



**Smart Card
Alliance**



Technology: Smart Cards and Payments Security

Welcome – Rori Ferensic

Director of Education and Professional Development, ETA

The Smart Card Payments Application Series

February 17, 2009





Smart Card
Alliance



Introductions

Randy Vanderhoof, Executive Director
Smart Card Alliance



Webinar Topics

Smart Cards and PKI in the Payments Landscape

- Jose Diaz, Director, Technical and Strategic Business Development, Thales Information Systems Security

Securing the Payment Environment

- Sally Ramadan, Director, Payment Card Compliance, First Data Corporation

Conclusions and Q&A

- Randy Vanderhoof, Executive Director, Smart Card Alliance

Smart Card Alliance

Smart Card Alliance mission

To stimulate the understanding, adoption, use and widespread application of smart card technology through educational programs, market analysis, advocacy, and industry relations

Over 170 members, including participants from financial, retail, government, corporate, and transit industries and technology providers to those users

Major activities

- **Industry and Technology Councils**
 - **Contactless and Mobile Payments Council**
 - **Healthcare Council**
 - **Identity Council**
 - **Physical Access Council**
 - **Transportation Council**
- **Conferences, symposia, web seminars and educational workshops**
- **Web-based resources and email newsletters**



Contactless and Mobile Payments Council

Mission: *Facilitate the adoption of contactless and mobile payments in the U.S. through education programs for consumers, merchants and issuers*

Over 48 active member organizations, including financial industry representatives and technology suppliers

Resources

- **Merchant and Issuer Advisory Groups**
- **Merchant Discussion Forum**
- **Educational publications on contactless and mobile payments**
 - *Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives*
 - *Merchant ROI Model & Implementation Guide*
 - *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*
 - *Contactless Payments: Frequently Asked Questions*
 - *The What, Who and Why of Contactless Payments*
- **Contactless and mobile payments resources and news**
- **Payments industry web seminars**





Smart Card
Alliance



Smart Cards and PKI in the Payments Landscape

Jose Diaz

Director, Technical and Strategic Business Development

Thales Information Systems Security

THALES



Payment System Security



Heartland Data Breach

- Total number of compromised card numbers yet to be determined but expected to be in the millions
- Sniffer malware was installed to obtain credit card numbers
- Similar incident occurred at Okemo Ski Resort in Vermont



Hannaford Data Breach

- 4.2 million customer card transactions were compromised
- Sensitive data was exposed when shoppers swiped their cards at checkouts and the information transmitted to banks for approval
- Not an attack on databases but an attack on data in transit



