

PCI-DSS Compliance: Hardware

May 19, 2009

9:45 a.m. – 10:45 a.m.

Disclaimer

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.

This presentation was prepared by a group of
suppliers and industry consultants.
No authorship is implied.

Presenters:



Scott McDowell, Director of Marketing, Dispenser Applications, Gilbarco Veeder-Root



Mike Tyler, Director of Marketing, Petroleum, VeriFone, Inc.



Tim Weston, Product Manager, Payment Technologies, Dresser Wayne

Moderator:



Lucy Sackett, Director, Marketing Communications, Gilbarco Veeder-Root

Agenda

- Overview of Payment Card Industry (PCI) Standards
- Payment Terminal Standards and Best Practices
- Fuel Dispenser Standards and Best Practices
- POS System Standards and Best Practices
- Summary and Q&A

Payment Card Industry Security Standards Council

PCI PED

Covers PIN Entry Devices at the pump or in the check-out lane

Stand Alone PED Device

PCI PED applies- PED device only



PCI PA-DSS

PA-DSS applies to software vendors who develop payment applications that store, process, or transmit cardholder data

PEDs Integrated with payment applications (POS, ATM)

PA DSS may apply*



Payment Applications (e.g. Shopping cart, POS)

Payment Applications in merchants/ service providers environment**

PCI DSS

PCI DSS applies to any business that stores, processes, and/or transmits cardholder data

Merchants' and Service Providers' cardholder data environment

PCI DSS applies – systems & networks



PCI PED

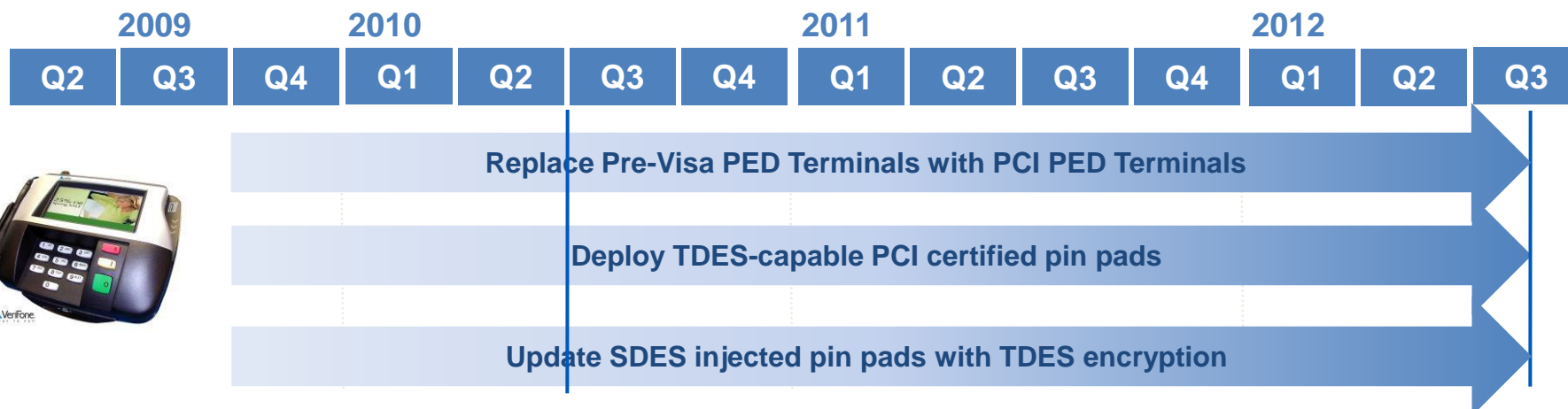
PIN Entry Device Compliance Timeline



Visa is mandating that attended PIN Entry Device terminals adhere to PCI PED standards and implement TDES encryption

What do I need to do?

