

Introduction to PCI –DSS Compliance

May 18, 2009

1:15 p.m. – 2:15 p.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.

Presenter:



Rick Dakin
President & Senior Security Strategist
Coalfire Systems, Inc.

Moderator:

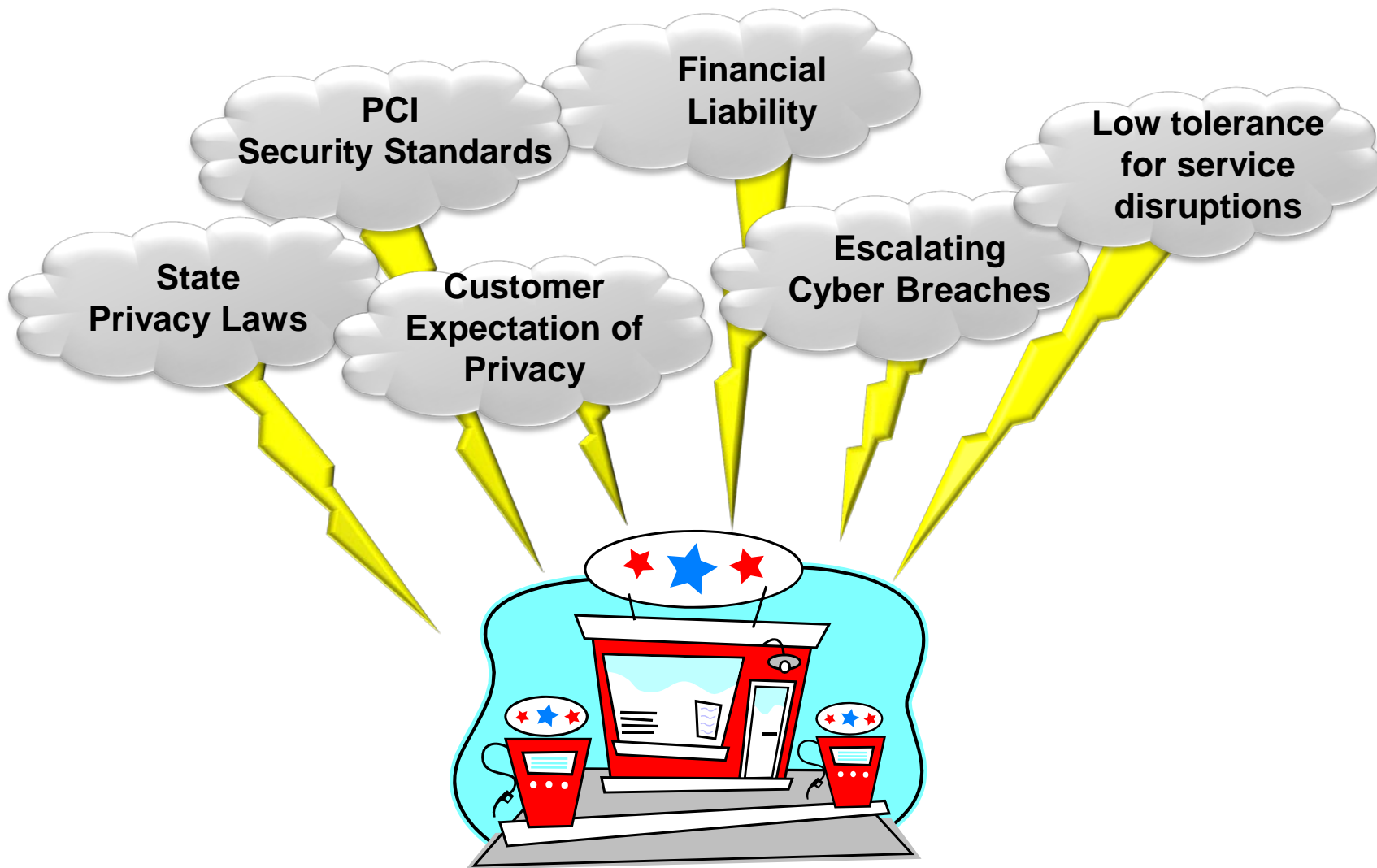


Jack McLaughlin
Director of Information Services
Tedeschi Food Shops Inc.