Lost/Misplaced Backup Data Tapes or Hard Drives

- Bank of New York Mellon, GE Money, Compass Bank



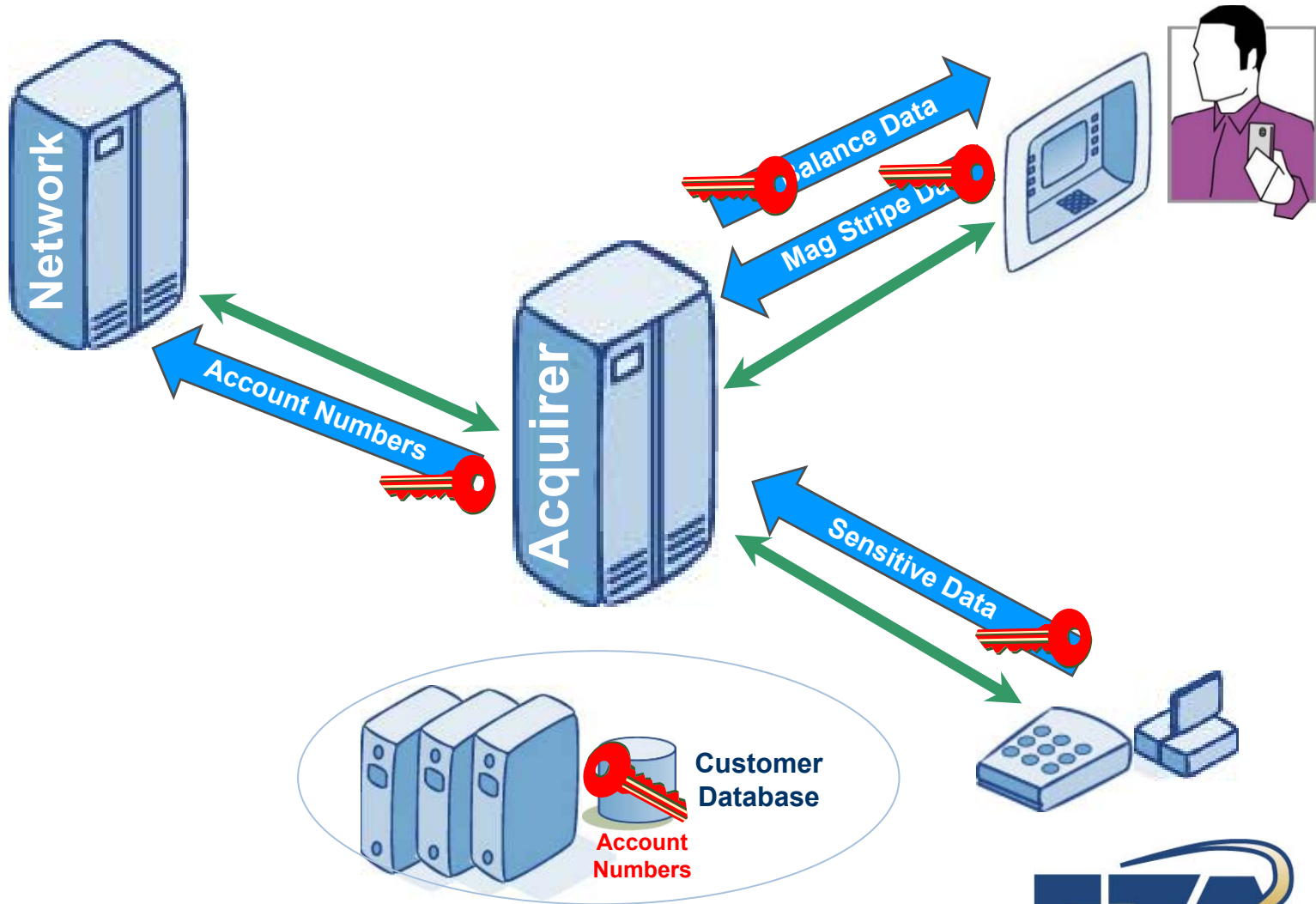
Other reported breaches

- TJX, Countrywide Financial, Montgomery Ward

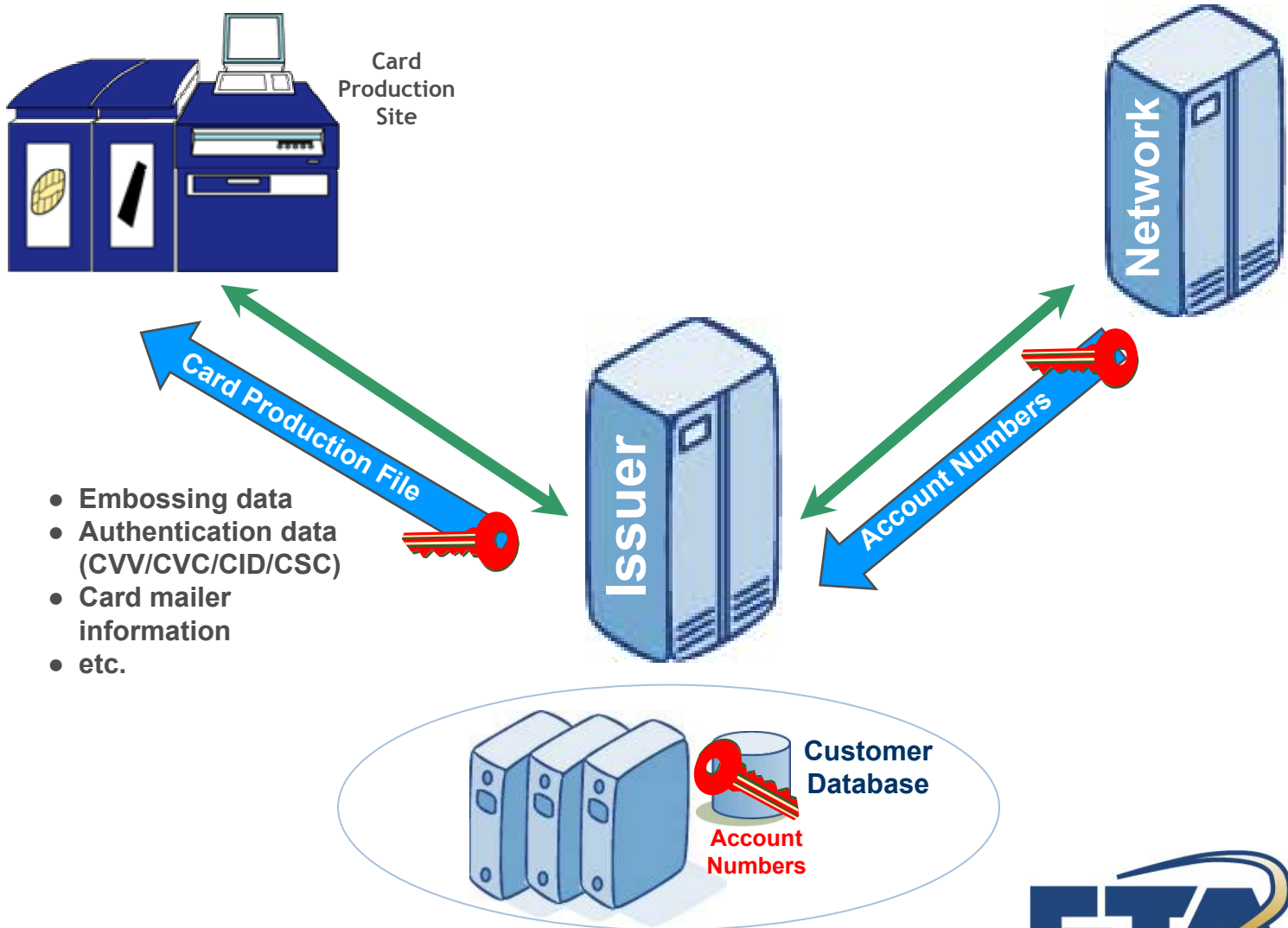
From a reputation perspective, the damage is immeasurable



“Total” Data Protection from Acquirer’s Viewpoint



“Total” Data Protection from Issuer’s Viewpoint





FFIEC Guidance On Multifactor Authentication

- Financial institutions are being required to establish and execute a risk-based assessment of their respective online banking delivery channel
- Financial institutions are being required to implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks
- Agencies consider single-factor (e.g., ID/password) authentication to be insufficient as the only means of control for high risk transactions
- High risk transactions involve the movement of funds to other parties (even within the FI) or access to customer information



www.ffiec.gov/pdf/authentication_guidance.pdf
www.ffiec.gov/pdf/authentication_faq.pdf
www.nacha.org



Authentication Functions

- What is a PIN verification?
 - A method to authenticate a customer
 - Used for ATM and POS transactions



- How do we address authentication of customers on virtual storefronts or when the customer is not physically present?

- Web-based services?
- Phone-based services?
- Other customer services?

