The Petroleum Marketer's PCI compliance Reference Guide

1. Become familiar with the 12 standards of card data security:

- **Build and maintain a secure network**
  - Requirement 1 – Install and maintain a firewall configuration to protect data.
  - Requirement 2 – Do not use **vendor-supplied defaults** for system passwords and security parameters
- **Protect cardholder data**
  - Requirement 3 – **Protect stored data**
  - Requirement 4 – Encrypt transmission of cardholder data and sensitive information across public networks
- **Maintain a vulnerability management program**
  - Requirement 5 – Use and regularly update **anti-virus software**
  - Requirement 6 – Develop and maintain secure systems and applications
- **Implement strong access control measures**
  - Requirement 7 – Restrict access to data by **business need-to-know**
  - Requirement 8 – Assign a **unique ID to each person** with computer access
  - Requirement 9 – **Restrict physical access** to cardholder data
- **Regularly monitor and test networks**
  - Requirement 10 – Track and monitor all access to network resources and cardholder data
  - Requirement 11 – **Regularly test** security systems and processes
- **Maintain an information security policy**
  - Requirement 12 – **Maintain a policy** that addresses information security

Notes to myself:

Much like healthily life styles, or responsible home ownership, PCI Compliance is MORE about adopting good habits and safe behaviors than anything else.

2. Be familiar with what can and cannot be stored in a POS system.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

** These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*

*** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).*

Notes:

There is also a "Good List" of PCI compliant software companies, I can visit on Visa's Website: http://www.usa.visa.com/merchants/risk_management/cisp_payment_applications.html If I don't see what I am looking for, I can always contact the software company to find out. If they tell me that they are PABP compliant, they should have a letter they can share with me from VISA certifying them to this standard.

I have to fill out the Self-Assessment Questionnaire on http://www.pcisecuritystandards.org both after the upgrade and each year. I will keep the most current copy in my PCI folder.

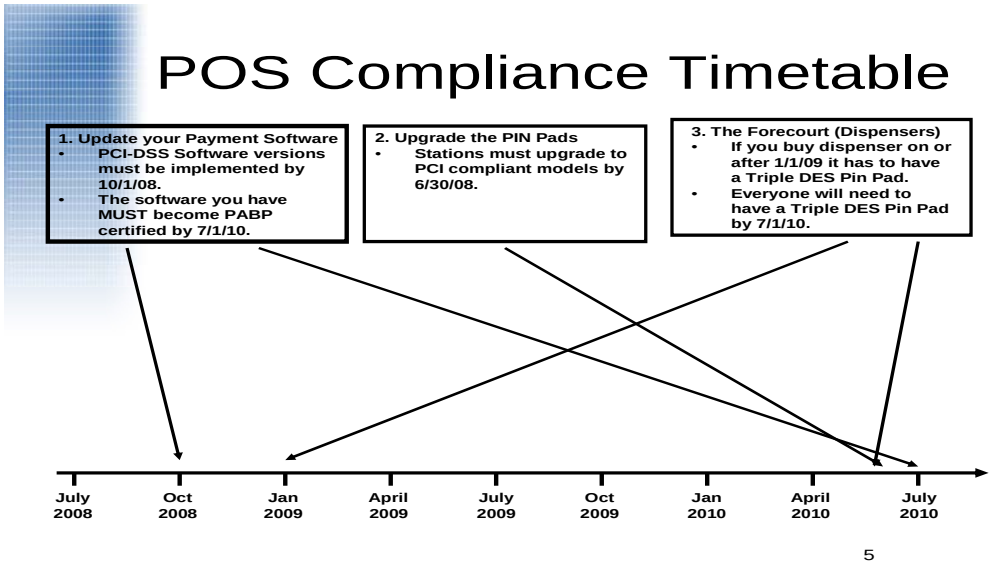
G-site is no longer available to unbranded stations in a PCI version. If I have a G-site product, I will need to upgrade it.

