigation)
 - You make PCI immaterial





NACS EZ PCI

Marc Lucas, Coalfire

- Compliance issues for the small merchant
- PCI validation issues

Compliance issues for the small market and convenience stores

- Why are we here today?
- Why do I care about PCI compliance?
- Level 4 merchant compliance requirements
- Safe harbor
- Compliance reporting

Why are we here today?

1. PCI requirements are a reality that we have to address ...one way or another
 - Try to change the rules
 - Hope that the PCI cops don't find us
 - Transfer the problem to someone else (banks, software vendors, major oils, service provider or trade association)
2. Meanwhile...the risk of cyber attack is increasing
 - State data privacy laws are growing
 - Our customers expect us to protect their data
3. It's not easy...we want to get some help (knowledge and tools) to make it easier.

The call you don't want

1. A franchise operator with 23 stores gets hacked ... loses 3,000 credit card numbers
 - Using a validated payment application
 - Following franchise instructions
 - The attack started 3 months ago and may still be ongoing
2. Visa investigation results in fines of over \$25,000, investigation charges of more than \$40,000, notice costs of \$15,000 and fraud reimbursement to be determined (could exceed \$200,000)
3. Who was responsible for all the damages?
 - THE MERCHANT Everyone else ran to the sidelines

Level 4 merchant requirements

- Be in compliance with the PCI DSS at all times
- Submit a Self-Assessment Questionnaire (SAQ) annually
- Submit 4 “clean” network quarterly scans

Is everyone with us today fully PCI compliant?
(POLL QUESTION)



Safe harbor

- If those three requirements are met, merchant receives “Safe Harbor”
- Ensures that merchant is not “at fault” in the event of a compromise
- Merchant receives protection from fines and fees associated with loss of cardholder data
- Ensures continued card processing and rate privileges
- HOWEVER – if you are breached, you are out of compliance; maintaining compliance critical

Compliance reporting

- You must submit your SAQ and scan reports in order to receive Safe Harbor
- Retail relationships and associations can cloud this issue for convenience store merchants
- Know your Ws:
 - What do I need to report?
 - Whom do I need to report to?
 - When are the reports due?



What do I report?

- Most store operators function as a single merchant with one relationship to an acquiring bank or processor
- However, convenience store operators may operate as more than one merchant
- You need to be capable of producing multiple SAQs across your stores to accommodate for these relationships
- These entities will set due dates for your reports



Validation issues for the small market

- Understanding your processing agreements
- Understanding your payment technologies
- Determining if scans are necessary

Understanding your processing agreements

- The “what” and “whom” of your reports typically begin with your card processing agreements.
- Who maintains your merchant account?
 - Franchisor?
 - Payment application/ POS provider?
 - Major oil?
 - You?

If you maintain multiple merchant accounts/relationships you may need to generate *multiple* SAQ reports.

Understanding your Payment Technologies

- Processing relationships may not always be clear
- Think through your payment technologies. Where does the transaction go after leaving your store?
 - Pay at Pump -> Major Oil Network -> Oil's Bank
 - In Store POS -> Our Internal Network -> My Bank
 - Car Wash -> Service Provider Network -> ?
 - Restaurant Dial-Out Terminal -> Telephone -> My Bank

You may need three different SAQs under this scenario- one to the Major Oil, one to your bank, and one to the Car wash service provider.

Do I need network scans?

- An SAQ is always required, but what about scans?
- Scans are only needed if your transactions:
 - Are conducted over the Internet from your stores
 - Are conducted on an internal network in your stores that is connected to the Internet
- Telephone-based dial-out terminals and imprint machines would not require scans
- Network-based POS systems require scans



Questions?

