Credit Card Industry Overview

PCI-DSS Compliance

Jeff Herman, Chase Paymentech
September 10, 2008

Outline of Discussion Topics

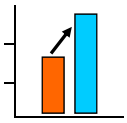
I. The severity of data security breaches.

II. The PCI Security Standards Council and their requirements

III. POS Companies in the Petrol Industry & Compliance

IV. The Petroleum Marketer's roadmap to becoming Compliant

V. The Petroleum Marketer's roadmap to staying Compliant



PCI Compliance for Petroleum Marketers

Petroleum Marketers should understand PCI Security issues impacting:

1. Payment at the fuel dispenser
2. Payment inside the store at the register
3. Hard copy documentation containing card info

Petroleum Marketers need to understand PCI Security Requirements involving

1. Their Industry
2. The map to being compliant
3. How to remaining compliant

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

3

Payment Card Industry Terminology

- PCI-SSC
  - Payment Card Industry Security Standards Council
- PCI-DSS
  - Payment Card Industry Data Security Standards
- PA-DSS
  - Payment Application Data Security Standard
- PABP
  - Payment Application Best Practices
- Payment Brands' Data Security Programs
  - CISP - Visa **C**ardholder **I**nformation **S**ecurity **P**rogram
  - SDP - MasterCard **S**ite **D**ata **P**rotection
  - DSOP/DISC - AMEX and Discover Data Security Programs

POS Software

4

CHASE Paymentech

I.

The severity of security breaches

PMCI
PETROLEUM MARKETERS AND CONVENIENCE STORES OF IOWA

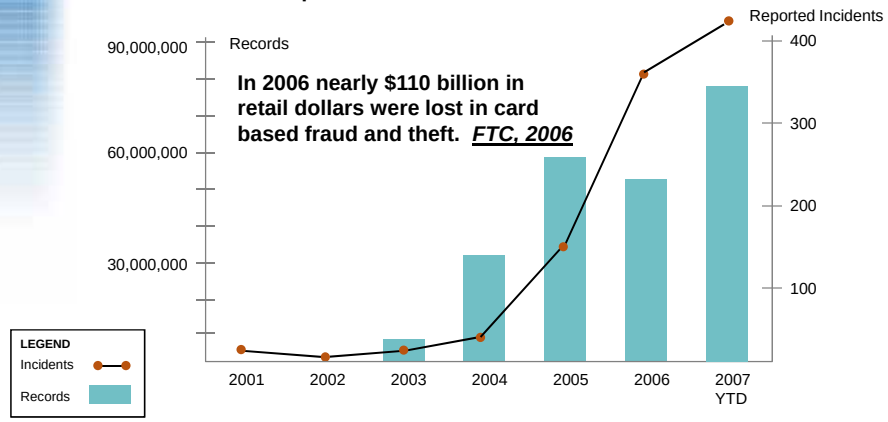
5

Compromises

6

Data compromises on the rise in the US

Increasing data breaches has resulted in a sharp rise in reported security compromises. Card based fraud represents 33% of all fraud activities.

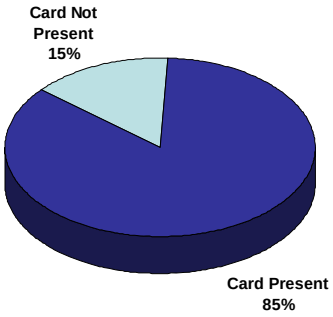


Source: www.etiolated.org – Includes all reported data compromises

7

Myth v. Reality

***Myth:* "Breach incidents happen more often in the dot.com world."**



REALITY:

- About 5 out of every 6 cases is a traditional Brick and Mortar environment.
- Card Present Merchants are not aware of these risks!

Data Provided by Verifone & Trustwave

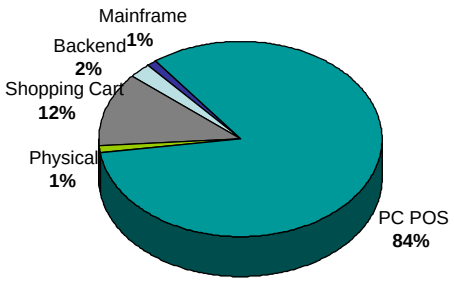
8

Myth v. Reality

Myth: **"*Breach incidents happen outside of my Point of Sale somewhere in the Netherworld"**

REALITY:

- Majority of the cases involved a compromise of a PC based POS system.
- None of these systems were PCI DSS compliant.

