



Vermont Grocers'
Association
Since 1934



Data Security

& PCI Compliance: Making Sense of It All

Vermont Grocers' Association
Webinar April 28, 2010



The Association for Convenience & Petroleum Retailing



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

The Association for Convenience & Petroleum Retailing



NACS would like to recognize the following organizations and their staffs for their assistance in making this presentation possible:

- PCATS, the Petroleum and Convenience Alliance for Technology Standards – Alan Thiemann
- W. Capra – Pat Raycroft & Jim Huguelet
- Coalfire Systems - Rick Dakin
- Vorys, Sater, Seymour & Pease LLC – Benita Kahn



The Association for Convenience & Petroleum Retailing



Agenda

- About NACS
- About our Industry
- Data Security Risks & Mitigation
 - Requirements and Remedies
 - Payment Card Data Security
 - Regulatory (the other monopoly)
 - Enterprise risk
- Interchange – if we have time

The Association for Convenience & Petroleum Retailing



About NACS

- Founded in 1961
- More than 2,000 retail member companies
 - Operating more than 75,000 stores in the US
 - Operating more than 300,000 stores globally
 - Members in 49 countries
 - 49 of the 50 largest companies in the industry
 - 79% of our US members operate 10 or fewer stores
 - Increasingly diverse retail membership
 - Jack-In-The Box, Delta Sonic, Kroger, Publix, Giant Eagle, Home Depot, both Follett and Barnes & Noble College Book Stores, TA Travel Centers
 - Petro Canada, Quickie Convenience Stores, Tesco, Marks & Spencer, BWG, Musgrave, Topaz, Welcome Break, Total, Pick n Pay, Seicomart, Dairy Mart, Famima, PTT, Woolworths AU, Coles Express, JMEL, OXXO, Repsol, Ipiranga
- More than 2,000 supplier member companies

The Association for Convenience & Petroleum Retailing



NACS' three pronged focus

- **Knowledge**
 - State of the Industry (SOI) Data
 - Support Technology standards (PCATS)
 - Industry research
 - Educational products
- **Connections**
 - The NACS Show
 - NACStech Show
 - SOI Summit
 - HR Forum
 - Category Management Conferences
 - Business Planning Conferences
 - NACS Global Forum & Study Tours
- **Advocacy**
 - Government & Monopoly Relations
 - Media Relations

The Association for Convenience & Petroleum Retailing



About our industry

The Association for Convenience & Petroleum Retailing

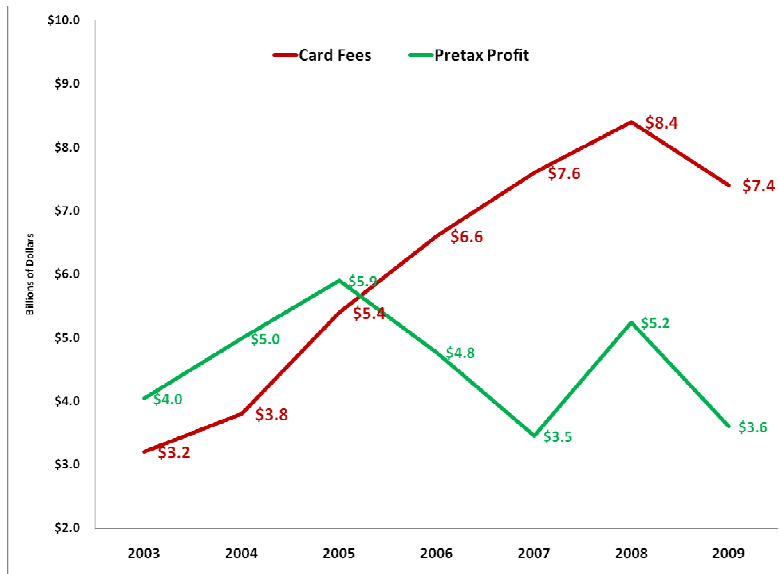


About our industry

- Our 144,000 + stores...
 - = 50,000 more than: Warehouse clubs+ Supercenters + Dollar stores + Mass merchandise stores + Supermarkets + Drug stores
 - Over 90,000 of stores are run by single store operators
 - We employ 1.7 million citizens
- Our 2009 sales totaled US\$511.1 billion equaling over 4% of the US GDP
 - 7% of Visa/MasterCard sales volume
- 140 million transactions per day
 - Every 40 hours the industry serves the equivalent of the entire mobile population of America (6 years to 85 years old)
- 98% of Americans shop at c-stores once/month
- We sell 80% of the motor fuel sold in the U.S.

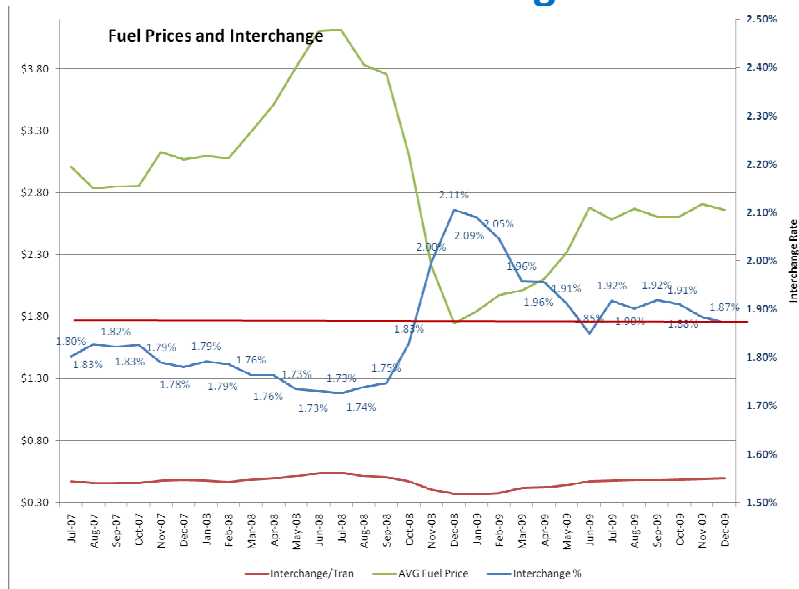
The Association for Convenience & Petroleum Retailing