Please “raise your hand” using the Webinar tools on right of your screen



NACS EZ PCI

Mark Lucas, Coalfire



Pulling your program together: NACS EZ PCI

- Flexible reporting groups for store networks
- Year-over-year program management
- Tracking payment technologies
- Automated diligence
- Scan services
- QSA interaction and support
- Automated interactivity with franchisors, payment application providers and others



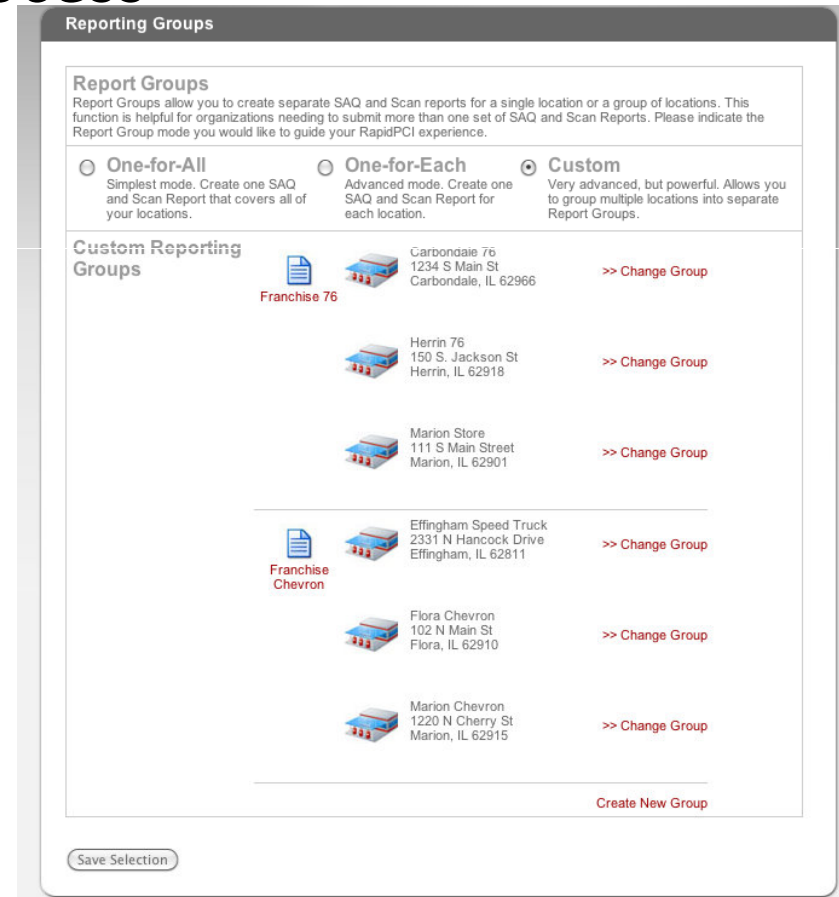
NACS EZ PCI

NACS EZ PCI Demonstration

Reporting groups

NACS EZ PCI allows you to manage the “who” and “what” of your reporting process

- You can create as many different SAQs as you need to fulfill your reporting requirements.
- Your store locations can be grouped by SAQs, allowing you to submit different SAQs to different banks or processors.
- Reports can be matched up to different franchises, payment processors, etc.



Reporting Groups

Report Groups
Report Groups allow you to create separate SAQ and Scan reports for a single location or a group of locations. This function is helpful for organizations needing to submit more than one set of SAQ and Scan Reports. Please indicate the Report Group mode you would like to guide your RapidPCI experience.

One-for-All
Simplest mode. Create one SAQ and Scan Report that covers all of your locations.

One-for-Each
Advanced mode. Create one SAQ and Scan Report for each location.

Custom
Very advanced, but powerful. Allows you to group multiple locations into separate Report Groups.

Custom Reporting Groups

Franchise 76	Carbondale 76 1234 S Main St Carbondale, IL 62966	>> Change Group
	Herrin 76 150 S. Jackson St Herrin, IL 62918	>> Change Group
	Marion Store 111 S Main Street Marion, IL 62901	>> Change Group
Franchise Chevron	Effingham Speed Truck 2331 N Hancock Drive Effingham, IL 62811	>> Change Group
	Flora Chevron 102 N Main St Flora, IL 62910	>> Change Group
	Marion Chevron 1220 N Cherry St Marion, IL 62915	>> Change Group

Create New Group

Save Selection





Reporting groups (cont.)