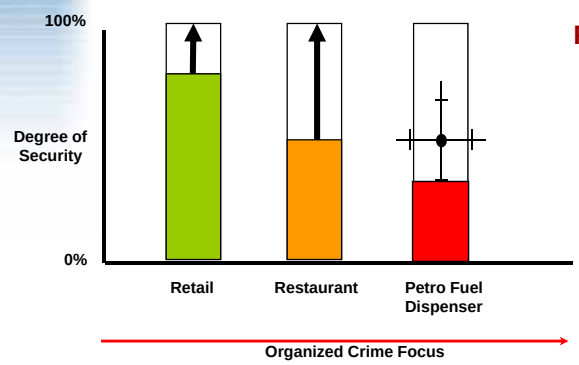


Data Provided by Verifone & Trustwave

9

Myth v. Reality

Myth: **"*The risk of POS breach incidents are greater in the other industries.***



REALITY:

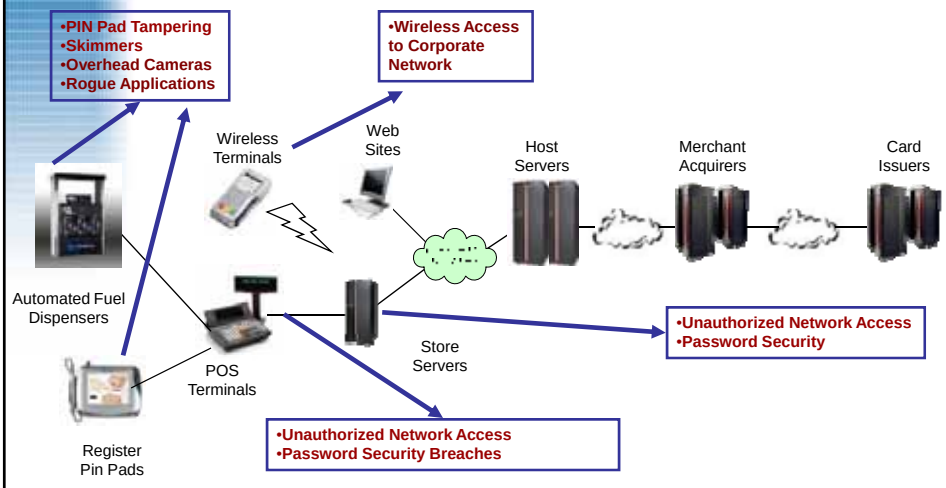
Gas stations with their unattended pumps are considered to be the weakest link in the security chain…

Gartner, Inc."

Data Provided by CSP News 6/07

10

Petroleum Marketers: Payment System Vulnerabilities



11

Organized crime rings are becoming savvy

- **Objective:** To obtain magnetic stripe data & PIN #'s.

- **The Means Used:**
  - Gel Overlays(Key Pad Covers)
  - Skimmers (Internal to Pump OL)
  - Tappers (Data Storage)
  - Wireless Devices (RT Transmission)
  - Bugs Inserted into Non-PCI registers & Pin Pads

- **Goal:** To manufacture Counterfeit cards

12

Forensic Investigations

13

CHASE Paymentech

II.

The PCI Standards Council and their requirements

PMCI
PETROLEUM MARKETERS AND CONVENIENCE STORES OF IOWA

14

PCI Security Standards Council

- The organization
  - Mission — Enhance security through Standards
  - 5 major payment brands
  - 21 member advisory board
  - 275 participating organizations
- Scope of Mission
  - Develop uniform PCI Data Security Standards
  - Develop Qualified Software Vendor list
  - Develop Approved Scanning Vendor list
  - Develop Qualified Security Assessors list
  - Create Path of Security Standards in the Future

15

PCI-DSS Compliance in a Nutshell

A. For all Credit Card Processors:

- Processor networks to have firewalls,
- Data encryption, secure transmission,
- Observe the committee's certification/decertification rules,
- Educate partners and clients on PCI-DSS compliance

B. POS Software Developers:

- Write POS software code to eliminate risks of security breaches.
- Create encryption elements in devices.
- Establish a physical impossibility.