Card Fees vs. Pretax Profit



The Association for Convenience & Petroleum Retailing

Interchange v. Fuel Price



The Association for Convenience & Petroleum Retailing

Data Security Risk & Mitigation

Home Office

Risk	Store	Settlement	Wholesale	Payroll	Benefits	Treasury
Litigation	Class Action	Slight	None	Slight	Slight	None
PCI	Fines, Clawbacks	Fines, Clawbacks	Depends	None	None	None
Atty Gen'l	Fines, Sanctions	Fines, Sanctions	None	Fines, Sanctions	Fines, Sanctions	None
FTC	Fines, Sanctions	Fines, Sanctions	Fines, Sanctions	Fines, Sanctions	Fines, Sanctions	None
State Data Security Law	Sanctions	Slight	Slight	Sanctions	Sanctions	None
Direct Loss	Chargebacks	None	Depends	None	None	High Risk

Highest Risk, Most Adversaries, Least Control

Highest Risk, Least Adversaries, Most Control

The Association for Convenience & Petroleum Retailing

This Discussion Applies to you . . .

- If you accept credit cards
- If you establish and maintain employee records
- If you extend credit to individuals, DBA's and Sub S Corporations
- If you maintain employee medical histories
- If you collect and maintain more than 2 pieces of consumer identification

The Association for Convenience & Petroleum Retailing



PAYMENT CARD RISK & MITIGATION

The Association for Convenience & Petroleum Retailing



Case Study

TOO SMALL & REMOTE TO HACK

The Association for Convenience & Petroleum Retailing



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

The Association for Convenience & Petroleum Retailing



Mel's Diner – Broussard, LA

- 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

The Association for Convenience & Petroleum Retailing



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 \$ -0-
- 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

The Association for Convenience & Petroleum Retailing



General Data Security Environment

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

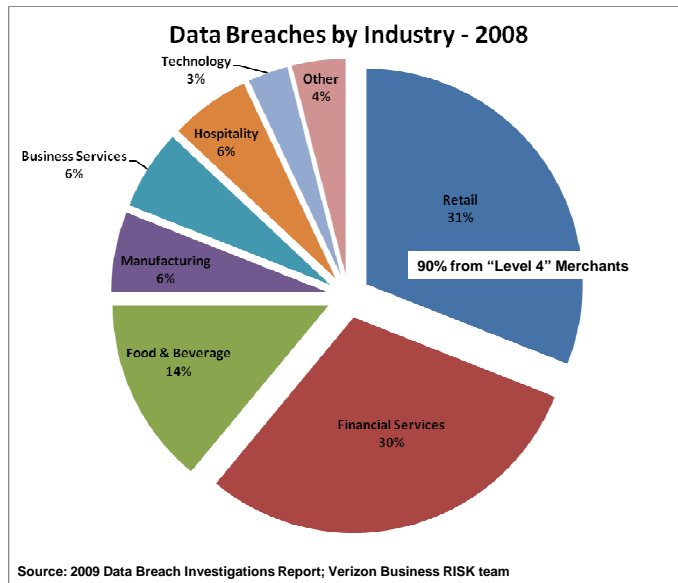
- PCI DSS is focal point of card companies' efforts to improve security
 - Large retail has mostly adopted
 - Small retail – majority of US sales – has not adopted
- Consumer confidence in financial system is at risk
- Legislators and regulators have identified the threat and are working to require data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

The Association for Convenience & Petroleum Retailing

PAYMENT CARDS

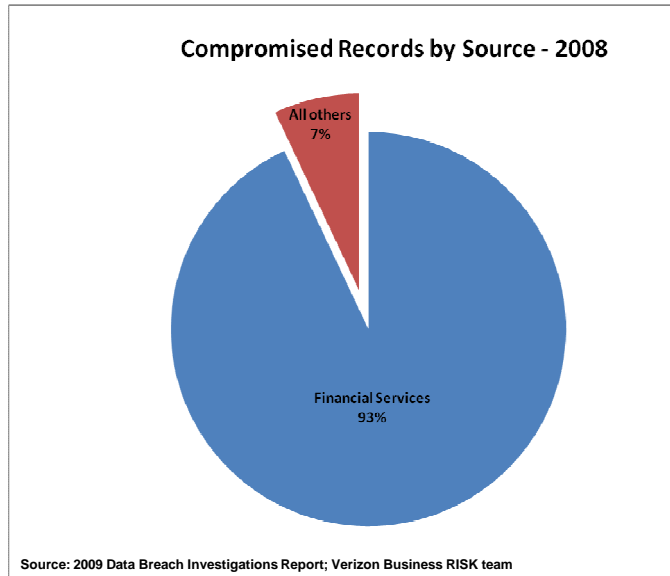
The Association for Convenience & Petroleum Retailing

Breaches Occur in All Markets. . .