Event management and reporting tools allow you to manage year-over-year tasks


- Manage and track your report due dates.
- Receive alerts when reports are due.

Due Dates

SAQ Due Date **Friday, January 15, 2010**
This is the date that you submit your Self Assessment Questionnaire to your acquirer or processor. This is an annual date and will recur once a year.  [Update Date](#)

Scan Due Date **Friday, April 09, 2010**
This is the date that you are tracking to for your quarterly scan reports. You may or may not be required to submit this report to your acquirer or processor. This date will recur every three months.  [Update Date](#)

Reports

Report Name	Report Details
SAQ Report	Herrin 76 Date: 12/29/2009 This is a saved snapshot report, it shows the SAQ responses that were saved when the report was generated. 

Report Type

Live

Archive

Support

Having problems?
No problem! Just contact the Coalfire ServiceDesk for assistance. You may contact the ServiceDesk in the following ways:

Email: servicedesk@coalfiresystems.com

Support Ticket [Click Here](#) to open a support ticket with the Service Desk.

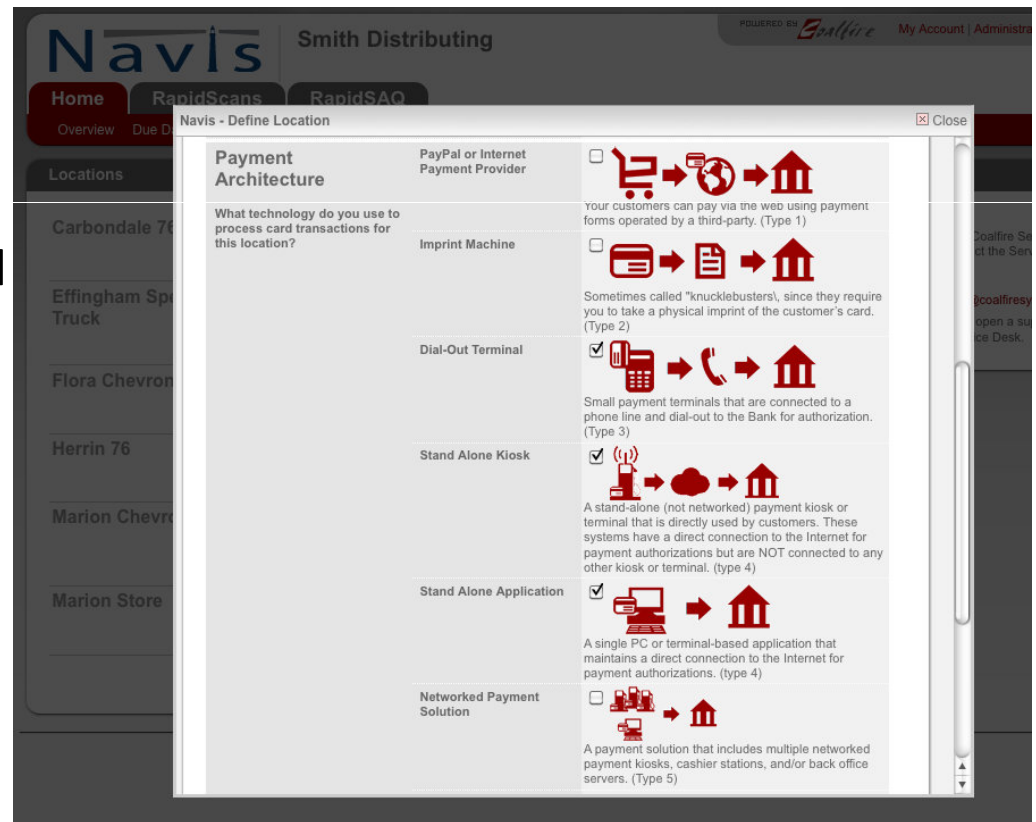
- Access live current year reports.
- Access historical reports from previous compliance periods.