- Ensure all new pin pads purchased are TDES-capable and PCI certified
- Ensure DUKPT encryption is loaded (either Single-DES or Triple-DES)
- Have Single-DES PIN pads loaded with Triple-DES before 7/1/2010
- Replace Pre-Visa PED Terminals with PCI PED Terminals by 7/1/2010



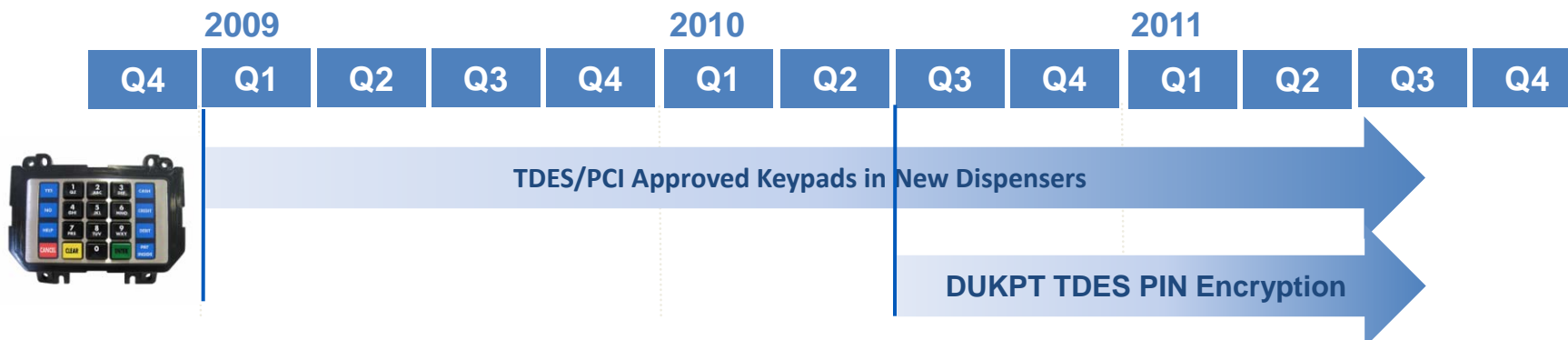
PCI EPP

Automated Fuel Dispenser
Compliance Timeline

Visa is mandating that *new* PIN accepting fuel dispensers adhere to PCI EPP standards to support industry migration to TDES

What do I need to do?

- Ensure all new dispensers purchased include TDES-capable PCI EPP certified keypads
- Ensure DUKPT encryption is loaded (either Single-DES or Triple-DES)
- Understand liability impact (and potential fines) related to PIN compromise involving any use of Single-DES encryption after June 2010
- Consider TDES migration of existing dispensers to maintain liability protection



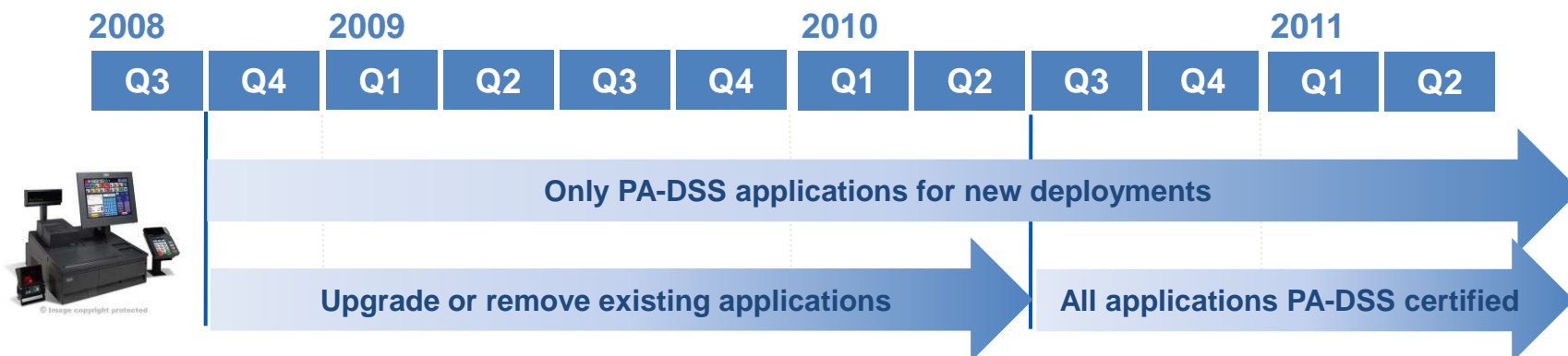
PCI PA-DSS

Payment Application
Compliance Timeline

Visa is implementing a series of mandates to eliminate the use of non-secure payment applications from the Visa payment system.