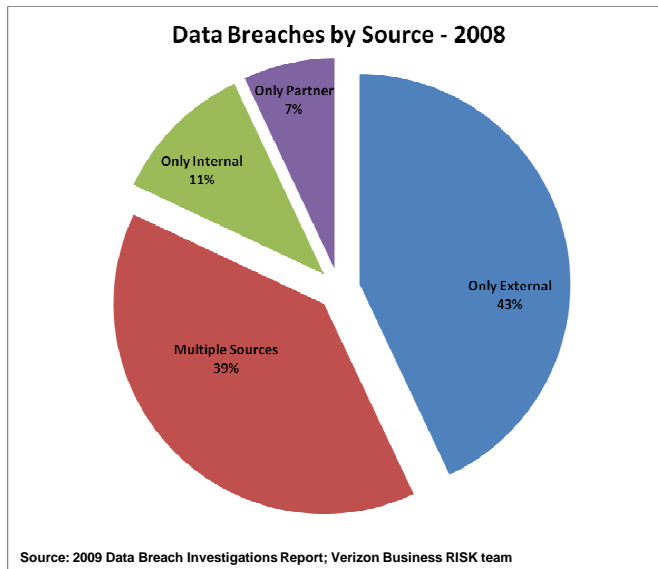
The Association for Convenience & Petroleum Retailing

But Financial Services Have Most Compromises



The Association for Convenience & Petroleum Retailing

Where are the Attacks Coming From?



The Association for Convenience & Petroleum Retailing

Financial Risk Landscape

Per Bank of America VP of Risk and Fraud, 2/17/10



The Association for Convenience & Petroleum Retailing

Card Data Targets:



Visa, Mastercard, Discover
CID Location.



American Express
CID Location.



- PIN Values
- Cardholder Verification Numbers



CVV2

No one is allowed to record this data!

The Association for Convenience & Petroleum Retailing

The threat is real

Skimmers are our biggest retail threat



FRAUD ALERT

NEW CARD SKIMMING DEVICE





The Association for Convenience & Petroleum Retailing

Recent Industry Incidents

Criminal hackers skim PIN numbers from gas pumps

AHARON ETENGOFF | Tue 23rd Feb 2010, 11:43 am

technology security atm-machines Add | View comments

Criminal hackers have reportedly managed to install electronic "skimming" devices at 150 gas stations across the state of Utah.

According to Police Sgt. Troy Arnold, the automated "skimmers" copied card and PIN numbers, which granted the criminals "free access" to the victim's [bank account](#).

The stolen data was then used to withdraw more than \$11,000 from ATM machines in Los Angeles.

"The skimming device [was] actually located inside the gas pumps!" Arnold told ABC News.



THE SACRAMENTO BEE [sacbee.com](#)
This story is taken from Sacbee / Our Towns / Roseville/Placer County News

More people report debit info stolen at Rocklin gas pumps
blindel@sacbee.com
PUBLISHED FIRST, DEC. 25, 2009

Rocklin police said Thursday that a growing number of people are reporting that their debit card information was stolen by a sophisticated device hidden in two Rocklin gas pumps.

"It's getting more and more scary," Rocklin Police Lt. Len Milka. "We are getting more and more victims. They are coming out of the woodwork."

At least two dozen victims have come forward since the devices were discovered Dec. 21 in the pumps at the AM/PM gas station at Sunset Boulevard and Park Drive. One victim had \$1,416 taken out of his bank account over three days, and another had almost \$1,000 stolen.

In the past, thieves used devices on the outside of gas pumps to get PIN numbers and information from cards. They installed tiny cameras and card skimmers to steal the information and then dip into a victim's account.

In this case, somebody had placed devices inside gas pumps. Police believe the device intercepts information and sends the PIN number and other debit card information to someone with a laptop.

The criminal then creates a card that allows him to go to an ATM and withdraw money from the victim's account.

"They are able to get into the actual gas pump," said Milka. "So, obviously, those pumps are not very secure. Whoever manufactures them has to come up with something better."

The Association for Convenience & Petroleum Retailing



Criminals Hide Payment-Card Skimmers Inside Gas Station Pumps

Wave of recent bank-card skimming incidents demonstrate how sophisticated the scam has become

By Kelly Jackson Higgins, [DarkReading](#)
Feb. 22, 2010
URL: <http://www.darkreading.com/story/showArticle.jhtml?articleID=223100223>

Criminals hid bank card-skimming devices inside gas pumps -- in at least one case, even completely replacing the front panel of a pump -- in a recent wave of attacks that demonstrate a more sophisticated, insidious method of stealing money from unsuspecting victims filling up their gas tanks.

Some 180 gas stations in Utah, from Salt Lake City to Provo, were reportedly found with these skimming devices [sitting inside the gas pumps](#). The scam was first discovered when a California bank's fraud department discovered that multiple bank card victims reporting problems had all used the same gas pump at a 7-Eleven store in Utah.



Cost of Compromise

- Direct costs: \$60 to \$182/compromised account
 - Notification, hotlines, websites, credit monitoring, fines, loss recovery, card reissuance, forensic investigation
- Brand damage
 - TJX breach cost the company hundreds of millions of market value
- Open to Litigation & Consumer Protection Fines
 - “Small” breach (5,000 accounts) costs \$1+ million
 - Median business breach: 50,000 to 100,000 accounts

Take-Away: Don't Forget Your State's AG, FTC and the Trial Bar!