Payment technologies

Define your payment technologies on a store by-store basis and quickly derive appropriate controls

- Select your payment architecture based on pictorial representations.
- Automatic determination of SAQ questions and controls.

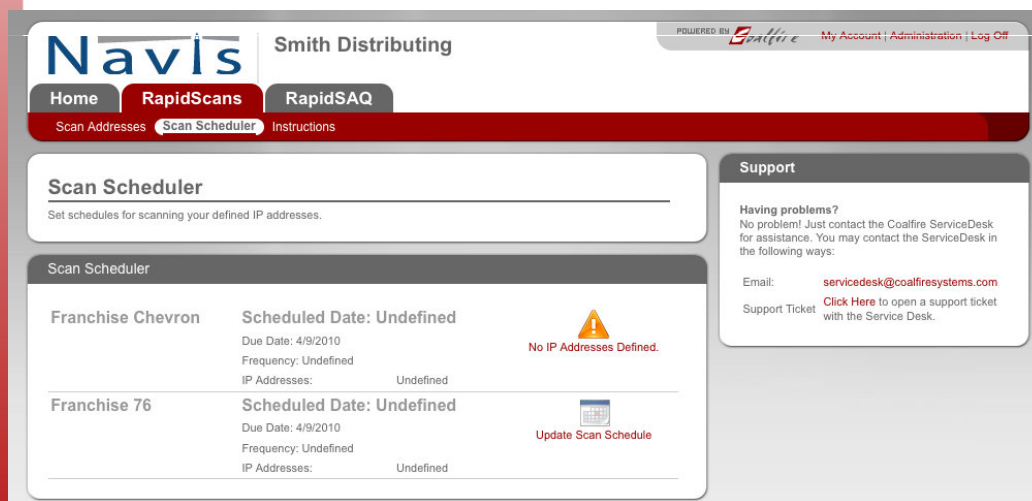


The screenshot shows the 'Navis - Define Location' window in the Navis system. The window is titled 'Navis - Define Location' and has a 'Close' button in the top right corner. The main content area is a table with the following columns: 'Payment Architecture', 'PayPal or Internet Payment Provider', and a description with a pictorial representation. The table is as follows:


Payment Architecture	PayPal or Internet Payment Provider	Description and Pictorial Representation
What technology do you use to process card transactions for this location?		Your customers can pay via the web using payment forms operated by a third-party. (Type 1)
Imprint Machine	<input type="checkbox"/>	Sometimes called "knucklebusters", since they require you to take a physical imprint of the customer's card. (Type 2)
Dial-Out Terminal	<input checked="" type="checkbox"/>	Small payment terminals that are connected to a phone line and dial-out to the Bank for authorization. (Type 3)
Stand Alone Kiosk	<input checked="" type="checkbox"/>	A stand-alone (not networked) payment kiosk or terminal that is directly used by customers. These systems have a direct connection to the Internet for payment authorizations but are NOT connected to any other kiosk or terminal. (type 4)
Stand Alone Application	<input checked="" type="checkbox"/>	A single PC or terminal-based application that maintains a direct connection to the Internet for payment authorizations. (type 4)
Networked Payment Solution	<input type="checkbox"/>	A payment solution that includes multiple networked payment kiosks, cashier stations, and/or back office servers. (Type 5)

Scan services

EZ PCI SAQ+ service provides you with online quarterly scan tools



Navis Smith Distributing

POWERED BY  My Account | Administration | Log Off

Home RapidScans RapidSAQ

Scan Addresses Scan Scheduler Instructions

Scan Scheduler

Set schedules for scanning your defined IP addresses.