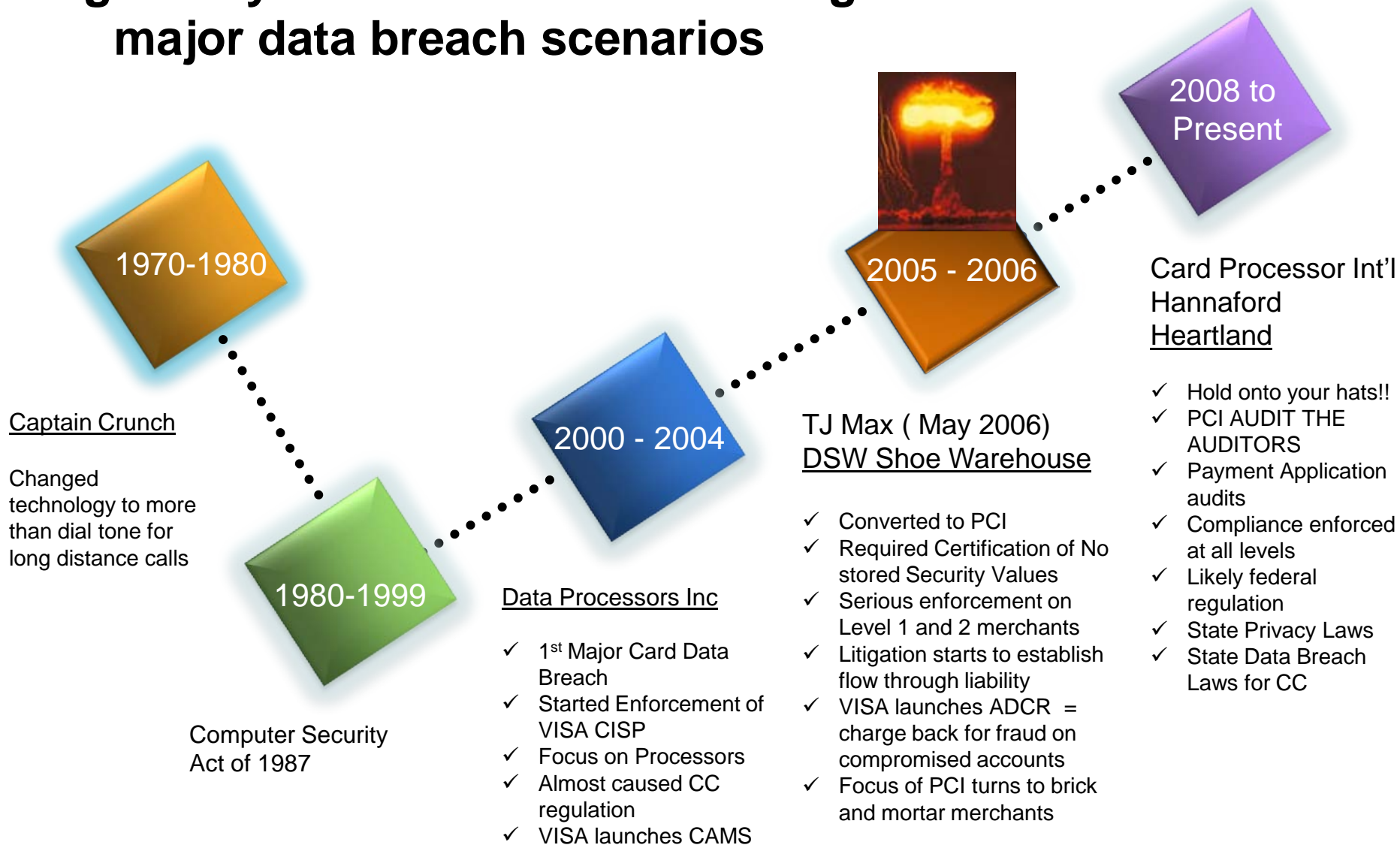
Agenda

- Regulatory Landscape
- Scary Bedtime Stories ... What went wrong?
- PCI Compliance Process
 - What are we protecting
 - PCI compliance requirements
 - Compliance strategies
 - Issues
- Questions

The Perfect Storm



Regulatory Environment is following major data breach scenarios



State Privacy Laws

In the event of an actual or suspected data privacy breach, organizations have a legal obligation to notify impacted consumers

Organizations must establish basic information security programs

Organizations must proactively manage their confidential consumer information

Organizations must take steps to know when their defenses have been breached

Compromise Statistics

- Over 80% of compromised systems were “card present” or in person transactions
- 90% of all compromised merchants are PCI level 4 merchants (less than 1 million transactions per year)
- No fully compliant merchant has ever been compromised
- 50% of the merchants do not survive the breach ...
or, operate with the same independence

Impact of Organized Crime



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

There is a multi-tiered market for stolen personal information.