C. For Business Owners:

- Must upgrade systems to compliant versions.
- Must use their POS responsibly.
- Must engage in safe behavior respecting other aspects at their site.

16

What does not fall within the PCI-DSS Compliance Rules?

A. Dishonest Clerks and Aggressive Felons:

Ex: Clerk jots down card number from customer for later use.

Ex: Felons breaking in at to forcibly remove secured information.

B. Web server Software hosted by a Network:

Ex: Internet based credit card terminals.

C. Terminals:

Ex: Eclipse, Omni, Hypercom

17

The 12 PCI DSS Standards

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

18

Prohibited Data Storage in POS Software

	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

Data Watermark

Security Required

Prohibitive Data

What Happens If I am found to be using software that stores prohibitive data or fails to secure permissible data?

Station Owners using non-compliant applications are:

- **NOT** compliant with the PCI Data Security Standards
- At an elevated risk of compromise
- Subject to increased fines ($184 per card replacement & $5,000 per mo.)

19

CHASE Paymentech

III.
POS Companies in the Petrol Industry & Compliance

PMCI PETROLEUM MARKETERS AND CONVENIENCE STORES OF IOWA

20

List of What To Do at the POS

3 Key areas

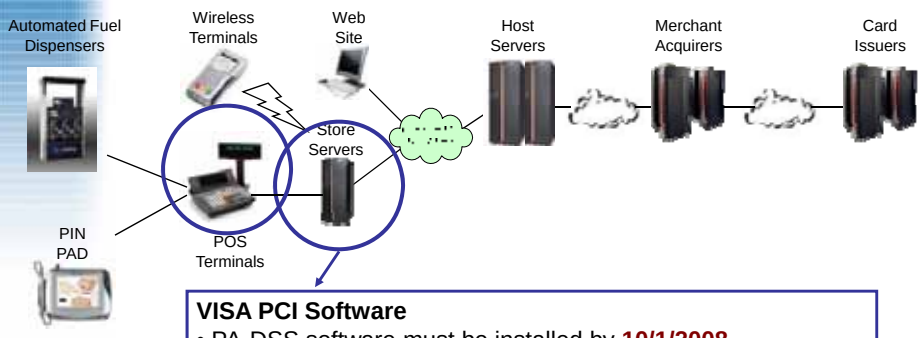
1. **Update your Payment Software**
   - Replace non-PABP Applications & Systems

2. **Upgrade the PIN Pads**
   - Replace outdated Pin Pads at the register.

3. **Secure the Forecourt (Pumps)**
   - Replace outdated dispenser kits at the Pump.

21

PCI (Payment Applications)



VISA PCI Software
- PA-DSS software must be installed by **10/1/2008**
- Final PABP certification of software by **7/1/2009**
- Must have Security features
- Must comply with data storage requirements
- **Manufacturer Responsibility to develop**
- **Penalty to dealer for non-compliance**

