

Credit Card Industry Overview

PCI-DSS Compliance

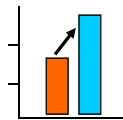


Jeff Herman, Chase Paymentech
September 10, 2008

1 of this document may be used or reproduced without the written permission of Chase Paymentech Solutions

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 healthy 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

I.

The severity of security breaches



Compromises

washingtonpost.com
Marriott Discloses Missing Data Files
 Backup Tapes Lost At Time-Share Unit
 By Michael S. Rowland
 Washington Post Staff Writer
 Washington, December 20, 2005, 600
 Marriott International Inc.'s time-share division said yesterday that it is missing backup computer tapes containing information on the Social Security numbers of about 206,000 time-share owners and customers of the company.

THE WALL STREET JOURNAL
 January 23, 2007
Wide Credit-Card Fraud Surfaces in TJX Hacking
 By ANNE TEKLE
 Issues 11, 387, Page B1
 Fraudulent purchases using credit cards and debit cards issued by TJX Cos. have surfaced in such Jersey plains as Hong Kong and Singapore.

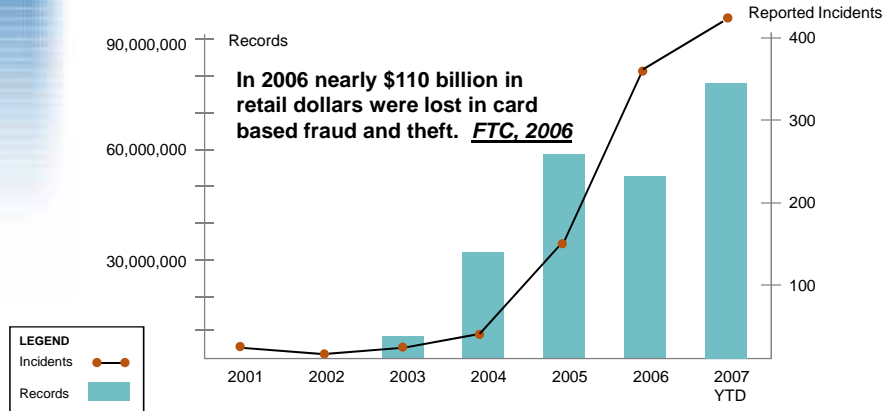
Card firms deal with data theft
 TJX COS.
 In the first signs of such fraud in Japan, a company is warning the public.

B of A: Stolen Laptop Had Customer Data
 Bank of America Corp. has warned some of its Visa Bank prepaid debit card users that sensitive data of theirs may have been compromised by the theft of a laptop.
 In a letter sent to Bank users on Sept. 23, the Charlotte company said that customers' names and credit card bank account, and routing transit numbers might have been compromised by the theft. Social Security numbers were not, however, kept on the computer, spokeswoman Betty Riess said.
 (Visa Bank is a prepaid credit card for nonagency Bank of America stopped selling the card in January.)
 The laptop was stolen Aug. 29 and belonged to a "service provider," Ms. Riess said. B of A was notified of the theft Sept. 9 by the service provider and began alerting consumers after a two-week investigation, she said.
 Ms. Riess said that the computer held only "a very small number" of customer accounts, and that so far there is no evidence that any have been affected.
 B of A is providing a year of free credit-monitoring services to those customers who may be affected by the breach, she said.
 In March the company confirmed that an identity-theft ring had accessed about 60,000 customer accounts. A month earlier B of A revealed that it had lost digital tapes containing the credit card account records of 1.1 million federal employees.

Security breach is wider than thought
 Skimming Devices Target Debit-Card Holders
 The Wall Street Journal
 Issues 11, 387, Page B1
 Skimming devices are targeting debit-card holders, not just credit cards, according to a new report from the Federal Reserve.

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.

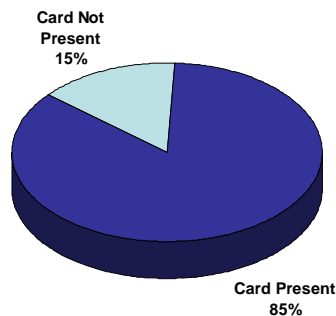


Source: www.etiolated.org – Includes all reported data compromises

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

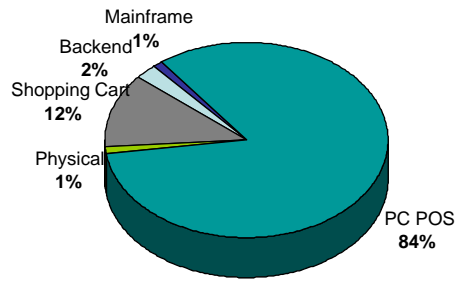
8

Myth v. Reality

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

REALITY:

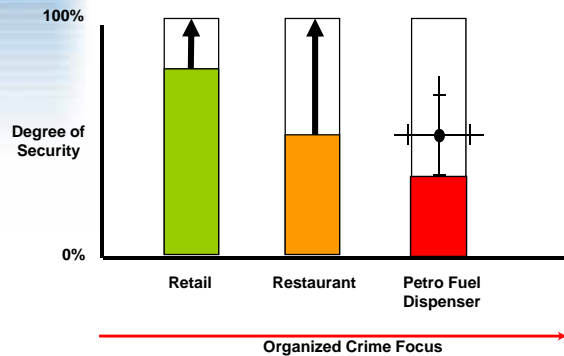
- Majority of the cases involved a compromise of a PC based POS system.
- None of these systems were PCI DSS compliant.



Data Provided by Verifone & Trustwave

Myth v. Reality

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



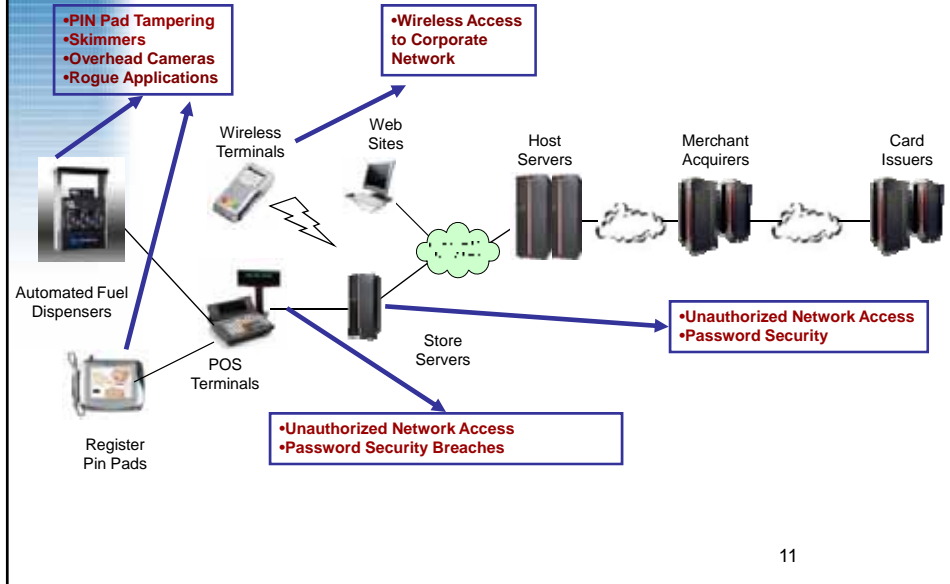
REALITY:

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

Petroleum Marketers: Payment System Vulnerabilities



Organized crime rings are becoming savvy

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

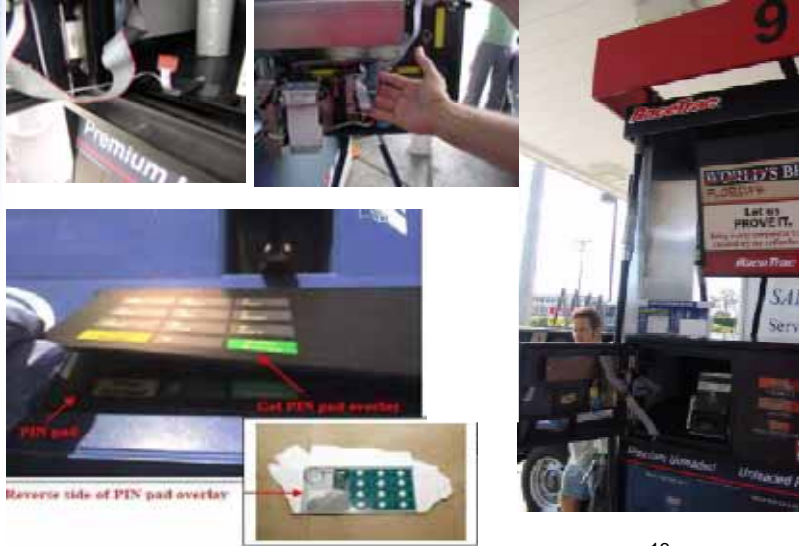
- **The Means Used:**

- 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

Forensic Investigations



13

CHASE
Paymentech

II.