What do I need to do?

- Ensure all new POS deployments are only with PA-DSS certified POS applications
- Remove all known vulnerable applications from the network by October 2009
- Replace or upgrade existing POS terminals with PA-DSS certified applications before the July 2010 deadline



Payment Security Mandates

**1**

Secure the forecourt
with DES or TDES

- **January 1, 2009**
New dispensers
- **July 1, 2010**
Existing dispensers

**2**

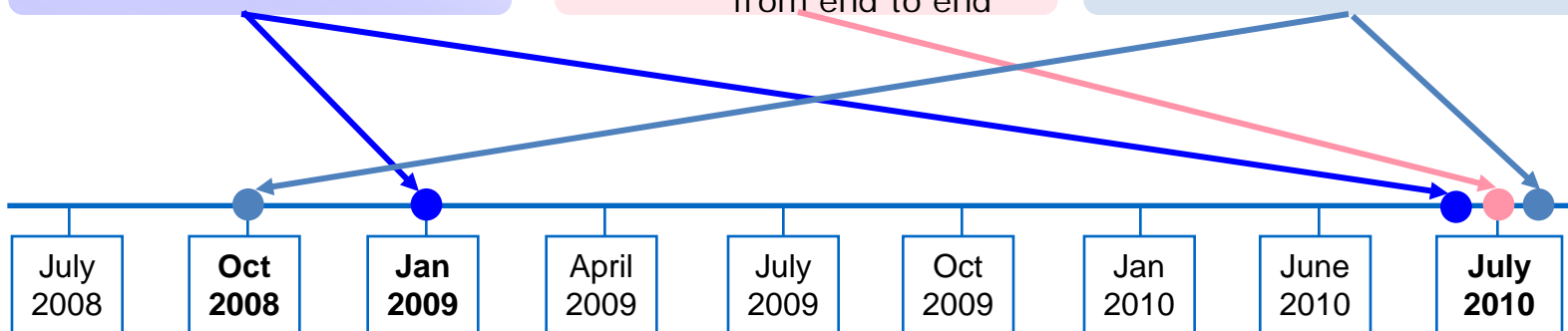
Upgrade to PCI PED
PIN Pads & TDES

- **July 1, 2010**
VISA PED or PCI
PED approved Pin
Pads and TDES
from end to end