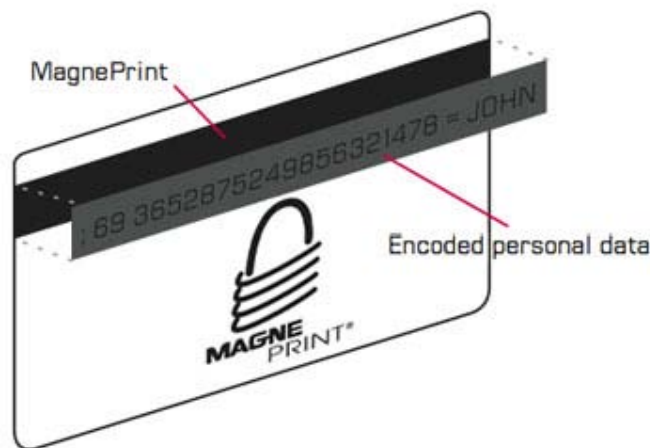
The thieves are generally not the ones who use it to commit fraud.

Economics of a Breach

A hypothetical merchant compromises 10,000 accounts

- Notify Clients $\$30 \times 10,000 = \$300,000$
- Fines and Penalties $\$50,000+$
- Increased audit needs $\$25,000 \times 3 \text{ years} = \$75,000$ (minimum)
- Fraud liability $1,000 \text{ accounts} \times \$500 = \$500,000$
- **Total Financial Impact** **Up to \$925,000**
- Reputation Loss **PRICELESS!**

What are We Protecting?

