



# **PCI Compliance 101: Developing a Plan for 'Best Practices' in Moving Towards Compliance**

Monday, May 5, 2008

1:15 pm – 2:15 pm

## **COPYRIGHT NOTICE**

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproduction of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be "used for other purpose than private study, scholarship or research." If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of "fair use," that person may be liable for copyright infringement.

## **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.

# PCI Data Security Overview



**Rick Dakin, QSA**  
**Coalfire Systems, Inc.**  
**[Rick.dakin@coalfiresystems.com](mailto:Rick.dakin@coalfiresystems.com)**

**May 5, 2008**

**NACStech**  
NACS PCATS

# Objectives

- Provide an overview of the PCI compliance requirements from an auditor's perspective
- Raise awareness for the cost of compliance failure
- Prepare you for a subsequent Q&A session

# Security Environment

## **Increasing industry, regulatory and legislative focus on security due to high profile data compromises**

- Criminals are targeting full track data, Card Verification Value 2 (CVV2) and PINs in data compromises
- Merchant compliance with the Payment Card Industry Data Security Standard (PCI DSS) is growing among large merchants
- Small merchant education, awareness and compliance efforts are comprehensive and ramping up
- Industry-wide coordination is increasing with the establishment of the PCI Security Standards Council (SSC)
- Legislators and regulators have become involved and there are a number of state laws, as well as pending federal legislative initiatives
- Consumer confidence is impacted by data compromises

# VISA Compromise Statistics

- **Notable increase in compromise frequency:**
  - 2005 – 59 incidents / 5 per month
  - 2006 – 84 incidents / 7 per month
  - 2007 (through October) – 165 incidents / 16 per month
- **56% / 44% split – brick & mortar vs. e-commerce merchants**
  - Brick and mortar compromises involving full track data account for 76% of exposed accounts
  - Food services account for 44% of compromises followed by direct marketing at 7%, universities at 7%, computer equipment at 4% and clothing retailers at 4%
  - In terms of number of accounts exposed, clothing retailers account for 68% of accounts, while food services account for about 2%