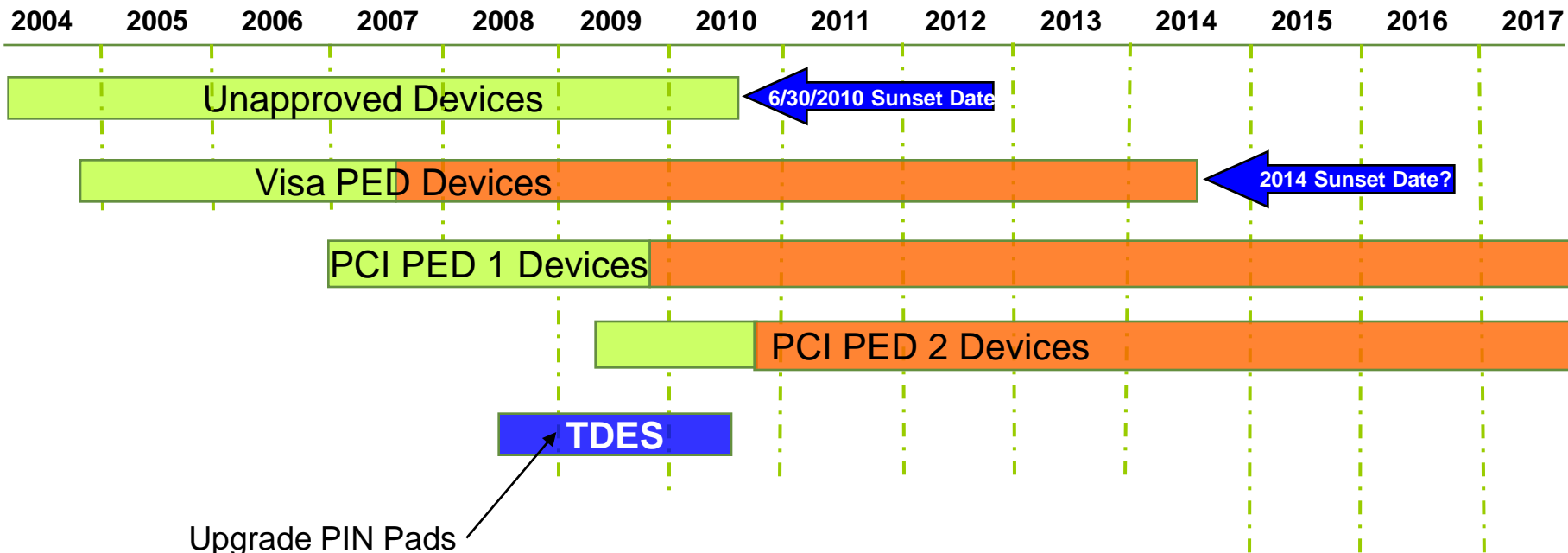
**3**

Update Payment
Software to PA-DSS

- **October 1, 2008**
New Stores
- **July 1, 2010**
All Stores



PCI PED Terminal Timetable



Upgrade PIN Pads

IMPACT: Time your replacement cycles to take advantage of newer terminals with improved security standards. Replace Visa PED in 2013

Legend
OK to Purchase
OK to Use

PIN Pad Security Best Practices

1. Train managers and cashiers on PIN Pad security
2. Weekly visual terminal inspections
3. Visual serial number validation
4. Monitor PIN Pad payment problems
5. Secure terminal storage
6. Terminal asset tracking
7. Do not allow unauthorized service calls
8. Mount PIN Pads securely to counter
9. Install cameras to monitor PIN Pad activity
10. Encrypt data from the PIN Pad
11. Electronic serial number validation
12. Change default PIN Pad password
13. Authenticate applications
14. Maintain employee work schedules for investigations
15. Purchase from authorized sources
16. Use authorized repair centers
17. Develop a Response Plan!

IMPACT: Implement procedural practices immediately. Schedule serial number validation, application authentication and end-to-end encryption during the next POS software cycle.