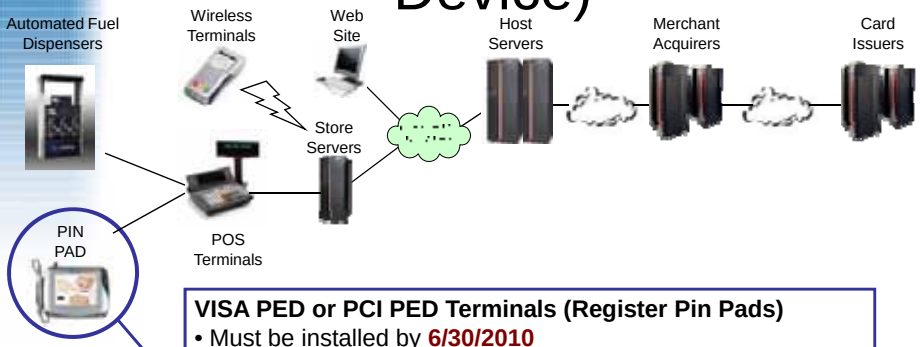
22

Payment Applications

VUNERABLE APPLICATIONS	PA-DSS or PABP COMPLIANT
Dresser Wayne 2000 / Nucleus	Dresser Wayne Nucleus 19
Gilbarco G-site	Passport Version 6 and above
Verifone Ruby Versions 1,2,3	Verifone Ruby Version 4 (CPS)
Petrovend Version 7.8	Petrovend Ver. 8.03 (ETA 9/15/08)

23

PCI PED (PIN Encrypting Device)



VISA PED or PCI PED Terminals (Register Pin Pads)
- Must be installed by **6/30/2010**
- Prevent Tampering
- Secures PIN Encryption
- Protects Magnetic Stripe Data
- **Manufacturer Responsibility to develop**
- **Penalty to dealer for non-compliance**

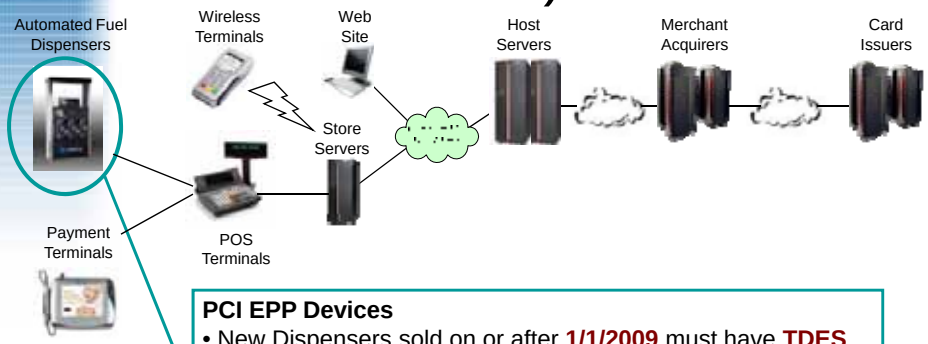
24

Register Pin Pads

VUNERABLE PIN PADS	SAFE PIN PADS
Hypercom S7S & S8	Hypercom 1300
Verifone 101,102,1000,2000	Verifone 1000SE-2
Everest Model P003-3xx	MX830, MX850
Ingenico eN-Crypt 2400	Ingenico 3070

25

PCI EPP (Encrypting PIN Pad)



PCI EPP Devices
- New Dispensers sold on or after **1/1/2009** must have **TDES**
- All existing Dispensers must upgrade to **TDES by 7/1/2010**
- Prevent Tampering Protect Magnetic Stripe Data
- Incorporates TDES form of encryption at the fuel Dispenser
- **Manufacturer Responsibility to develop**
- **Penalty to station owner for non-compliance**

26

Approved EPP Devices

Triple Data Encryption Standard (TDES) Global Mandates:
Visa establishes end-to-end mandates for TDES usage to protect online PIN-based transactions processed at the pumps, as well as other ATM and host systems.

VeriFone - **Secure PumpPAY**

Gilbarco - **Encore S system**

Dresser-Wayne – **PT4000**

Common Characteristics
- Retrofit kits
- Fused parts
- Smaller space
- Buried contacts

27

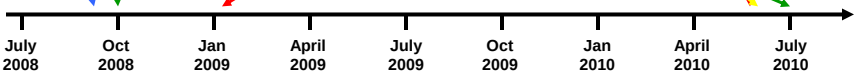
A Final look at each component…

1. Update your Payment Software
- **PCI-DSS Software versions must be implemented by 10/1/08.**
- **The software you have MUST become PABP certified by 7/1/10.**

2. Upgrade the PIN Pads
- **Stations must upgrade to PCI compliant models by 6/30/08.**

3. The Forecourt (Dispensers)
- **If you buy dispenser on or after 1/1/09 it has to have a Triple DES Pin Pad.**
- **Everyone will need to have a Triple DES Pin Pad by 7/1/10.**