## *Russian Hackers*

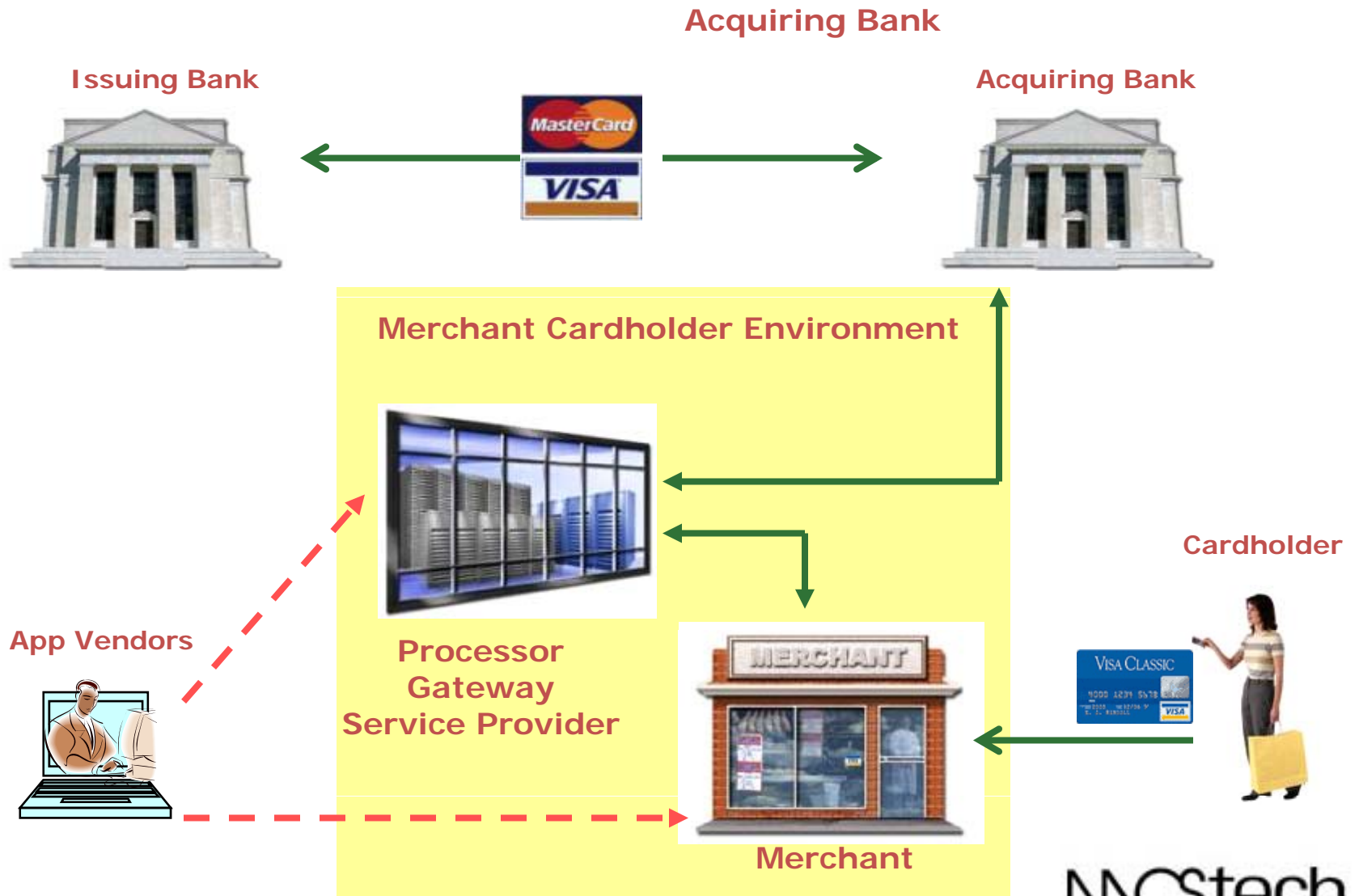


# Stolen Account Data Value



```
[23:56] <ccs4santa> hey  
[23:56] <ccs4santa> u selling fullz and cc# with cvv2?  
[00:03] <makdollar> yes  
[00:04] <ccs4santa> how much for a fullz?  
[00:13] <makdollar> 100$  
[00:14] <ccs4santa> ok..how much for card number and ccv2 info?  
[00:15] <makdollar> same  
[00:16] <ccs4santa> ok..you also sellin bank logins...boa / wells / EU / UK?  
[00:17] <makdollar> yes  
[00:17] <ccs4santa> bank logins vary or...?  
[00:18] <makdollar> wbt?  
[00:20] <ccs4santa> how much for bank logins?  
[00:21] <makdollar> 320$
```

# PCI Relationship Matrix



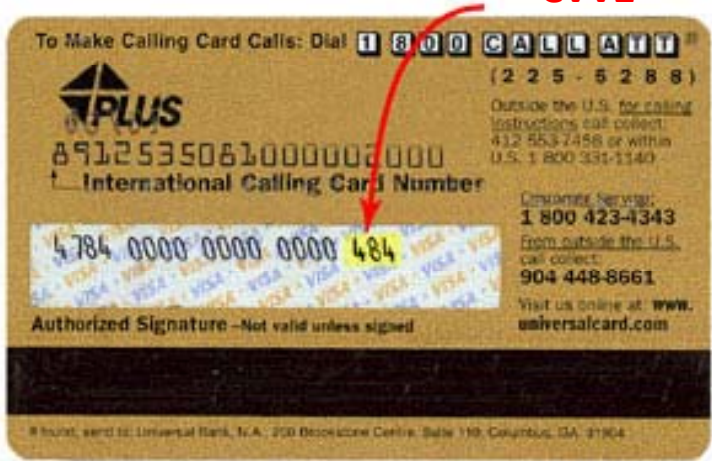
# Prohibited Data



Visa, Mastercard, Discover  
CID Location.



American Express  
CID Location.



Cardholder Verification Number (CVN)  
(CID/CVV2/CVC2)