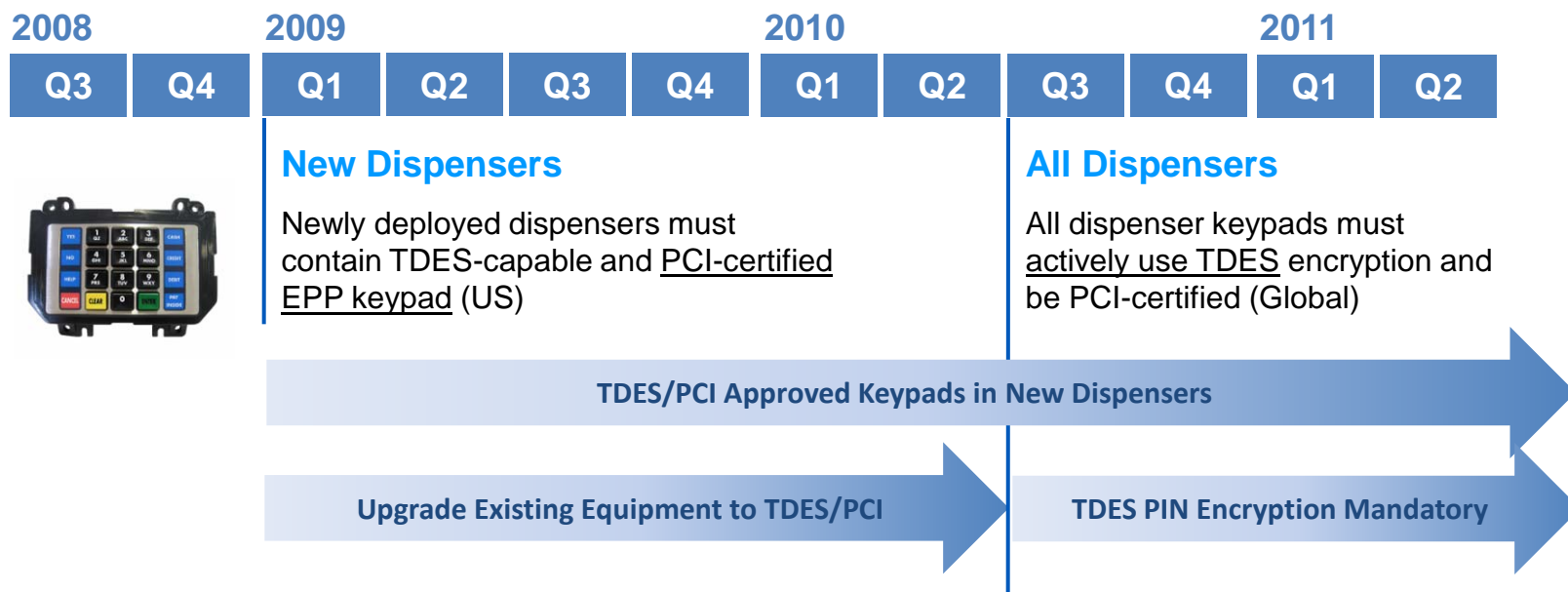
Payment Security at the Dispenser

- Applies to all dispensers that accept PIN debit
 - Requires replacement of the key pad
 - An EPP (Encrypting PIN Pad) or a Payment Device that includes an EPP that is capable of Triple DES Encryption
 - Triple DES keys required to be fully compliant
 - PIN encryption must be done within the keypad
 - Upgrade procedures vary by vendor



Fuel Dispenser Compliance Timeline

Visa is mandating that PIN accepting fuel dispensers adhere to PCI EPP standards to support aggressive industry deadlines.



Visa TDES Enforcement Changes

Updated Enforcement Statement Released
April 22, 2009

The date didn't change...

But enforcement changes give retailers time to comply.

- Key difference – **finer will not automatically be assessed** for retailers using at least **Single-DES or Triple-DES** DUKPT on their dispensers by July 1, 2010.
 - *Previous position required Triple-DES DUKPT to avoid fines*
 - *Use of Master-Session would still be subject to fines*

Visa TDES Enforcement Changes

However...

In the event of a PIN compromise, acquirers will continue to be subject to compromise program liability (in addition to potential fines) if the entity is found to be non-compliant, including any use of Single-DES past July 1, 2010.

- This implies that **retailers willing to assume risk of non-compliance** in the case of a breach **can continue to use Single-DES DUKPT** after the deadline provided there is a plan to upgrade to Triple DES after July 1, 2010.

Visa also cautioned that this enforcement policy is based on the current risk environment and may change with emerging threats.

Choices for Retailers

What options to retailers have?

- Upgrade Dispensers with PCI Encrypting PIN Pads and TDES
- Install new TDES capable PCI compliant fuel dispensers
- Require debit customers to pay in store
- Do nothing now and stop accepting PIN debit as of June 2010
- Assume risk of non-compliance and continue to use Single-DES DUKPT after the deadline

Note: Your Processor or Major Oil Brand may limit your choices



Fuel Dispenser Security Best Practices

1. Periodically change the programming access codes for the dispenser.
2. For areas subject to high risk of theft, add special keys/locks to replace the standard locks.
3. Remove the manager's keypads from the dispensers and store them in a safe location.
4. Monitor and compare 'pump total' and 'station total' reports regularly on the store point of sale and tank monitor.
5. Maintain employee views of the fueling islands because thieves don't like to be seen.
6. Be alert to any pump off-line messages at the POS.