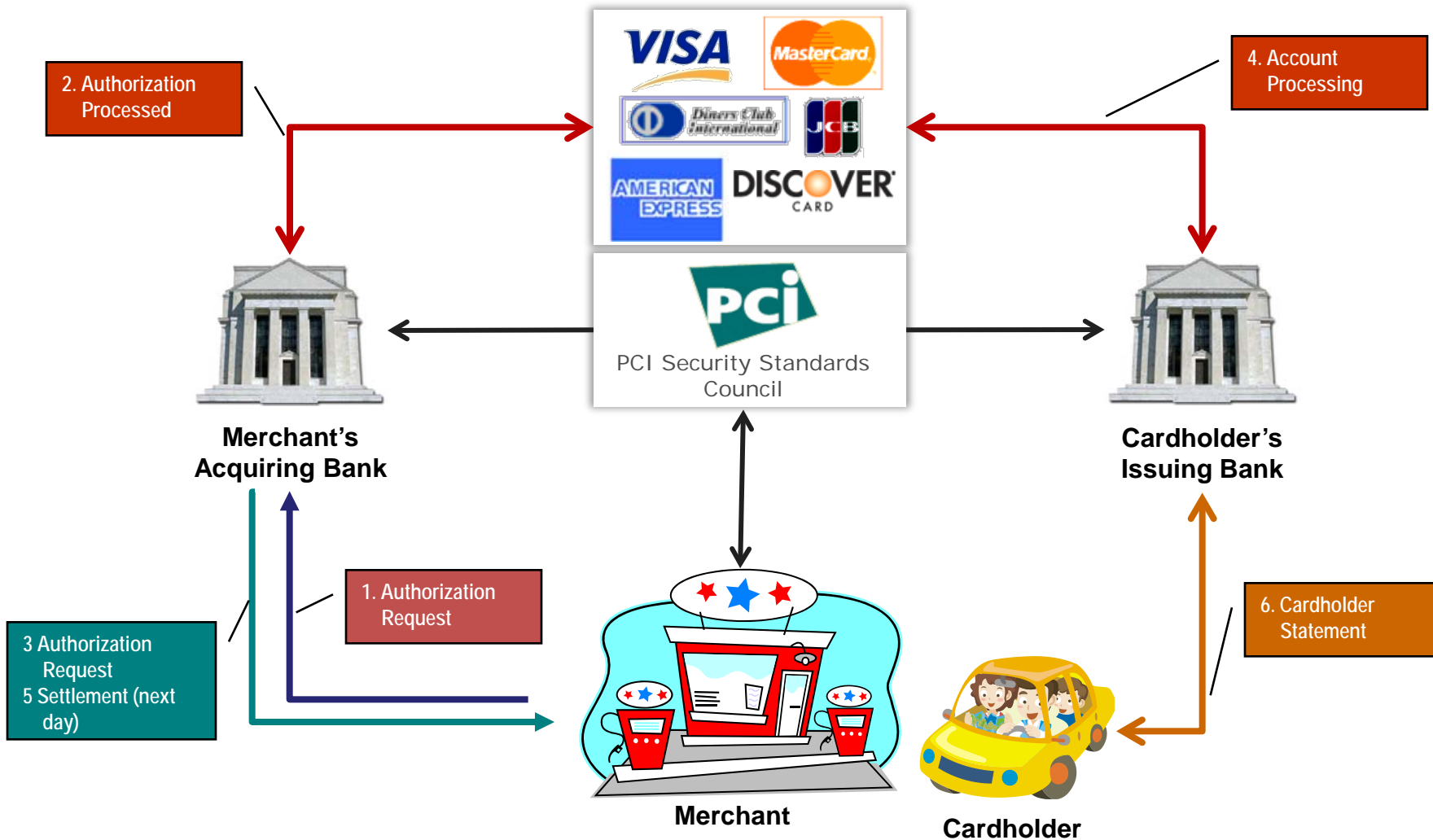


Visa, Mastercard, Discover
CID Location.



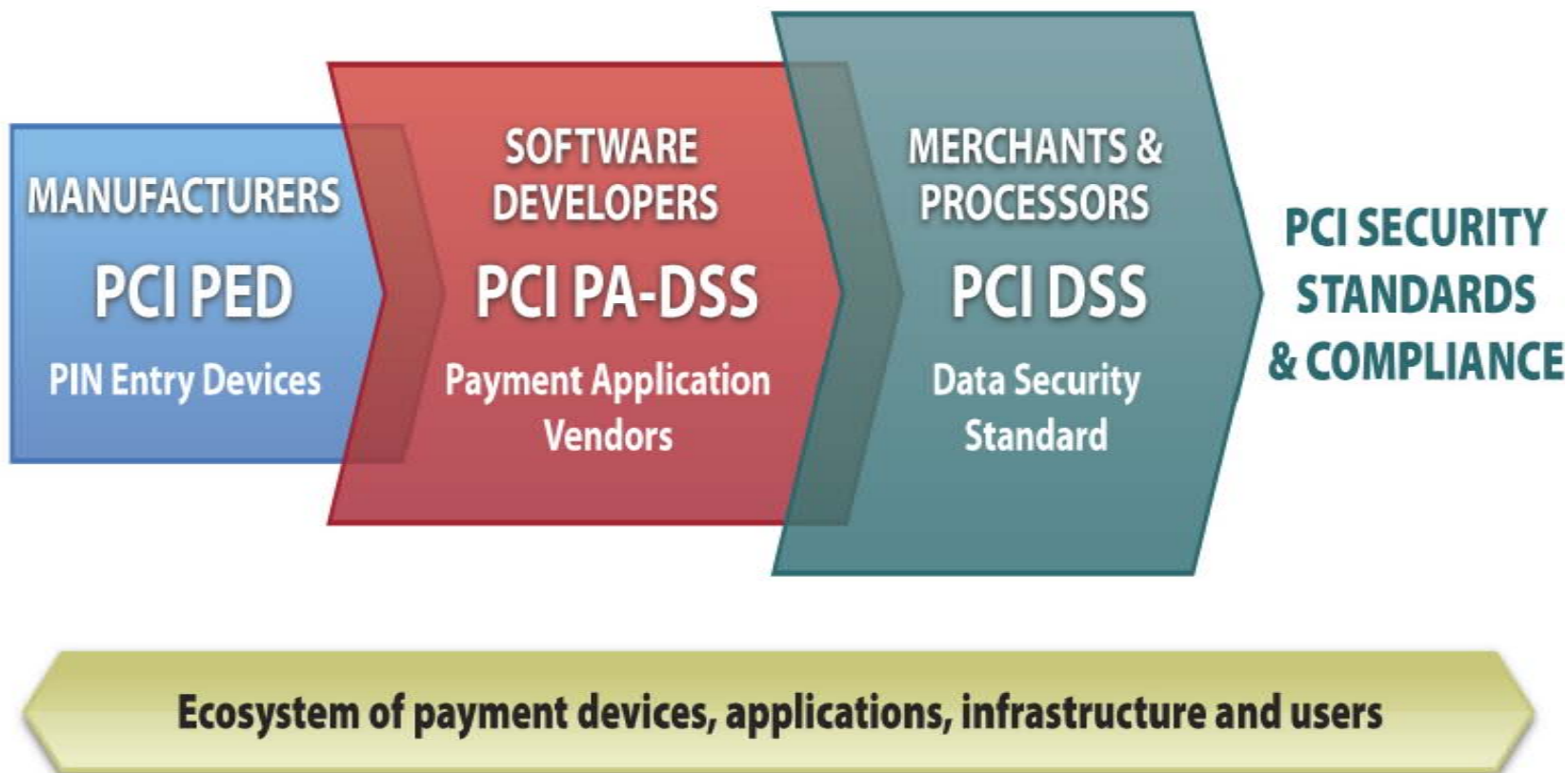
1. Cardholder Verification Number (CVN)
 - Visa/Discover's Card Verification Value (CVV)
 - Mastercard's Card Validation Code (CVC)
2. Primary Account Number (PAN)