The Association for Convenience & Petroleum Retailing



Strategic Cost of Breaches

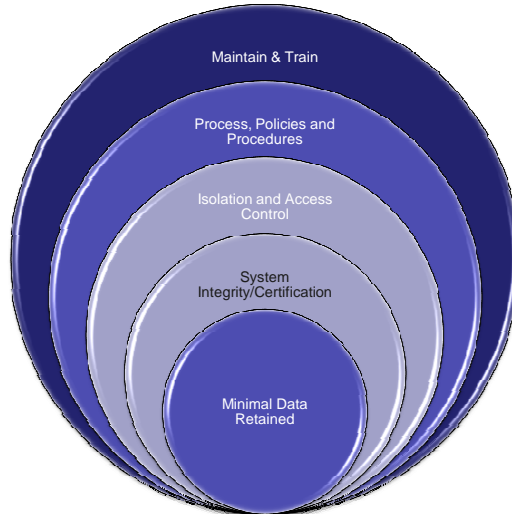
- Accelerated technology mandates

Accelerated TDES Upgrades:	\$1.5 B
Accelerated Chip & PIN Upgrades	<u>\$3.2 B</u>
Total, excluding cost of PCI	\$4.7 B
- Erosion of position on card issues
 - Supports card brand justification of high interchange
 - Supports PCI leadership position
- Industry brand damage
 - Further “proof” we operate “dangerous places”

We must self-regulate or be regulated

The Association for Convenience & Petroleum Retailing

Basic Blocks to Data Security



The Association for Convenience & Petroleum Retailing

PCI Security Standards Council One Element of Data Security

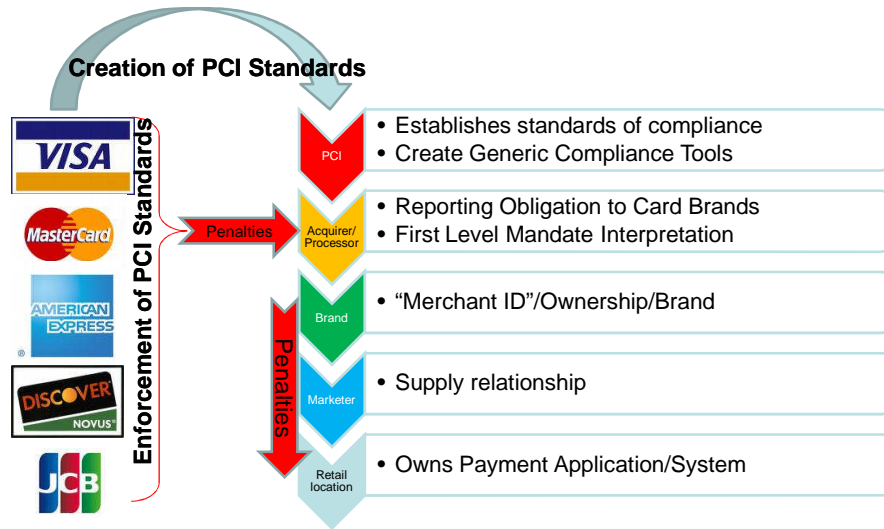


- The Payment Card Industry Security Standards Council is led by a policy-setting Executive Committee, composed of representatives from the founding payment brands. Operational decisions are made by a Management Committee, also from the payment brands.



The Association for Convenience & Petroleum Retailing

Hierarchy of Data Security Mandates



Compliance is mandatory through the Merchant Agreement!

The Association for Convenience & Petroleum Retailing

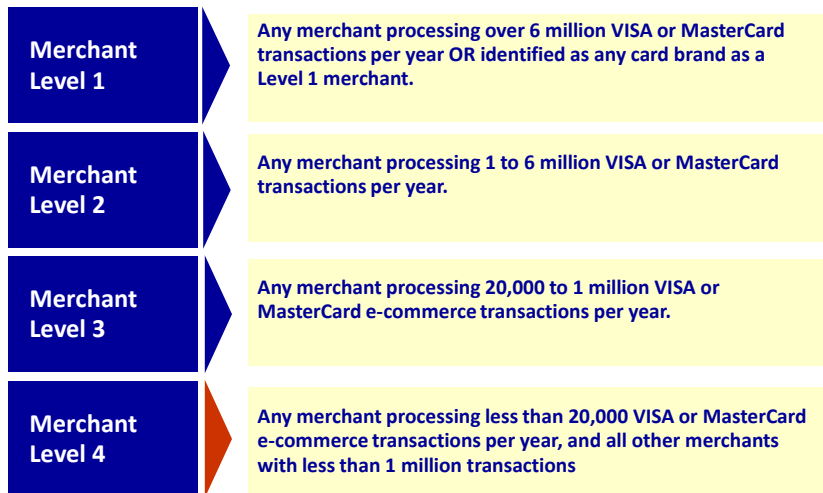
PCI-DSS applies to...

- You if you store, process or transmit cardholder data
- Systems that process or store data and systems that connect to them
- Compliance is mandatory
 - Required through the “merchant agreement”
 - Required through brand contract

The Association for Convenience & Petroleum Retailing



PCI Merchant Levels



The Association for Convenience & Petroleum Retailing



What is NACS' Position?

- 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
 - You make PCI immaterial

The Association for Convenience & Petroleum Retailing



What is NACS doing?