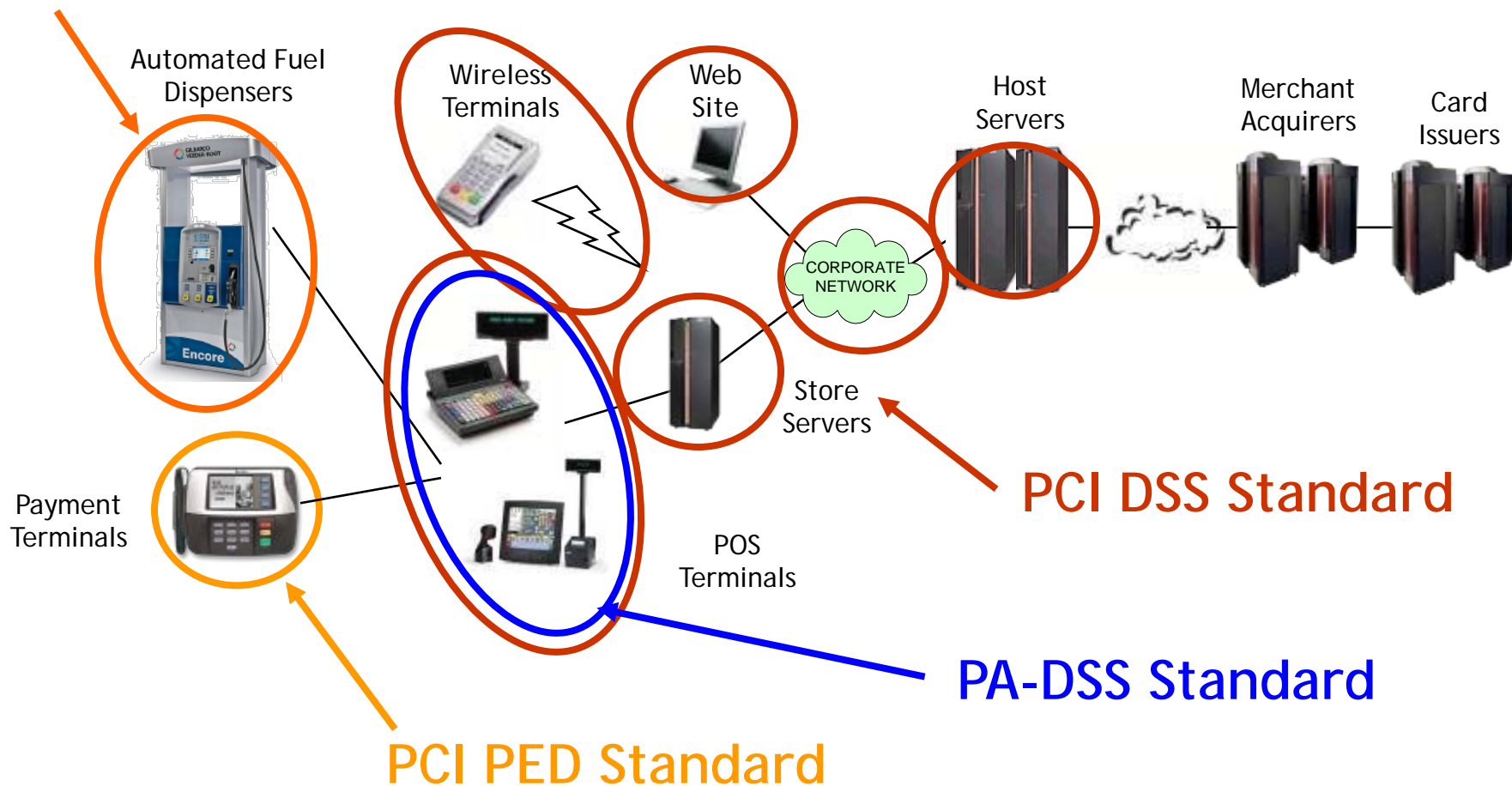


Fuel Dispenser Security Best Practices

7. Be alert to service calls for dispensers that have been 'off-line', which may indicate fraud has occurred.
8. Inspect your site frequently, keeping watch for loose pump faces, doors, stray wires or other parts.
9. Be alert for abnormal traffic patterns on the forecourt.
10. Check the video security camera tape daily for suspicious activity at the pump.
11. Check the POS settings and change settings on any older POS that allows a “hot-authorization feature.”