The PCI Standards Council and their requirements

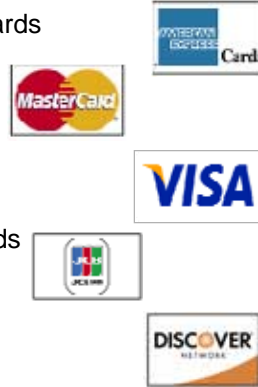
PMCI
ESTABLISH MARKETS AND
CONVENIENCE STORES OF JAPAN

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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored data. 4. Encrypt transmission of cardholder data and sensitive. Information across public networks.
Maintain a vulnerability management program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.
Implement strong access control measures	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 10. Track and monitor all access network resources and card holder data. 11. Regularly test security systems and processes.
Maintain an information security policy	<ol style="list-style-type: none"> 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	Security Required
	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	Prohibitive Data
	CVC/CVV2/CID	NO	N/A	N/A	
	PIN / PIN Block	NO	N/A	N/A	

Data Watermark

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 INDIA

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.



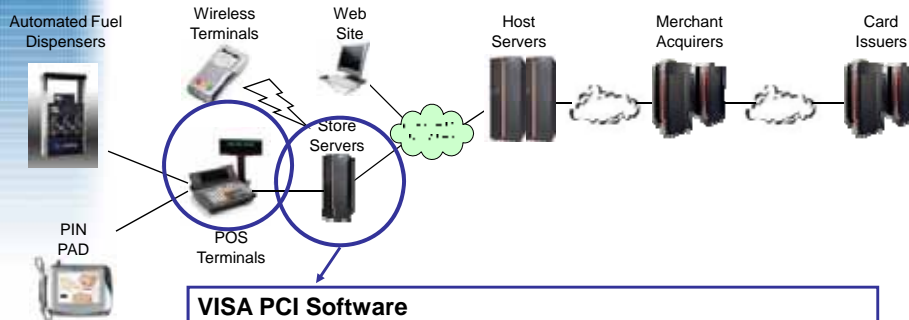
3. Secure the Forecourt (Pumps)

- 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**

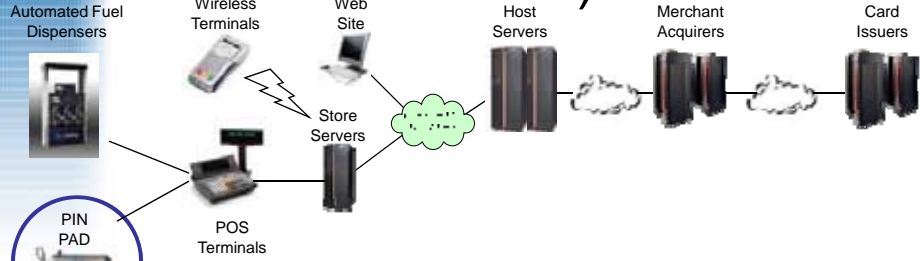
22

Payment Applications



VULNERABLE 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)

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**

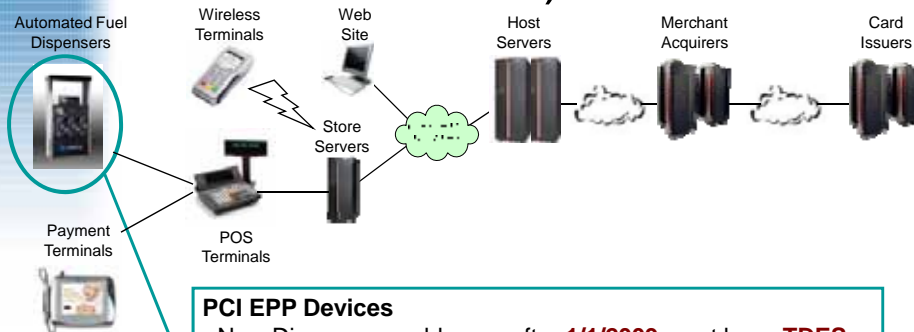
Register Pin Pads



VULNERABLE 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.