# *PCI Data Security Standard*

**Build and Maintain a  
Secure Network**


**Protect Cardholder Data**

**Maintain a Vulnerability  
Management Program**

**Implement Strong Access  
Control Measures**

**Regularly Monitor and  
Test Networks**

**Maintain an Information  
Security Policy**

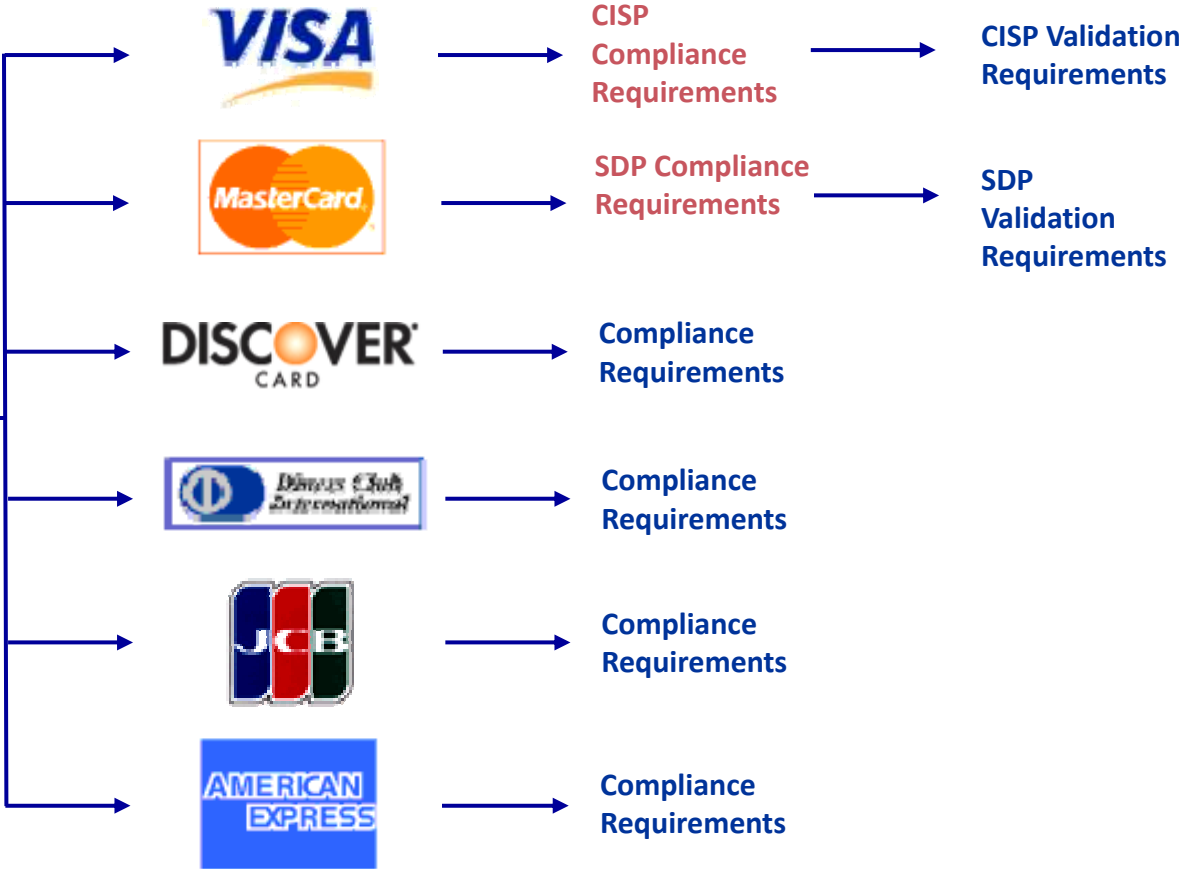


Tested by up to 218  
individual audit criteria

# Industry Alignment to PCI



PCI Security Standards Council



# *PCI Compliance Levels*

**Merchant  
Level 1**

Any merchant processing over 6 million VISA or MasterCard transactions per year OR identified as any card brand as a Level 1 merchant.

**Merchant  
Level 2**

Any merchant processing 1 to 6 million VISA or MasterCard transactions per year.

**Merchant  
Level 3**

Any merchant processing 20,000 to 1 million VISA or MasterCard e-commerce transactions per year.

**Merchant  
Level 4**

Any merchant processing less than 20,000 VISA or MasterCard e-commerce transactions per year, and all other merchants with less than 1 million transactions

# Compliance Validation Requirements

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

# New Self Assessment Questionnaire (SAQ)

According to payment brand rules, all merchants and service providers are required to comply with the PCI Data Security Standard in its entirety. There are five SAQ Validation categories, shown briefly in the table below and described in more detail in the following paragraphs. Use the table to gauge which SAQ applies to your organization, then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. <i>This would never apply to face-to-face merchants.</i>	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone dial-up terminal merchants, no electronic cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A-C above) and <b>all</b> service providers defined by a payment brand as eligible to complete an SAQ.	D