- NACS has been making members and the industry aware of PCI and data security since 2004 through:
 - NACS has joined the PCI Council as a Participating Organization
 - Advocating in Washington:
 - Homeland Security – Congress, DHS
 - Federal Reserve Bank; pushing Fed to take the lead on security
 - Advocating directly with the card brands
 - Educating the industry by working with state associations and other trade groups
 - NACS has worked with PCATS to create the Data Security Standards Committee

The Association for Convenience & Petroleum Retailing



ExxonMobil ConocoPhillips RaceTrac

bp

Chevron

Gulf

CITGO

MARATHON

Sinclair

Implementation & Compliance

Education & Best Practices

Strategy & Roadmap

The Association for Convenience & Petroleum Retailing

PCATS
PETROLEUM CONVENIENCE ALLIANCE
FOR TECHNOLOGY STANDARDS



Industry Risk Profile

Risk Priority	Risk Element	Lower Risk	Medium Risk	Higher Risk
1	Payment Application (PA-DSS) .	* PA-DSS Certified * Installed and Maintained according to the implementation guide	* Bespoke application that has not been verified against PA-DSS.	* non PA-DSS Certified * PA-DSS that is not installed or maintained properly * PABP Only Certified Application
2	Network Segmentation	* Adequate segmentation between POS and Backoffice * Dial-Up Only * No Network at site	* on IP Network; but able to track when devices get added	* No Adequate Segmentation * No control or awareness of new devices added to network
3	Firewall Configuration / Management	* Dial-Up * Private Network * Stateful hardware firewall installed - CISCO PIX		* Broadband - connection to Public Internet - if don't have Firewall configured properly * Public Facing presense * No Firewall installed
4	Remote Access/Management	* Allow connection only from specific (known) IP / MAC Address * Connect by 3rd Party w/ 2-factor authentication		Connections allowed on any IP / MAC Address
5	Vendor Default Settings	* Settings updated and passwords changed on install to unique passwords * Diagnostic settings are disabled		* Vendor default settings and passwords not changed
6	Access Controls	* Strong and managed Access Controls installed (e.g. Passwords) and Locked Down		* No strong access controls installed
7	Installation of Payment Application			
7	Technicians @ Site	* Vendors/Distributors have contracts in place * Ticket management system in place		No qualifications
8	Automated Fuel Dispenser	* AFD - DUKPT / TDES * Hardware (Security Kits, Tapes, Anti-Skimming Devices) is used to secure CRIND * Frequent Monitoring	* AFD - Master Session	* No Monitoring * AFD not hardened or secure
9	Paper Handling	* Process in place for Credit Card Applications * Chargeback information comes to site encrypted		* Processes not in place to handle for Cardholder Data * Process not in place to handle "destruction" of Cardholder Data
10	Memory Parser Software;	* Antimalware virus applications running real time * POS with embedded O/S	POS on Linux	* PCA with Windows based O/S * POS on Proprietary O/S * Malware; Windows Defender turned off
11	Network Vulnerability Scanning	Have tools in place to manage it		in place, but no management of asset
11	Penetration Testing			
12	Employee Education	Operations at Site handled with Best Practices defined to reduce/minimize fraud or breach		Operations at Site not handled with Best Practice inviting Fraud and/or Breach to occur
13 Dankin	Patch Management ((Operating System Patch including POS Application))	* Current - Critical Patches installed within 30 days; Security Patches installed timely * Proper segmentation * Whitelisting		Unpatched

The Association for Convenience & Petroleum Retailing



The PCI food chain ...or who owns PCI at my sites?

- Opinions Vary:
 - One marketer: “I just provide fuel; I'm simply another vendor to sites”
 - One site operator: “my brand is fully responsible for PCI”
 - One major oil company: “site owners are ultimately responsible for the PCI of their sites, but its our butts if they get breached”
 - Another major oil company: “.....”

The Association for Convenience & Petroleum Retailing



The PCI food chain ...or who owns PCI at my sites?

- Overarching Rule: ***follow the contracts***
- It is critical for everyone (MOCs, jobbers, dealers, operators) to get absolute clarity and agreement on who owns what aspects of implementing PCI at each site (which might vary by jobber, MOC, etc.) and what “lines of demarcation” exist
 - Consider having a face to face meeting with all involved parties to discuss all aspects of implementation across all components in your payment processing chain
 - Review all contracts for definition of liabilities related to sensitive data
- Personal advice...
 - Until you know different; assume you own it!
- **LIABILITY, LIKE A LOT OF “THINGS” FLOWS DOWNHILL!**

The Association for Convenience & Petroleum Retailing



What really are the PCI DSS deadlines?

SURPRISE!!!

According to the “Merchant Agreement” and its reference to the “Operating Rules”, we’ve always been responsible for sensitive card holder security in one way or another...

- Perhaps said best by American Express: “since its introduction in 2002, the data security operating policy has applied to your business under our card acceptance agreement”
- Or Visa: “mandated since June 2001, Visa’s CISP is intended to protect Visa cardholder data—wherever it resides”
- Officially, Levels 1 – 3 merchants were to be PCI compliant by end of 2005

HOWEVER – Visa has recently announced compliance “holidays”

The Association for Convenience & Petroleum Retailing



What tough questions should I be asking my POS/IT vendor and network provider?

- Is my POS PCI PA-DSS validated?
- Get a copy of the “Implementation Guide”
 - How do I migrate my current system and erase old card data
 - Has the method of remote access used to support POS systems been PCI PA-DSS validated?
 - Does each instance of my POS have unique user IDs and passwords for remote support? If so, how are IDs added, managed, and removed?
 - Does my POS log each and every system access? Including “root” or “administrator” access during infrequent activities like OS upgrades?
- How can I review the log files from my POS?
- Can my site system support a segmented site Local Area Network (LAN) architecture?