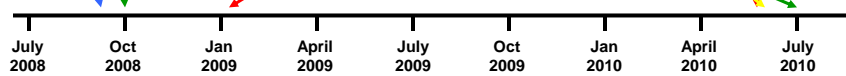
2. Upgrade the PIN Pads

- 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

IV. Becoming Compliant

-and-

V. Staying Compliant

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



Validated Payment Applications Standard

VISA List of Validated Payment Applications

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

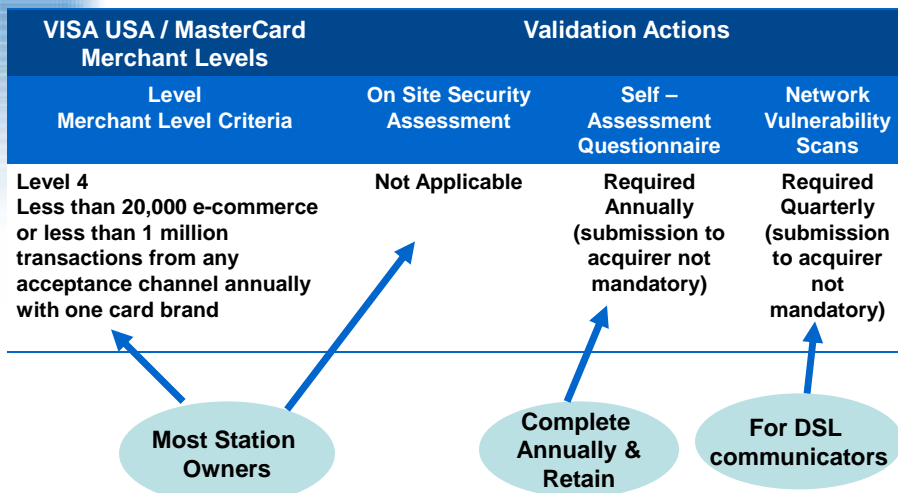
As of October 15, 2007

Information on this list indicates only that the applicable version of payment application has successfully completed an assessment following Payment Application Best Practices. Please be advised that this does not indicate the involvement of applications or products or each of their respective developers or distributors and disclaims all warranties, express or implied. Members remain responsible for performing their own evaluation and due diligence, to ensure the full compliance of their merchants and service providers. The applications reviewed here may be only one component of a suite of payment applications, with the suite consisting of other vendors' products or programs that have not been reviewed. To be a fully compliant solution, all applications in a payment suite must first undergo this same review. VISA has not evaluated and does not express any opinion as to the compatibility or effectiveness of any other vendor's products or programs when used in conjunction with another vendor's payment application.

STATUS: Releases are valid for one year, with annual re-evaluation due to VISA a one year from the below "VALIDATION DATE". Additions that are from 1-60 days late are noted in **green** and reports that are from 60-90 days late are noted in **red**. Entries with reports over 90 days past due will be removed from the list.

SOFTWARE VENDOR	PAYMENT APPLICATION	APPLICATION VERSION	VALIDATION DATE (S)	DESCRIPTION
111 Software www.111software.com	ONELINE	2.0.26	JANUARY 13, 2006 (no change)	Payment application processing that offers multiple forms of funds for SECURITY (LOCAL, REMOTE, A/C, CASH, CHECK, PIN, Terminal, and ACP) (not change)
ACT INFORMATION INC. www.actinfo.com	BASE/INTELL	5.2.0	AUGUST 11, 2006 (no change)	TERMINAL/WEB/SMART PROCESSORS
	BASE/INTELL	5.2.0	AUGUST 11, 2006 (no change)	TERMINAL/WEB/SMART PROCESSORS
	BASE/INTELL	5.2.0	AUGUST 11, 2006 (no change)	TERMINAL/WEB/SMART PROCESSORS
	BASE/INTELL	5.2.0	AUGUST 11, 2006 (no change)	TERMINAL/WEB/SMART PROCESSORS
ADRENALIN SYSTEMS INC.	RETAIL/POS	10.1	DECEMBER 31, 2005 (no change)	POINT OF SALE SOFTWARE FOR THE POS SERVICE MARKET.
AMERISYS www.amerisys.com	AMERISYS/POS	1.0 and 1.1	MAY 4, 2005 (no change)	Payment solution for the cellular phone market.
AMT	AMT/POS	3.0	AUGUST 21, 2007	Payment services solution for the banking, education, and government markets. Includes a wide range of services, such as change of address, card, change of price, etc.