3. TIMELINES (What are the PCI deadlines that concern my business?)

Processor Network and Software Company

Phase	Proposed Mandate	Effective Date
I	Newly boarded merchants may not use applications with known vulnerabilities	01/01/2008
II	Payment networks must only certify PA-DSS-validated payment applications	07/01/2008
III	Newly boarded Level 3 and **Level 4** merchants must be **PCI DSS compliant** or use **PA-DSS validated applications**	**10/01/2008**
IV	Payment networks must decertify known vulnerable payment applications	01/01/2009
V	Members must ensure their merchants use **Payment Application Best Practices (PABP)** validated applications	07/01/2010

The Petroleum Marketers Timeline



Notes to myself:

MY SOFTWARE: I should make sure that I have a PCI compliant system in place no later than **October 1, 2008.** (Ruby=Version 4 / Passport=Version 6 or 7 / Dresser Wayne Nucleus = Version 2)
At my dispenser: • If I am getting brand new dispensers after 1/1/2009, they **MUST** have **Triple DES encrypted PIN PAD overlays.** • If I don't buy any, I **MUST** replace my old ones with **Triple DES encrypted overlays no later than 7/1/2010**
For my register PIN PADS: I need to make sure to have VISA PED or PCI PED Terminals no later than 6/30/2010. (Good ones to have are: Hypercom 1300, Verifone 1000SE-2, MX800's and Ingenico 3070.

MY Steps to becoming the PABP compliant:

What are the steps I should take to become compliant? [PA]

Define Your Point A →
- -Look To CISP Good List
- -Take Inventory of your POS Hardware / Software

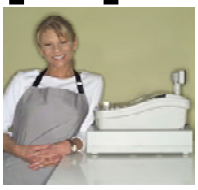
Understand Where you need to be →
- -Contact Equipment Co. for a Site survey
- -Take Self-assessment
- -Get cost quote

Execute to Plan →
- -Install Software
- -Install Hardware where required.
- -TAKE THE USER TRAINING

1

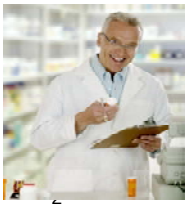
What are the steps I should take to remain compliant? [BP]

Use your Point of Sale Safely →
- -Follow recommended user/admin/manager functions
- -Avoid making short cuts
- -Regularly change difficult Passwords



Secure your hardcopies →
- -Lock box customer receipts
- -Destroy all hand written notes of card numbers

Follow the prescriptive →
- -Take self assessment annually
- -User scanner services from a if DSL
- -Ask Equipment co to periodically inspect your devices when on site

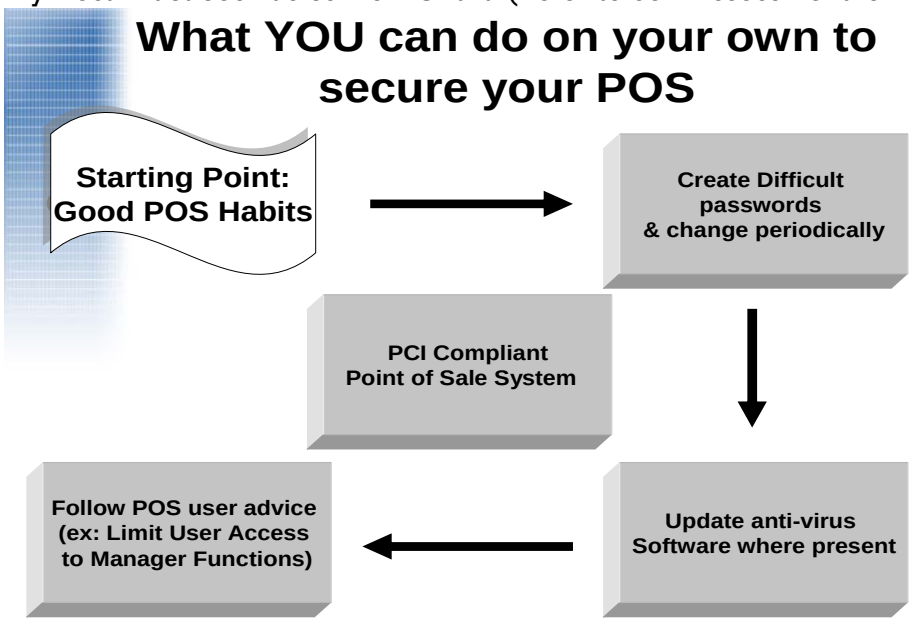


2

Notes:

For Scanning Services I can contact Trustwave. www.Trustwave.com Phone number is: 888-878-7817

My **B**est **P**ractices Basics Flow Chart: (Refer to Self-Assessment for more details)



Notes:

If I find a security breach or an attempted breach, I should contact my equipment provider and my credit card processor. Chase Paymentech's PCI compliance reporting officer is: **Veronica Murphy - 214-849-3257**.