Franchise	Scheduled Date	Due Date	Frequency	IP Addresses	Action
Franchise Chevron	Undefined	4/9/2010	Undefined	Undefined	No IP Addresses Defined.
Franchise 76	Undefined	4/9/2010	Undefined	Undefined	Update Scan Schedule

Support

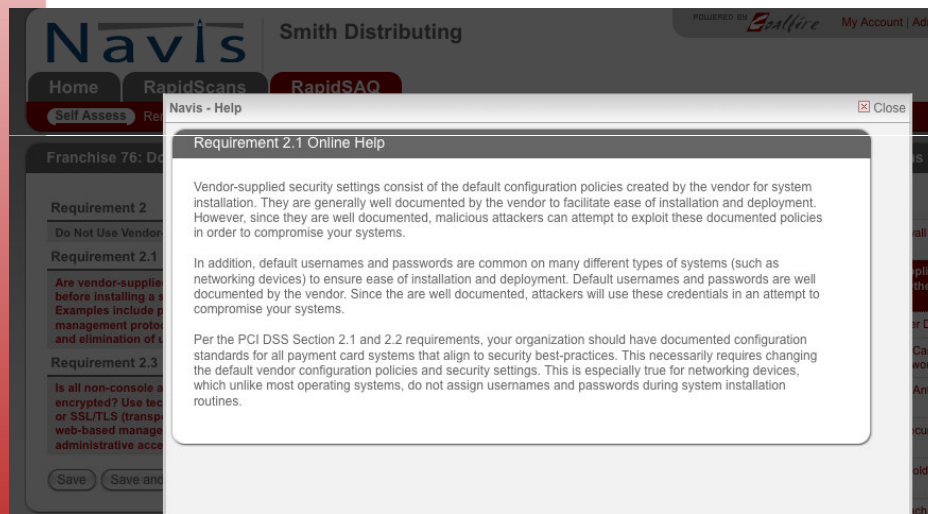
Having problems?
No problem! Just contact the Coalfire ServiceDesk for assistance. You may contact the ServiceDesk in the following ways:

Email: servicedesk@coalfiresystems.com
Support Ticket [Click Here](#) to open a support ticket with the Service Desk.

- Define IPs by store/locations.
- Schedule scans to run whenever you need them.
- Powerful scan reports, including full remediation tracking spreadsheets.
- Automated guidance for remediating each detected vulnerability.

QSA support

Interact with a QSA to help get you through tough questions and control responses



Navis - Help

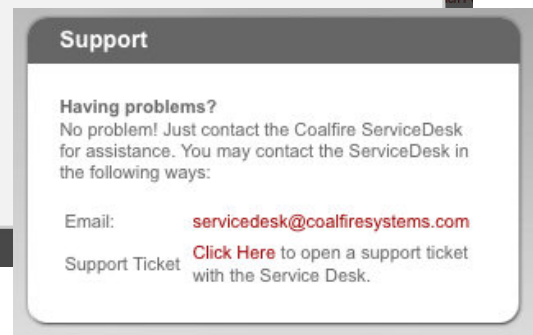
Requirement 2.1 Online Help

Vendor-supplied security settings consist of the default configuration policies created by the vendor for system installation. They are generally well documented by the vendor to facilitate ease of installation and deployment. However, since they are well documented, malicious attackers can attempt to exploit these documented policies in order to compromise your systems.

In addition, default usernames and passwords are common on many different types of systems (such as networking devices) to ensure ease of installation and deployment. Default usernames and passwords are well documented by the vendor. Since they are well documented, attackers will use these credentials in an attempt to compromise your systems.

Per the PCI DSS Section 2.1 and 2.2 requirements, your organization should have documented configuration standards for all payment card systems that align to security best-practices. This necessarily requires changing the default vendor configuration policies and security settings. This is especially true for networking devices, which unlike most operating systems, do not assign usernames and passwords during system installation routines.

- Facilitated help from QSAs is available in our “Facilitated” package.
- Engage a QSA to review your SAQ responses and evidence.