PCI EPP Standard



Payment Application Data Security Standard (PA-DSS)

- PA-DSS ←—— Visa's Payment Application Best Practices (PABP)
- PA-DSS Applies to:
 - Purchased Applications – not in house or custom development
 - Payment Applications that store, process or transmit cardholder data
 - POS, payment switches, middleware, kiosks, shopping carts, etc.
 - Does not apply to operating systems, database software, routers, etc.
- PA-DSS Requirements Support the PCI DSS Requirements
 - PA-DSS does not mean you are PCI DSS compliant
- PA-DSS Compliance Deadlines
 - No new deployments with non-PA-DSS applications after 10/01/08
 - **All covered applications must be PA-DSS by 7/01/10**

PA-DSS Requirements

PA-DSS consists of 14 primary requirements, with multiple secondary requirements



Payment Application – Data Security Standard

- | | |
|---|---|
| 1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data | |
| 2. Protect stored cardholder data | ✖ |
| 3. Provide secure authentication features | ✖ |
| 4. Log payment application activity | ✖ |
| 5. Develop secure payment applications | |
| 6. Protect wireless transmissions | ✖ |
| 7. Test payment applications to address vulnerabilities | |
| 8. Facilitate secure network implementation | ✖ |
| 9. Cardholder data must never be stored on a server connected to the Internet | |
| 10. Facilitate secure remote software updates | ✖ |
| 11. Facilitate secure remote access to payment application | ✖ |
| 12. Encrypt sensitive traffic over public networks | |
| 13. Encrypt all non-console administrative access | ✖ |
| 14. Maintain instructional documentation and training programs for customers, resellers, and integrators | ✖ |

What Do I Need to Know?

- **Covers the entire software development lifecycle**
- **Focuses on “what” instead of “how”**
- **Includes software applications, infrastructure, procedures, and processes**
- **Responsibility is shared between the vendor and merchant**
- **PA-DSS alone does not insure PCI DSS compliance**
- **Certifications expire, meaning compliance is an ongoing process**



Payment Security Best Practices




Lessons Learned from Recent Breaches

- Review Your Patch Policy
- Monitor Event Logs
- Reduce the Sensitive Data Stored & Protect what is stored
- Use White-listing versus Virus/Malware Scanning

PCI Impact on Petroleum Retail

Three main standards drive PCI Compliance for Petroleum Retail

- **PCI PA DSS: Data protection for credit and debit transactions**
- **PCI PED: PIN protection for debit transactions**
- **PCI EPP: PIN protection for debit transactions**

Standard	Mandate Description	Compliance Upgrade Dates	Compliance Enforcement	Inside Store		Outside Store
				PED 	POS 	
PA DSS	Protect Debit and Credit	New Stores as of 10/1/09	All Stores compliant by 7/1/10		<input checked="" type="checkbox"/>	
PED	Protect debit PIN	Liability Shift 7/1/10	Non-compliance fines may start 8/1/2012	<input checked="" type="checkbox"/>		
EPP	Protect Debit PIN	Liability Shift 7/1/10	SDES or TDES; SDES Liability			<input checked="" type="checkbox"/>

Getting Started

www.pcisecuritystandards.org

- Education (PCI-DSS, PA-DSS, PED, EPP)
 - PCI Security Standards Council
 - PCI Quick Reference Guide
- Self Assessment (PCI-DSS, PA-DSS)
 - Inventory and document site infrastructure
 - Self Assessment Questionnaire
 - Standards Training
- Look at the big picture
- Talk to your Vendors
- Engage a QSA
- Don't wait





Q&A Session