Merchant Validation Standard Level 4 (For Best Practices)



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

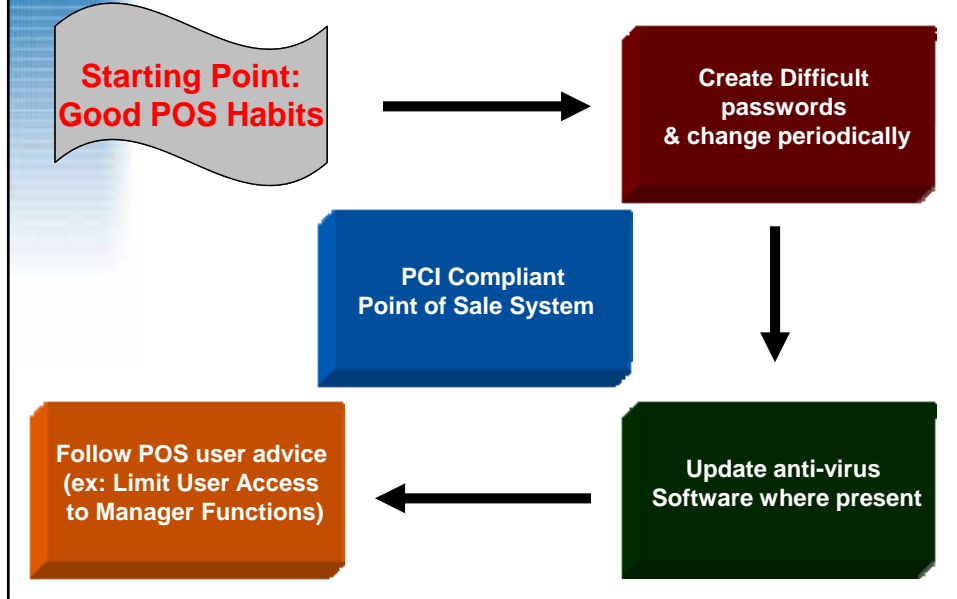


Where to find them

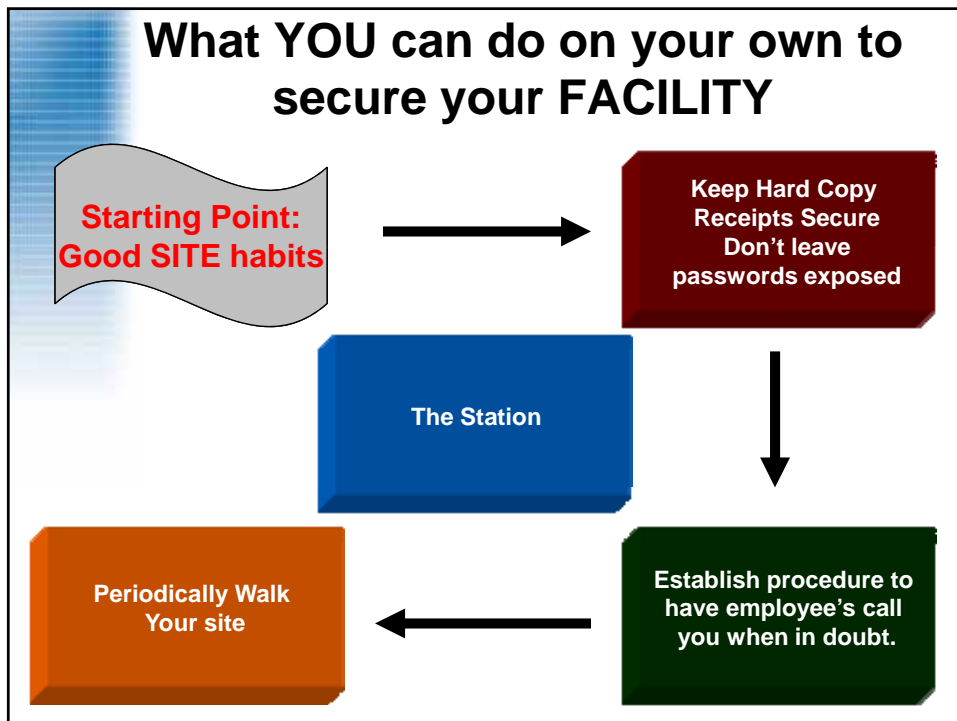
- Scanner services for DSL connections (Trustwave)
 - www.trustwave.com
 - Monthly Internet-facing network scans
 - Annual subscription services are reasonable \$250 per year
- Other Trustwave Programs Offered (Not Required)
 - Risk Profiler (free service)
 - Risk Ranking results
 - Trustkeeper
 - Annual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

See your Appendix for hard copies

What YOU can do on your own to secure your POS



What YOU can do on your own to secure your FACILITY



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



40