PCI Class 9/10/08



28

CHASE Paymentech

IV.
Becoming Compliant

-and-

V.
Staying Compliant

29

PCI-DSS Mandate Timeline

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 (i.e. Applications that are not PA-DSS validated)	01/01/2009
V	Members must ensure their merchants use **Payment Application Best Practices (PABP)** validated applications	07/01/2010

PA

Not just having the system

BP

But using it wisely

30

Validated **P**ayment **A**pplications Standard

- Published monthly since 2005
- 195 applications from 101 vendors certified as of Sept. 2007
- Also know as “the Good List”
- Certificates will be issued to POS companies


VISA List of Validated Payment Applications

As of October 15, 2007

31

Merchant Validation Standard Level 4 (For **B**est **P**ractices)

VISA USA / MasterCard Merchant Levels	Validation Actions		
Level Merchant Level Criteria	On Site Security Assessment	Self – Assessment Questionnaire	Network Vulnerability Scans
Level 4 Less than 20,000 e-commerce or less than 1 million transactions from any acceptance channel annually with one card brand	Not Applicable	Required Annually (submission to acquirer not mandatory)	Required Quarterly (submission to acquirer not mandatory)

Most Station Owners

Complete Annually & Retain

For DSL communicators

32

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

33

Where to find them

- Validated Payment Applications list/ PABP (Good List)
  - www.usa.visa.com/download/merchants/validated_payment_applications.pdf
- Self Assessment
  - www.pcisecuritystandards.org/tech/instructions.htm

See your Appendix for hard copies

34

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

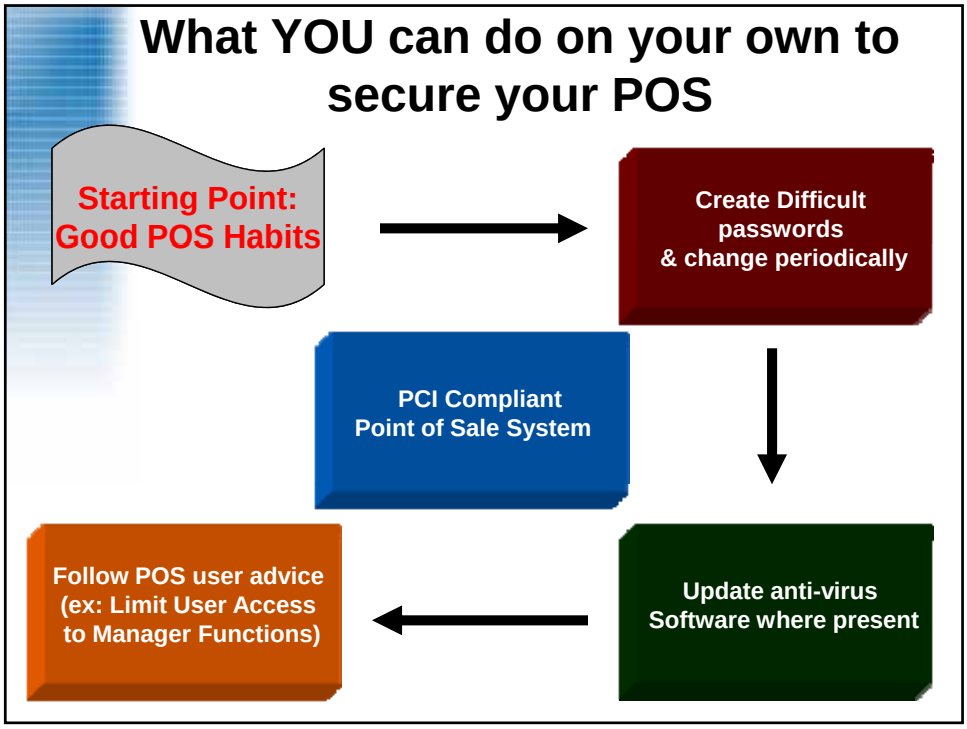
-Take self assessment annually
-User scanner services from a if DSL
-Ask Equipment co to periodically inspect your devices when on site