Responding to a Breach



PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



PCI Standards Security Council

- PCI SSC Is...
 - An Independent Industry Standard
 - Manages the technical and business requirements for how payment data should be stored and protected
 - Maintains List of Qualified Assessors
 - QSAs, ASVs, PA-QSA and PED
 - Labs
- PCI SSC Does Not...
 - Manage or Drive Compliance
 - Each brand continues to maintain its own compliance programs
 - Identifies stakeholders that need to validate compliance
 - Definitions of Validation Levels
 - Fines and Fees

Binding Contract



CISP is based on the Payment Card Industry Data Security Standard, with which all members, merchants and service providers must comply according to contracts.



SECTION 4 Visa Cardholder Information Security Program

What's Covered

- CISP Requirements
- Steps and Requirements for Compromised Entities
- Additional Security Requirements

With recent media reports of hacker incidences, stolen credit card numbers, and identity theft, consumers are increasingly concerned about information security. Today, consumers want absolute assurance from the merchants with whom they do business that their bankcard account number and other personal information are safe.

To address these concerns, Visa has established the *Visa USA Cardholder Information Security Program (CISP)* in 2001 to define standards for protecting sensitive cardholder information.

CISP is based upon the Payment Card Industry (PCI) Data Security Standard, with which all members, merchants, and service providers must comply. In order to ensure compliance, Visa may require all merchants to validate their implementation of the CISP standards. Validation requirements are based on Visa transaction volume and the risk factors associated with a merchant's business.

More information about CISP, including the detailed PCI Data Security Standard and CISP compliance validation requirements are available at www.visa.com/cisp.

Top System Risks to Watch

Vulnerability	Remediation Efforts
<i>Vulnerable payment applications (e.g., Storing prohibited track, CVV2 or PIN data, insecure remote access)</i>	<i>PCI DSS; PCI PA-DSS, PIN Security Requirements</i> Replace vulnerable software; delete all stored data; ensure software vendor uses secure remote access
<i>Packet sniffers and key loggers targeting payment data</i>	<i>PCI DSS</i> Establish policies, procedures and processes for updating and maintaining system security patches and anti-virus software
<i>Inadequate perimeter security</i>	<i>PCI DSS</i> Execute disciplined firewall policy management and network security; conduct routine testing of all systems
<i>Vendor default settings and passwords</i>	<i>PCI DSS</i> Enable security settings and ensure default passwords provided by the vendor are changed; utilize strong encryption and security features to protect wireless environments
<i>SQL injection attacks</i>	<i>PCI DSS</i> Conduct regular testing for susceptibility to SQL injection utilizing automated tools or manual techniques