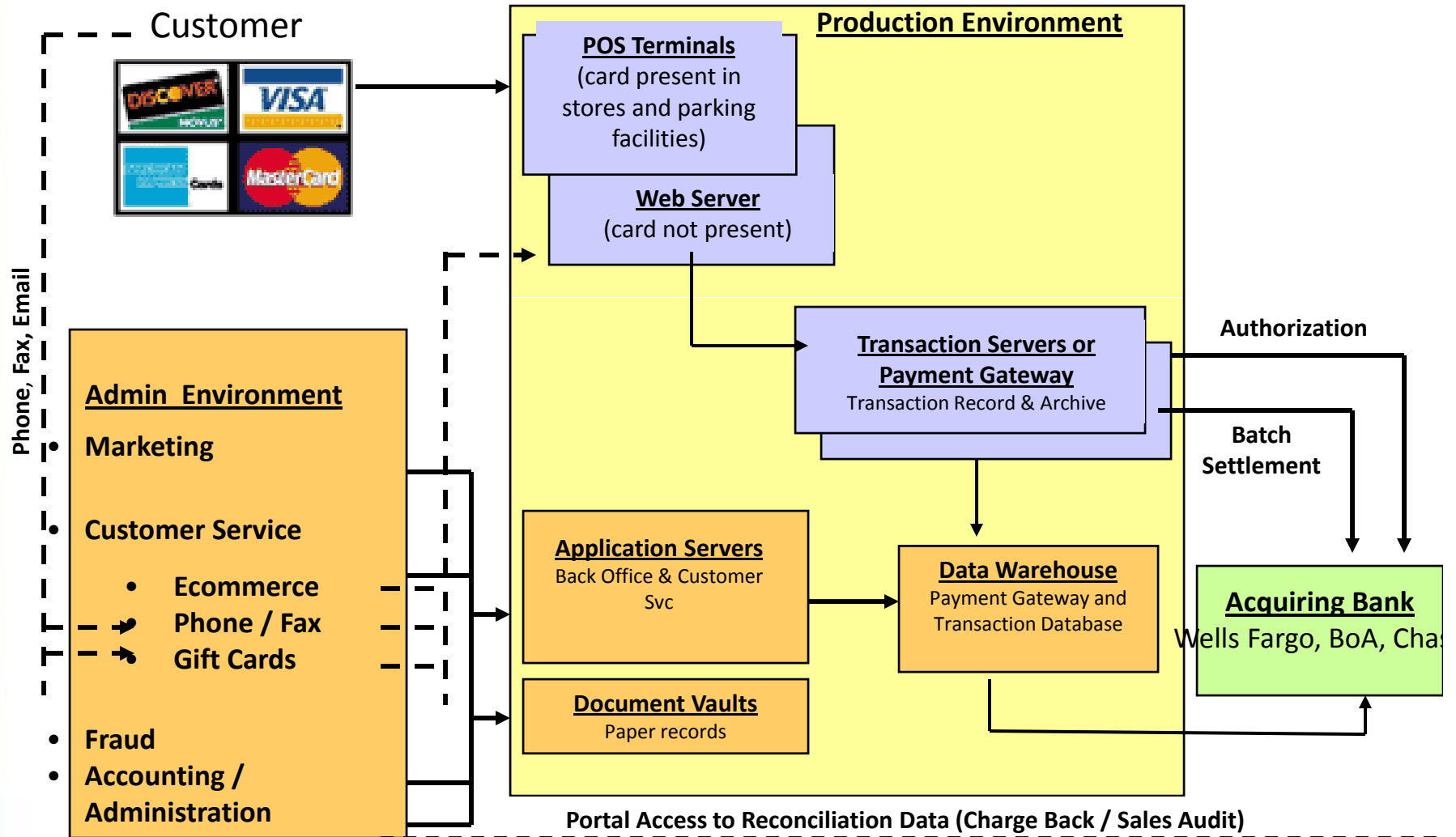
# Cost of a PCI Compromise

A hypothetical merchant compromises 100,000 accounts when a third party service provider has a server stolen.  
What is the potential financial impact?

- Notify Clients and Provide Privacy Guard       $\$50 \times 100,000 = \$5 \text{ million}$
- Fines and Penalties       $\$100,000 \text{ to } \$10 \text{ million}$
- Loss of Clients       $100,000 \text{ clients} - 15\% = 15,000 \text{ clients}$   
 $15,000 \times \$100 \text{ in fees} = \$1.5\text{m in lost fees}$
- Fraud liability       $1,000 \text{ accounts} \times \$500 = \$500,000$
- Reputation Loss      **PRICELESS!**

# Sample Payment Processing Data Flow

Where is the card holder data?