The Association for Convenience & Petroleum Retailing



What tough questions should I be asking my POS/IT vendors and network provider?

- How are unique user IDs and passwords managed on each network endpoint such as a DSL router, VSAT Customer Premises Equipment (CPE), etc.)
- Does my POS log each and every system access to on-site network components?
- Are your service personnel trained in PCI process
- Will you indemnify me from breaches caused by you

The Association for Convenience & Petroleum Retailing

Consider PCI an Ongoing Process

Level	Validation Actions	SCOPE	Validated By
1	<ul style="list-style-type: none"> Annual On-Site Security Audit - AND - 	<ul style="list-style-type: none"> Authorization and Settlement Systems 	<ul style="list-style-type: none"> Independent Assessor or Internal Audit if signed by Officer
	<ul style="list-style-type: none"> Quarterly Network Scan 	<ul style="list-style-type: none"> Internet Facing Perimeter Systems 	<ul style="list-style-type: none"> Qualified Independent Scan Vendor
2 & 3	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire - AND - 	<ul style="list-style-type: none"> Any system storing, processing, or transmitting cardholder data 	<ul style="list-style-type: none"> Merchant Optional support from qualified vendor
	<ul style="list-style-type: none"> Quarterly Network Scan 	<ul style="list-style-type: none"> Internet Facing Perimeter Systems 	<ul style="list-style-type: none"> Qualified Independent Scan Vendor
4	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire 	<ul style="list-style-type: none"> Internet Facing Perimeter Systems 	<ul style="list-style-type: none"> Merchant Optional support from qualified vendor
	<ul style="list-style-type: none"> Network Scan Recommended 	<ul style="list-style-type: none"> Internet Facing Perimeter Systems 	<ul style="list-style-type: none"> Qualified Independent Scan Vendor

The Association for Convenience & Petroleum Retailing

PCI Cheat Sheet

	PCI DSS	PCI Payment Application (PA-DSS)	PCI PIN Entry Device (Visa Driven)
Deadline	<ul style="list-style-type: none"> Now (technically) 	<ul style="list-style-type: none"> Now (technically) July 1, 2010 material deadline 	July 1, 2010 <ul style="list-style-type: none"> POS TDES "go live" Island card terminals must be TDES or SDES DUKPT
Scope	<ul style="list-style-type: none"> Any system transporting or supporting card acceptance 	<ul style="list-style-type: none"> Any hardware and/or software performing card transactions or storing allowed data 	Any store accepting Visa or MasterCard debit cards <ul style="list-style-type: none"> POS PIN Pads Dispenser PIN Pads
Risk of non – Compliance	<ul style="list-style-type: none"> Breach Liability Brand Damage 	<ul style="list-style-type: none"> Breach Liability Brand Damage Loss of card acceptance 	<ul style="list-style-type: none"> Cannot accept Visa and MasterCard logo debit cards Non-logo debit still ok
Point of Focus	<ul style="list-style-type: none"> All chain systems not "firewalled" from Payment Applications 	<ul style="list-style-type: none"> Point of Sale Card Terminal NOT Dispensers! 	<ul style="list-style-type: none"> Point of Sale Card Terminal
Basic Activity Focus	<ol style="list-style-type: none"> Determine Merchant Tier Self Assessment (SAQ) Remediate SAQ issues Re-Assess Keep document records Periodic scans (per Tier) Annual review/audit 	<ol style="list-style-type: none"> Install certified PA systems Self Assessment (SAQ) Determine Merchant Tier Remediate SAQ issues Re-Assess Keep document records Periodic scans (per Tier) Operating systems updates Annual review/audit 	<ol style="list-style-type: none"> Assess need to continue accepting PIN debit Determine cost of upgrading Begin upgrading NO LATER than one year before deadline

The Association for Convenience & Petroleum Retailing



Process, Tools and Resources

PAYMENT CARD DATA SECURITY

The Association for Convenience & Petroleum Retailing



Energize You Organization

- **Appoint Data Security Czar**
 - Upper level resource reporting to CEO
 - Strong technical experience
 - Cross-functional scope
 - Legal, financial, fuels brands, personnel, operations, vendors
 - Invest in your Czar
 - Send them to data security training
 - Allow them to participate in industry calls & meetings
- **Make Data Security Part of Everyone's Job**
 - Corporate policy
 - Recurring training

The Association for Convenience & Petroleum Retailing



Determine Your Merchant Level

- Key Data
 - Annual transactions by card brand
- How & Where
 - Collect this by site as consolidation is tricky
 - Ask your processor or brand for this data
 - Key estimation - you are probably Level 4 if:
 - your total transaction count is less than 1.5 million per year
 - You have fewer than 30 sites

The Association for Convenience & Petroleum Retailing



Merchant Level Indicator

- Consolidate by brand/processor/business model
 - Use the following guidelines

Parent/Child Relationship	Remote Access	Data Aggregation	Parent Own POS	Tax ID	The Site Is Probably...
Brand OR Marketer/Distributor to Site					
Supply Agreement - non landlord	No	No	No	No	Level 4
Supply Agreement - landlord	No	No	No	No	Level 4
Tenant/Landlord - (incl sales over-ride)	No	No	No	No	Level 4
Partnership/Joint Venture	No	No	Yes	Yes	Subject to Volume Aggregation
Commission Marketing Agrmt - Product Only	No	No	No	No	Level 4
Commission Marketing Agrmt - Turnkey	Yes	Yes	Yes	No	Subject to Volume Aggregation
Franchisor/Franchisee	No	No	No	No	Level 4
Franchisor/Franchisee Aggregated Services	Yes	Yes	Yes	No	Subject to Volume Aggregation
Company Owned, Dealer Operated	No	No	Yes	Yes	Subject to Volume Aggregation
Company Owned, Company Operated	Yes	Yes	Yes	Yes	Subject to Volume Aggregation
Dealer owned/operated; PA Owned by Company	Yes	No	Yes	No	??