PCI Standards

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor defaults for system passwords & other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, 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 cardholder 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

- Compliance
 - All merchants must adhere to the PCI standard, regardless of size or number of transactions processed
 - Cyber security program
- Validation
 - Compliance must be tested and reported to Acquiring Banks based upon transactions volumes or risk levels
 - Audit of the cyber security program



Merchant 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

Merchant Validation Requirements

Merchant Level	Description	Validation Action	Validated By
1	<p>Merchants processing over 6 million Visa transactions annually (all channels) or global merchants identified as Level 1 by any Visa region</p> <p>Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.</p>	<ul style="list-style-type: none"> • Annual On-site PCI Data Security Assessment • Quarterly Network Scan 	<ul style="list-style-type: none"> • Qualified Security Assessor or Internal Audit if signed by Officer of the company • Approved Scanning Vendor
2	Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.	<ul style="list-style-type: none"> • Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan 	<ul style="list-style-type: none"> • Merchant • Approved Scanning Vendor
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.	<ul style="list-style-type: none"> • Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan 	<ul style="list-style-type: none"> • Merchant • Approved Scanning Vendor
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.	<ul style="list-style-type: none"> • Annual PCI Self-Assessment Questionnaire • Quarterly Network Scan (if applicable) 	<ul style="list-style-type: none"> • Merchant • Approved Scanning Vendor

Service Provider Validation Requirements

Service Provider Level	Description	Validation Requirements	Validated by
1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year	<ul style="list-style-type: none"> • Annual On-Site PCI Data Security Assessment • Quarterly Network Scan 	<ul style="list-style-type: none"> • Qualified Security Assessor • Approved Scanning Vendor
2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year	<ul style="list-style-type: none"> • Annual Self Assessment (SAQ) • Quarterly Network Scan 	<ul style="list-style-type: none"> • Service Provider • Approved Scanning Vendor



PCI's 5 Stage to Acceptance

1. Denial
 - It doesn't apply to me
 - *PCI compliance is mandatory*
2. Anger
 - It isn't fair
 - *PCI applies to all parties*
3. Bargaining
 - I'll do some of it
 - *Compliance is "pass / fail"*
4. Depression
 - I'll never get there
 - *Many merchants already have*
5. Acceptance
 - It'll be OK
 - *PCI doesn't introduce any new, alien concepts*