User ID	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Log On"/>	



Smart Card Alliance

User Authentication Options



*Mother's Maiden Name?
What city were you born?*

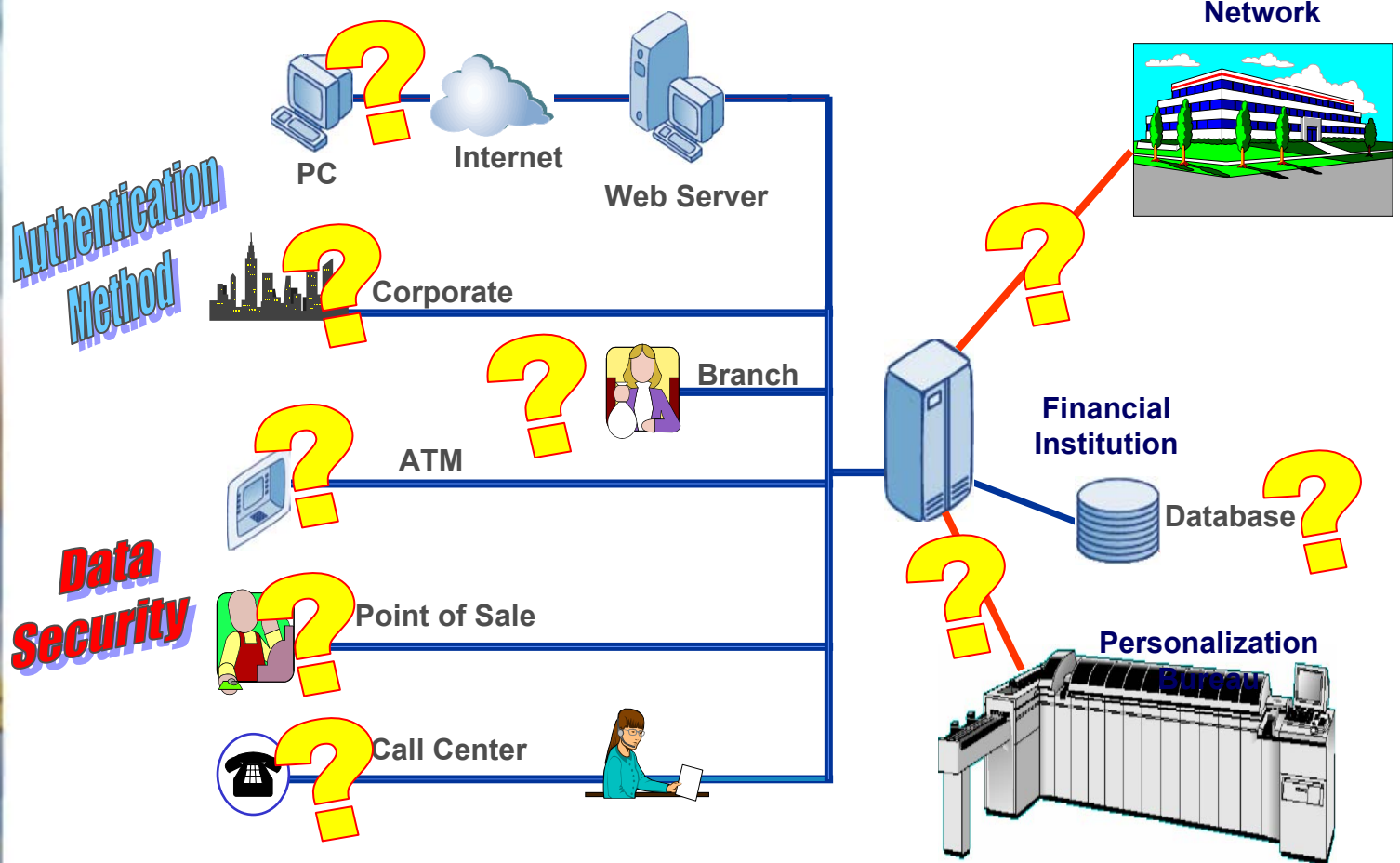
User ID	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Log On"/>	