The Association for Convenience & Petroleum Retailing



Complete Self Assessment (SAQ) Process

- Who, When?
 - If you are level 1 or 2, you are late
 - If you are Level 4, you have to assume 2010
- How?
 - Complete the free form from PCI
<https://www.pcisecuritystandards.org/saq/index.shtml>
 - Use a completion tool

The Association for Convenience & Petroleum Retailing



SAQ – 1040 Long Form or “TurboTax”?

Question	Response:	Yes	No	Special*
<i>Abbreviations, and Acronyms for additional information.</i>				
3.2.2	Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. <i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)? <i>Notes:</i> <ul style="list-style-type: none"> • This requirement does not apply to employees and other parties with a specific need to see the full PAN; • This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Is PAN, at a minimum, rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs.) by using any of the following approaches? <ul style="list-style-type: none"> • One-way hashes based on strong cryptography • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures. <i>The MINIMUM account information that must be rendered unreadable is the PAN.</i> <i>If for some reason, a company is unable to render the PAN unreadable, refer to Appendix B: “Compensating Controls.”</i> <i>Note: “Strong cryptography” is defined in the PCI DSS and PA-</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Question	Response:	Yes	No	Special*
<i>DSS Glossary of Terms, Abbreviations, and Acronyms.</i>				
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used: (a) Is logical access managed independently of native operating system access control mechanisms (for example, by not using local user account databases)? (b) Are decryption keys independent of user accounts?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Are cryptographic keys used for encryption of cardholder data protected against both disclosure and misuse?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5.1	Is access to cryptographic keys restricted to the fewest number of custodians necessary?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Are cryptographic keys stored securely, and in the fewest possible locations and forms?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6	(a) Are all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, fully documented and implemented? (b) Do they include the following?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1	Generation of strong cryptographic keys	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	Secure cryptographic key distribution	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Secure cryptographic key storage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Periodic changing of cryptographic keys: <ul style="list-style-type: none"> • As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically • At least annually 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Association for Convenience & Petroleum Retailing



Online Tools – “TurboTax” for PCI

- Pros
 - The free form is unintelligible to most small retailers
 - A good tool will
 - eliminate “NA” questions based on interview
 - allow reuse of data for additional SAQs
 - Offer remediation planning
 - Facilitate annual reporting process
 - A great tool
 - will comprehend the unique systems of petroleum retail
 - will allow online storage of proof files
 - Offer port scanning
 - Include meaningful breach insurance coverage
 - Offer template process and policies for your organization
- **CONS:** Like taxes, it is you who attest to quality of return – use a good vendor

The Association for Convenience & Petroleum Retailing



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 SAQ
 - \$149 per SAQ, with port scanning (1 IP address)

For more information contact Doug Spencer: dspencer@nacsonline.com

The Association for Convenience & Petroleum Retailing



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 and SAQ until requested
 - Complete it, have two copies notarized and store one copy off-site

The Association for Convenience & Petroleum Retailing



Card Data Security Rule of Thumb*

* Your presenter’s opinion

- **Update**
 - Your card handling systems (POS, routers, anti-virus)
 - Your card data communications to validated vendor
 - Change dispenser terminal locks to unique keys
- **Isolate**
 - Segment card handling environment – don’t co-mingle
 - WiFi public access should have dedicated internet
- **Educate**
 - Make data security company policy, and train for it!

The Association for Convenience & Petroleum Retailing



Q & A Data Security

The Association for Convenience & Petroleum Retailing



Survey of Data Security Legislation and Regulation

Special thanks to Benita Kahn, Partner, Vorys law firm, Columbus, OH

The Association for Convenience & Petroleum Retailing



Recent Settlements

June 23, 2009 - TJX settles with 41 state attorneys general

- Pays nearly \$9.8 million
- Implement extensive data security measures

Countrywide/Bank of America

- January 2009 settles with Connecticut AG for \$350,000 (30,000 Connecticut residents affected)

Veterans' Affairs (January 2009)

- \$20 million to current and former military personnel affected by the breach
- After 3 years of litigation
- Settles class action on behalf of 26.5 million active duty troops and veterans whose personal information, including names, dates of birth, and SSNs were on laptop and hard drive that went missing

The Association for Convenience & Petroleum Retailing



How Federal Law and Enforcement has Responded



The Association for Convenience & Petroleum Retailing



Federal Perspective: The Federal Trade Commission

- FTC enforces data security through Section 5 of the FTC Act – prohibits “unfair or deceptive acts or practices in or affecting commerce.”

“Corporations must protect their back doors from hackers, malware, spyware and other high-tech intrusion mechanisms and protect their front door by properly storing and disposing of consumers' data ...the FTC is not shy about knocking on anyone's door.”