Compliance Program

Charter

- Align team
- Scope Environment

Assess

- Conduct Testing to PCI DSS
- Identify Gaps
- Establish a Remediation Roadmap

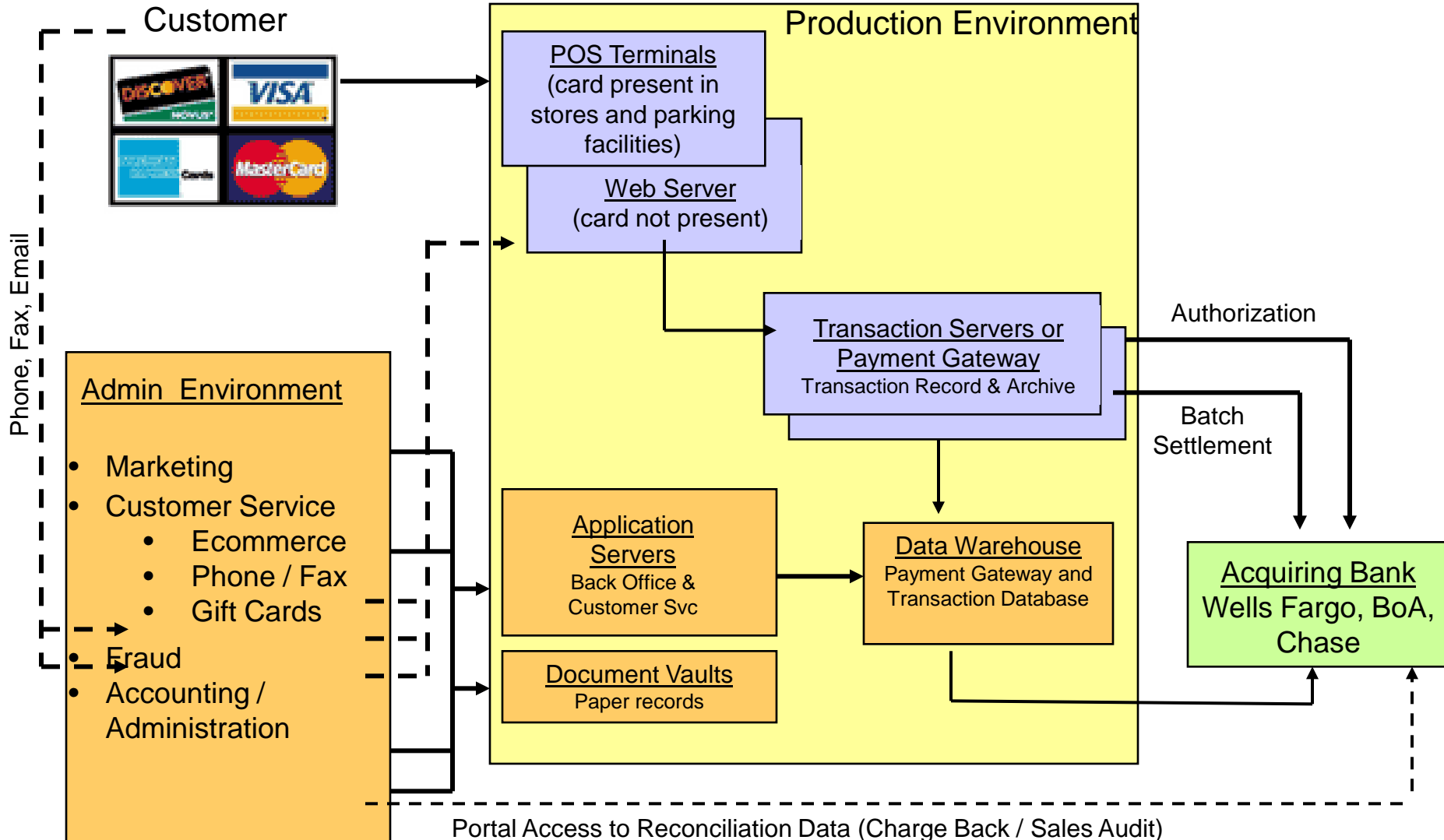
Remediate

- Align to a Project Plan (Time, \$)
- Policies, Plans and Procedure Documentation
- Infrastructure changes
- Training

Validate Compliance

- Final Testing (independent?)
- Report to Acquiring Banks
- Report to other airport merchants?

Where is the Cardholder data?



Sample Scanning Report

Overall Compliance Status		FAIL
Live IP Address Scanned	Security Risk Rating	Compliance Status
11.22.33.44	1.0	Pass
11.22.33.45	1.0	Pass
11.22.33.46	2.0	Pass
11.22.33.47	1.0	Pass
11.22.33.48	1.0	Pass
11.22.33.49	1.0	Pass
11.22.33.50	1.0	Pass
11.22.33.51	4.0	FAIL
11.22.33.52	1.0	Pass

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 all service providers defined by a payment brand as eligible to complete an SAQ.	D



Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire D
and Attestation of Compliance

**All other Merchants and all SAQ-Eligible
Service Providers**

Version 1.2
October 2008

PCI Compliance Strategies

- Confirm you are running a Validated Payment Application
- Read and Follow Your POS Implementation Guide
- If You Don't Need it, Don't Store It
- Segment your Network
- Implement Quarterly Scanning
- Complete a PCI SAQ
- Update Your Policies and Procedures
- Implement Logging and Monitoring
- Manage Security like your business depends on it