Support

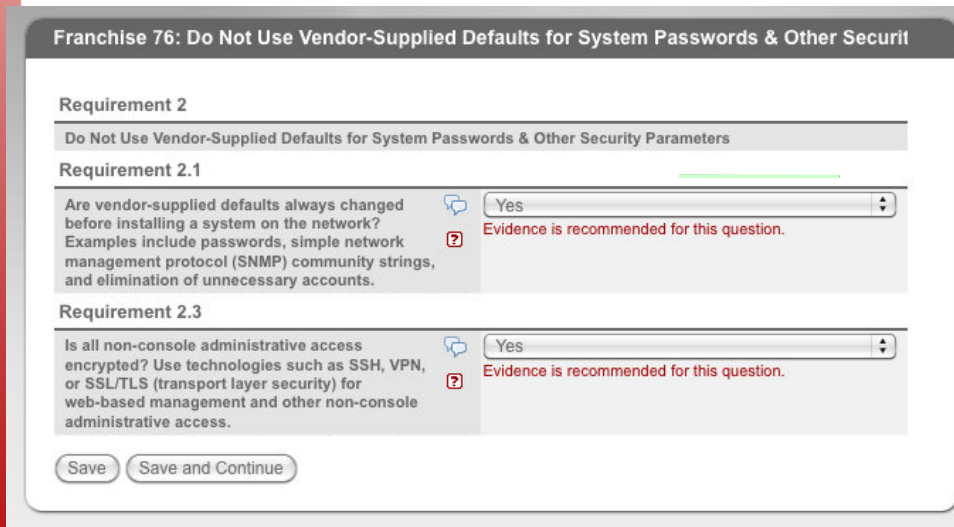
Having problems?
No problem! Just contact the Coalfire ServiceDesk for assistance. You may contact the ServiceDesk in the following ways:

Email: servicesdesk@coalfiresystems.com

Support Ticket [Click Here](#) to open a support ticket with the Service Desk.

Control recommendations

March update will include control recommendations from your franchisor or payment application provider

A screenshot of a software interface for "Franchise 76: Do Not Use Vendor-Supplied Defaults for System Passwords & Other Security". It displays two requirements, each with a dropdown menu set to "Yes" and a red question mark icon with the text "Evidence is recommended for this question." Below the requirements are "Save" and "Save and Continue" buttons.

Franchise 76: Do Not Use Vendor-Supplied Defaults for System Passwords & Other Security

Requirement 2

Do Not Use Vendor-Supplied Defaults for System Passwords & Other Security Parameters

Requirement 2.1

Are vendor-supplied defaults always changed before installing a system on the network? Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

Yes

Evidence is recommended for this question.

Requirement 2.3

Is all non-console administrative access encrypted? Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

Yes

Evidence is recommended for this question.

Save Save and Continue

- Allows franchisors, payment application providers and others to supply answers and evidence for your SAQ.
- Allows you to automatically submit reports electronically.
- Takes the guess-work out of controls within third-party applications, networks, and services.



Questions?

Please “raise your hand” using the Webinar tools on right of your screen



Back to Gray

FINAL THOUGHTS



An Online Tool Designed for Our Industry

- Designed by leading QSA: Coalfire
- Modified by the industry, for the industry
 - Major oil and retailer specialists revising base application
 - Several majors will adopt this tool for their marketers
 - NACS/PCATS committees will constantly revise
 - Compensating controls
 - Vendor implementation guides
 - Industry best practices
 - \$50,000 per site breach insurance, \$500,000 limit
- Cost reduced through aggregation
 - \$119 per location (\$169 per location, non-member)
 - \$149 per location, with port scanning (\$209 non-member)



Remediate & Comply

- You will not pass your first SAQ!
 - A truthfully answered SAQ will expose security risks in your business
 - Create a written remediation plan from “no” and “don’t know” answers
 - Make data security a corporate strategy/directive – legal & regulatory compliance should be included
 - SAQs are an open book test – you can keep taking it until you pass or are satisfied your risk is mitigated
- Do not submit an SAQ until requested
 - Complete it, have two copies notarized and store one copy off-site



Questions?

Please “raise your hand” using the Webinar tools on right of your screen



For More Information and to Enroll

- Go to: www.nacsonline.com/ezpci
- Contact Doug Spencer
dspencer@nacsonline.com
Direct Phone: 703.518.4293