March 2009, Jon Leibowitz, FTC Chairman (NationalJournal.com)

The Association for Convenience & Petroleum Retailing



Federal Perspective: The FTC

Privacy - relies on “deceptive” standard

- generally used against inflated or misleading privacy statements
- privacy policy statements inconsistent with actual practices

In Security arena – relies on “unfair” standard

– **Focuses on:**

- Likelihood of substantial harm
- Whether injury is reasonably avoidable by consumers and
- Whether outweighed by benefits to consumers or competition

The Association for Convenience & Petroleum Retailing



FTC Safeguards Rule

- Designation of employee to coordinate
- Identify and assess risks and evaluate controls
- Design and implement program to address risks
- Regularly test and monitor effectiveness of program
- Oversee service providers who have access to protected information
- Evaluate and adjust program to address weaknesses or new risks

The Association for Convenience & Petroleum Retailing



More Federal Response To Identity Theft “Red Flags Rule”

Fair and Accurate Credit Transactions Act of 2003 (FACTA) required regulations from FTC to mitigate incidents of identity theft

Final Rules published November 2007 include 3 duties

- [Address discrepancy](#) notification - 16 CFR 681.1
- [Red Flags Program](#) - detection, prevention and mitigation of identity theft – 16 CFR 681.2
- [Card Issuers](#) regarding changes of address – 16 CFR 681.3

The Association for Convenience & Petroleum Retailing



FACTA Red Flags Program Requirement

Implementation delayed to June, 2010

Creditors* with “covered accounts” must implement written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with:

- the opening of a covered account, or
- any existing covered account

Must include reasonable policies and procedures to:

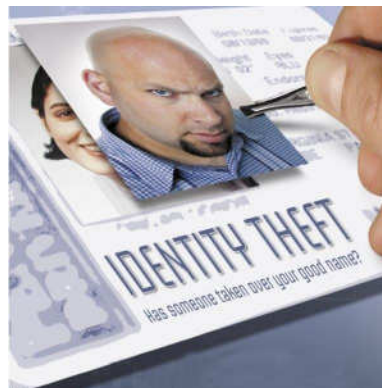
- Identify relevant red flags
- Detect red flags that are part of the Program
- Respond appropriately to any red flags that are detected
- Ensure the Program is updated to address changing risks

*Any person who regularly extends, renews or continues credit

The Association for Convenience & Petroleum Retailing



State Laws Enacted to Address Privacy and Identity Theft



The Association for Convenience & Petroleum Retailing



Notice of Breach Laws: 46 States

Personal Information is generally an individual's first name or initial and last name combined with one of the following:

- social security number,
- driver's license or state i.d. number, or
- account number, credit card or debit card number in combination with password, security code, or access code.
- California, Missouri and Texas have added healthcare information

Encryption

- Each of the state laws makes an exception for encrypted personal information.

The Association for Convenience & Petroleum Retailing



State: Data Security Laws

- **Some states have specific data security laws/regulations**
 - California
 - Massachusetts
 - Minnesota
 - New Jersey
 - Nevada
 - Texas

The Association for Convenience & Petroleum Retailing



Regulatory/Government Risk Mitigation

- Know your state and federal laws
 - State associations should be monitoring this!
 - You may find your state is considering onerous law on data security
- Legal and regulatory compliance is part of the “Czar’s” job description
 - Simplify and unify policies, compliance and procedures into one program – they are very similar!

The Association for Convenience & Petroleum Retailing



Incident Response



The Association for Convenience & Petroleum Retailing



Response to a Breach

Create an Incident Response Plan NOW

- Work with your counsel
 - Classify Information
 - Identify where cc#'s are located
 - Identify types of Events
 - Determine Roles and Responsibilities
 - Event detection – call center; internet; administrative offices; third party
 - Escalation – specific means of contact
 - Core Team and extended team
 - Assessment after event
 - Testing and Training

The Association for Convenience & Petroleum Retailing



Response to a Breach

Incident Identification and Investigation

- Identify nature and scope and need for forensic (retain evidence)
 - Work with forensics company before first draft is written
 - Consider hiring multiple forensics companies (privilege)
- Contain and deploy mitigation and remediation as appropriate

Identify notifications required by law

- Identify specific content requirements and timing
- Identify appropriate party to make notification

Identify notifications required by contract

- E.g., notification of acquiring bank if credit card numbers compromised.

Assess prevention

The Association for Convenience & Petroleum Retailing



PROTECTING TREASURY

The Association for Convenience & Petroleum Retailing



In Cyberspace, No One Can Hear You Scream

- Credential theft is the fastest growing fraud
 - Stealing account management and access credentials to use the system to move money
 - Your accounts can be cleaned out overnight
 - Bank liability is undefined and designed for bank indemnity
- Keystroke Loggers – Main Threat Vector
 - How?
 - Social engineering – get your CFO to visit a web site
 - Install logger through USB or CD
 - Packet sniffing across network

The Association for Convenience & Petroleum Retailing



Protecting Your Treasury – Mitigation Ideas

- Limit Access
 - All online account functions should be credentialed by user
 - Users should be limited to “need to use” – be strict – not even IT should access without user supervision
 - PCs used for account management should be physically secure and off the local area network
- Limit Exposure – “Clean” PC
 - Strong anti-virus and anti-malware, daily updates
 - Strong browser security
 - Limit URLs
 - All removable media ports under password control

The Association for Convenience & Petroleum Retailing



Thank you!

- Contact Info
 - Gray Taylor
NACS Payment Services
grayotaylor@gmail.com
(512) 508-3469
 - Michael Davis
NACS VP Member Services
mdavis@nacsonline.com
(888) 843-5705

The Association for Convenience & Petroleum Retailing