# *New Visa Payment Application Requirements*

*Stay tuned*

*To be covered by another panel member*

## *What can Merchants Do?*

- NEVER ... EVER ... store sensitive cardholder data after transaction authentication – *(Develop a data map)*
- Only deploy PA-DSS certified payment applications *(Replace all Vulnerable Payment Applications )*
- Implement an industry standard method to encrypted Primary Account Numbers (PAN) after authentication
- Maintain mature administrative, technical and physical controls to protect cardholder data
- Maintain and Incident Response Plan and Test It *(The CAMS system may identify your data breach)*
- Test and audit the cardholder environment AND sign the compliance validation attestation

# Compromised? (Using Visa's Procedures)

[http://usa.visa.com/merchants/risk\\_management/cisp.html](http://usa.visa.com/merchants/risk_management/cisp.html)



This *What To Do If Compromised* guide is intended for Visa members. It contains step-by-step instructions on how to respond to a security incident. In addition to the general instructions provided here, Visa may also require an investigation that includes, but is not limited to, providing access to premises and all pertinent records, including copies of analysis

*Thank you*  
*Questions?*

*Knowledge - Action = Risk Acceptance (\$)*



**Safe Harbor** requires validation of compliance at the time of compromise

So far, no compromised account has been compliant at the time of the incident



# Some Basics of PCI Compliance

*James Hervey*

*Global Product Marketing*

*Radiant Systems, Inc.*

# Radiant Systems Overview

- Financially sound and growing
  - 2005 revenues of \$172M and EPS of \$.18
  - Expected 2006 revenues of ~\$210M-\$218M and EPS of \$.48-\$.55
- #2 in Point of Sale shipments worldwide
  - 8,500 terminals per quarter
- Current C-store & Petroleum installation base of 13,000 sites and growing
  - 5,000 sites in progress
- Quick Service Restaurant installation base of 30,000+ sites and growing
- Speed and Security Solution Focus
  - P1550
  - Tiger Fuel Controller
  - Electronic Payment Controller III
  - PABP compliance

# Key Points to Remember About the PCI-DSS

- PCI-DSS is a merchant standard – not a vendor standard
  - POS vendors are PABP-validated (soon to be PCI PA-DSS)
- Vendors play a key role but many aspects of the standard must be addressed by the merchant
- A good PCI strategy requires good communication between the merchant, the assessor and all vendors that touch the cardholder environment
- Remember that all vendors with systems that are part of the cardholder environment will be part of the merchant's overall PCI compliance

# How We Achieve PABP Compliance

- Eliminate ALL 'sensitive' cardholder data immediately upon authorization
- Any cardholder data is stored in TDES-encrypted format and requires the merchant and Radiant to recover
- Provide methods to track and log access to our systems that process data

# What About Software Support

- Do you know who is accessing your site?
- Help desks will need a process where the technician uses two-factor authentication to log into the cardholder environment
- Can you track them once they are in there?
- PCI Section 12.8 requires you to have the conversation

# PCI Requires Securing Machines

- You are responsible for the machines your systems run on
- File integrity monitoring
- Logging
- Log review
- Firewalls
- Antivirus – *OS's that are prone to viruses*
  - *Basically any Windows 2000 or XP OS*
  - *Ensure enough disk space on the machine to make it run*
- Discuss with your vendor how to make these processes work with their systems

# The Future?

- PCI Compliance does not equal 100 percent secure
  - There are still vulnerabilities
- PCI does not require store LANs to encrypt traffic today
  - Can your vendors support this?
  - Radiant is seeing requests from clients to encrypt this traffic
  - How long before this becomes part of the standard?
- PCI does not require store-to-host encryption on private networks
  - Products available today that will encrypt cardholder data to the host
  - How long before PCI requires this?