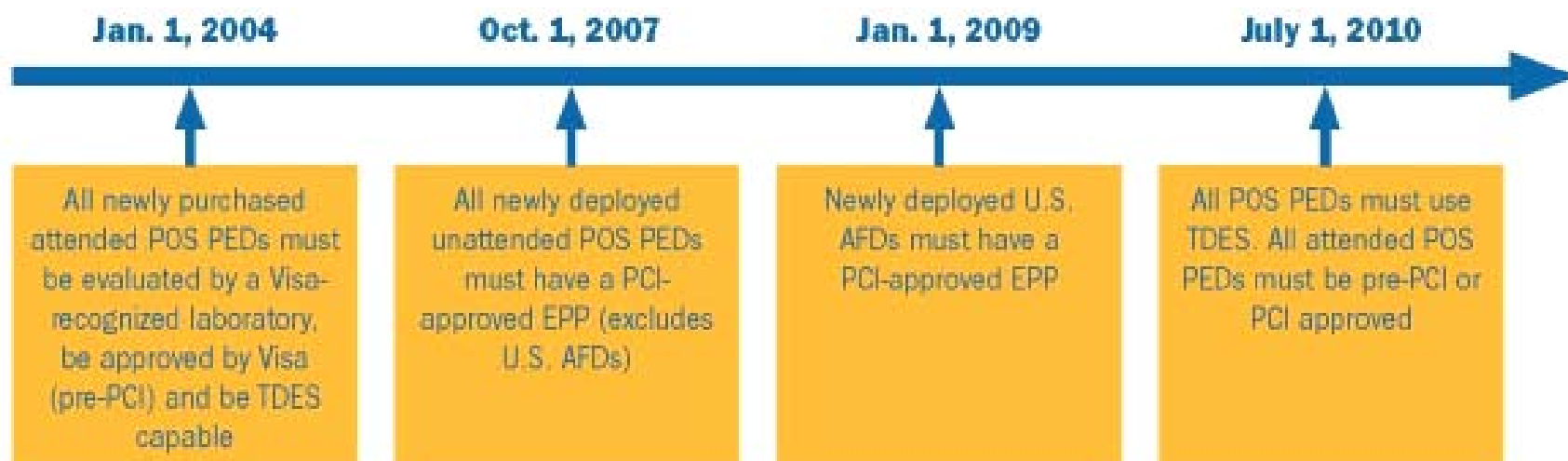
Summary

- PCI Compliance is an Ongoing PROCESS and NOT A PROJECT
 - This means an new ongoing operating expense
- Roles – everyone has a stake in the program success
- Key Activities
 - Map all cardholder processes
 - Validate with vendors that no unencrypted cardholder data or security values are stored
 - Identify all critical locations where cardholder data is processed, stored or transmitted
 - Remediate compliance gaps and train all key stakeholders
 - Provide well documented (i.e. justified with evidence) reports to senior management and Acquiring Banks
 - Schedule vulnerability scans
- Manage Risk and not just a in the box

References

- PCI Security Standards Council
 - <https://www.pcisecuritystandards.org/>
- PCI Blog – PCI Answers
 - <http://pcianswers.com/GAO Report on Continuing Security Weakness>
- State Notice of Data Breach Laws
 - <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>
- Rapid SAQ Resources
 - <https://navis.coalfiresystems.com>

PIN Entry Device Timeline



U.S. Petroleum Merchants — TDES Usage

- October 1, 2009:
 - Acquirers must submit to Visa a summary TDES compliance status report and plan to achieve full compliance for sponsored AFD activity.
- July 1, 2010:
 - Acquirers may be assessed fines for merchants that are not using at least SDES Derived Unique Key per Transaction (DUKPT) or TDES.
- Inside petroleum sales (non-AFD) will be managed under the POS category policy.

U.S. Petroleum Merchants—EPP Usage

- January 1, 2009:
 - Acquirers may be assessed fines for newly deployed AFDs without TDES-capable Payment Card Industry (PCI)-approved EPPs.
- October 1, 2009:
 - Acquirers must submit a summary AFD EPP attestation for newly deployed AFDs at sponsored merchants.

Impact

- The key change for petroleum retailers is that fines will not automatically be assessed to their acquirer for retailers using single DES DUKPT (Derived Unique Key Per Transaction) on their dispensers. The standard still calls for conversion to triple DES by July 1, 2010 as before. Fines, however, may not be automatically assessed to the acquirer now per the new statement.

Thank You



Questions?

Knowledge – Action = Negligence



Rick Dakin
President
Rick.Dakin@coalfiresystems.com
303.554.6333 ext. 7001