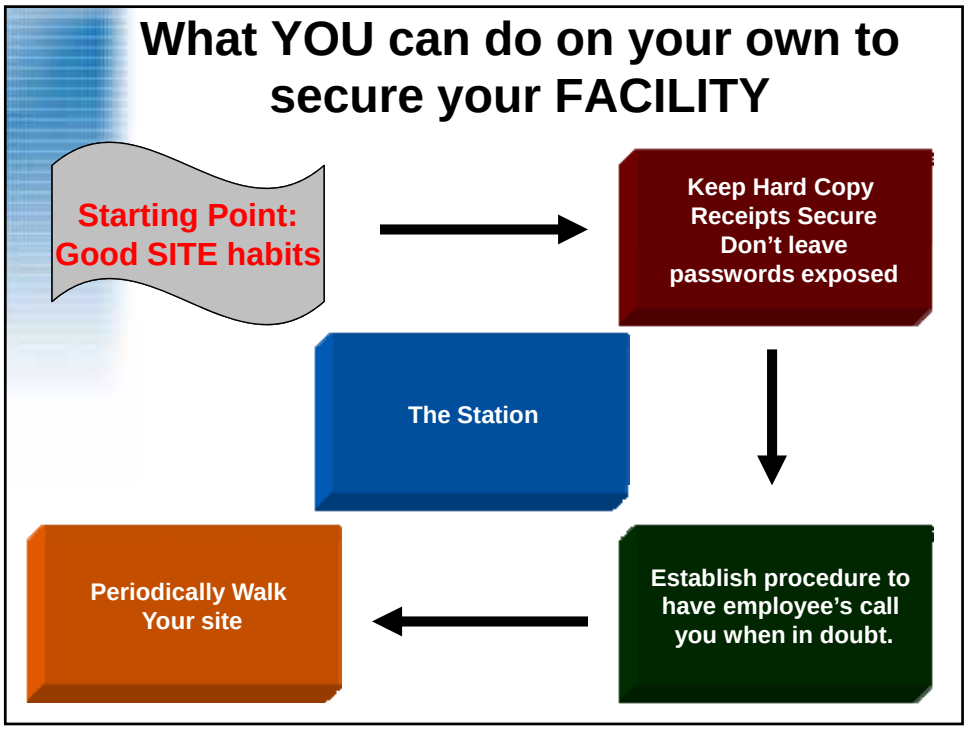
Where to find them

- Scanner services for DSL connections (Trustwave)
  - www.trustwave.com
    - Monthly Internet-facing network scans
    - **Annual subscription services are reasonable $250 per year**
- Other Trustwave Programs Offered (Not Required)
  - Risk Profiler (free service)
    - Risk Ranking results
  - Trustkeeper
    - Annual Self Assessment questionnaire
  - Security assessments and consultation

See your Appendix for hard copies

36


What YOU can do on your own to secure your POS
Starting Point: Good POS Habits
Create Difficult passwords & change periodically
PCI Compliant Point of Sale System
Update anti-virus Software where present
Follow POS user advice (ex: Limit User Access to Manager Functions)


What YOU can do on your own to secure your FACILITY
Starting Point: Good SITE habits
Keep Hard Copy Receipts Secure Don't leave passwords exposed
The Station
Establish procedure to have employee's call you when in doubt.
Periodically Walk Your site

What to do if you uncover a security breach

If breach is of a physical nature:

- Call local police to document incident
- Call your credit card processor
  Chase Paymentech
  Veronica Murphy - 214-849-3257
- Contact customers that you believe are impacted.

If breach is of a technical nature:

- Call local equipment provider with the description.
- Have yourself or your equipment provider disable device.
- Call your credit card processor.
  Chase Paymentech
  Veronica Murphy - 214-849-3257

39

Thank you!

Any questions please contact:

Jeff Herman

CHASE Paymentech

Tel: 763-428-8682

e-mail: jeff.herman@chasepaymentech.com

PMCI PETROLEUM MARKETERS AND CONVENIENCE STORES OF IOWA

40