Gilbarco Veeder Root  
**Dispenser Payment Security**

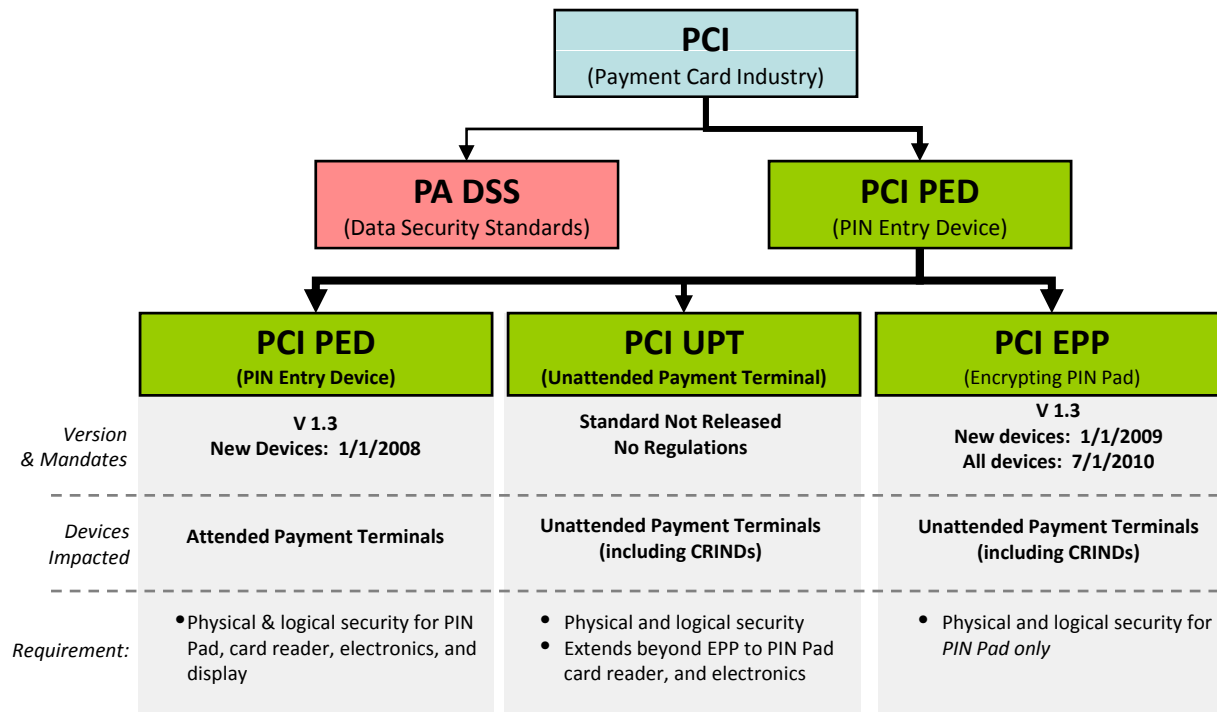
Scott McDowell

Marketing Manager, NA Payment

# Payment Security Mandates Influencing Dispensers

The EPP standard mandates PCI physical and logical security including the encryption of PINs using acquirer Derived Unique Key Per Transaction (DUKPT) keys.

A change to EPP is required for all AFDs taking debit before **July 1, 2010**; all new AFDs need EPP shipping after **January 1, 2009**.



*It is important to note that the only standard for which the card issuers have placed mandates for already installed equipment is PCI EPP*





G1

I made the change to attended vs unattended.

GVR, 12/9/2007

# Retailers have upgrade options...

Retailers have choices to make on the new security requirements for fuel dispensers....

<u>Decision Options</u>	<u>Product Solutions</u>	
No Debit	Is debit worth the upgrade?	
Compliance	PIN Pad only is needed	
Protect Transaction	PIN Pad and SCR protects both PIN and the Card Data	
CRIND™	Modular and Integrated secure CRIND components	

# Needed considerations when choosing your compliant solution...

- *Upgradeable* components that allow flexibility:
  - Upgrade only those components required or desired
  - Maintain other peripherals currently in use (cash acceptors, etc) or easily such additional peripherals in the future
  - Drop into existing real estate to ensure an integrated look and exceptional consumer experience
  - Kits that provide for easy field installation, avoiding costly and complicated field fitting activities

# Build Your Plan to Compliance...

1. Host a meeting with POS, Dispenser, and Bank
2. Complete plan to compliance based on available resources
3. Test PIN Pad solution in lab environment
4. Field Trial security solution at selected site
5. Rollout compliant solution to field
  - Factory Installed Dispensers
  - Retrofit program for legacy dispensers
  - Service and installation support

# Thank You

- Rick Dakin, QSA  
Coalfire Systems, Inc.  
[Rick.dakin@coalfiresystems.com](mailto:Rick.dakin@coalfiresystems.com)
- James Hervey  
Radiant Systems, Inc.  
[james.hervey@radiantsystems.com](mailto:james.hervey@radiantsystems.com)
- Scott McDowell  
Gilbarco Veeder Root  
[scott.mcdowell@gilbarco.com](mailto:scott.mcdowell@gilbarco.com)