IP = 192.130.40.54

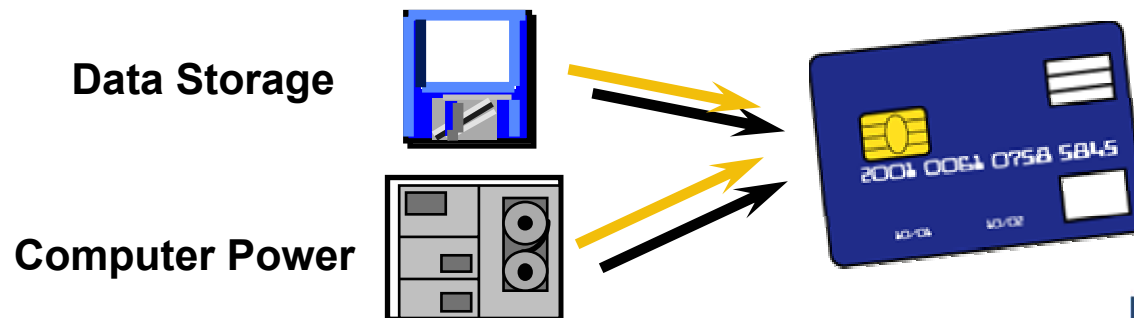


Payment System Infrastructure



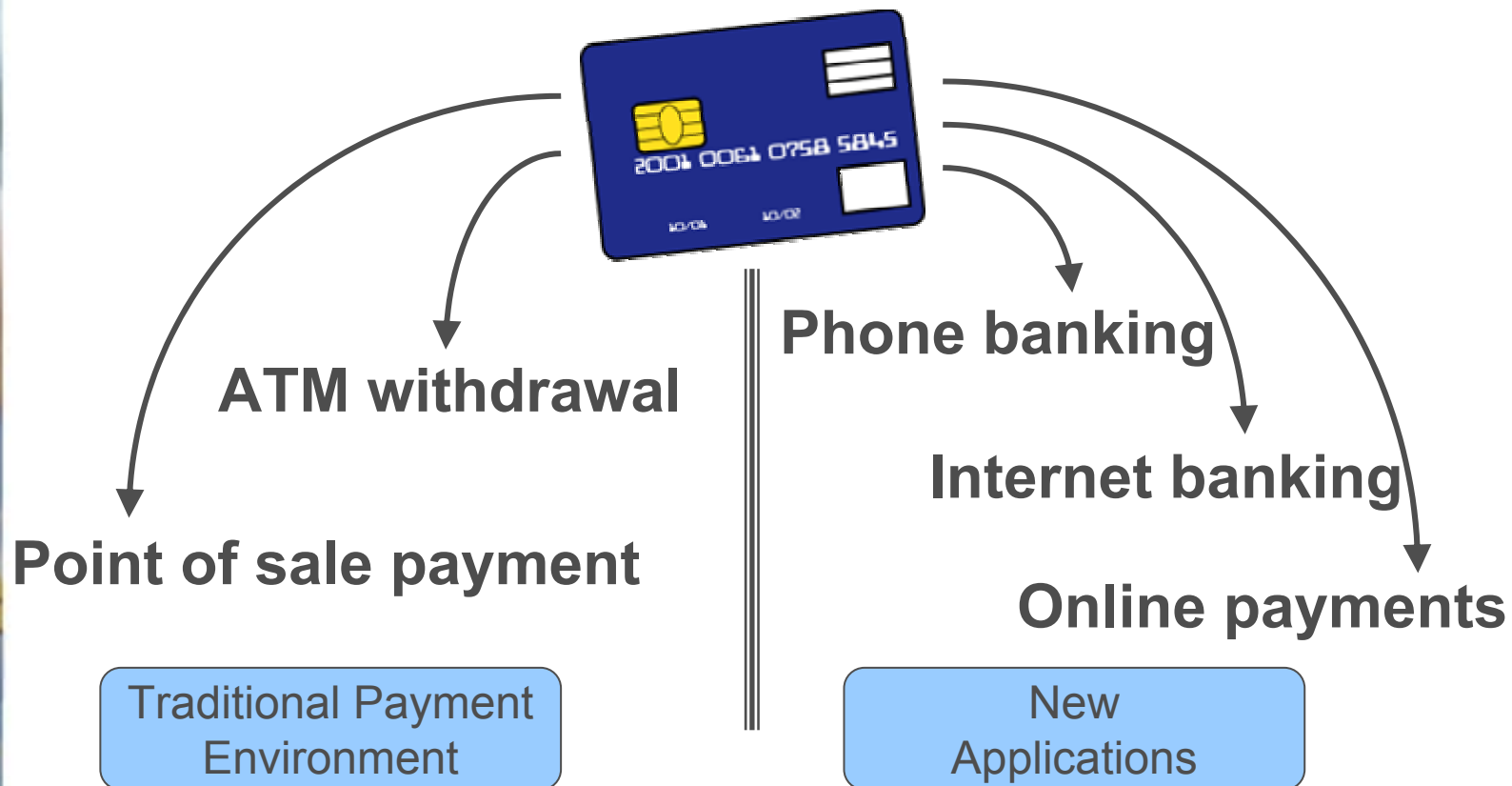
Smart Cards – What Are the Benefits?

- Secure and flexible technology for information and data storage
 - PIN can be used to control access to the card
 - Offers advanced fraud and risk management
 - Card can be “updated” at the service point
- Can also provide cryptographic services such as key generation and encryption
- Foundation for EMV-based payment cards
- Excellent solution for secure storage of user credential information (e.g. certificate)



EMV-based Authentication

Maximizing the use of EMV smart cards
as a secure authentication token



Programs for EMV-based Authentication

MasterCard

- Chip Authentication Program (CAP)



MasterCard.
SecureCode.

Visa

- Dynamic Passcode Authentication (DPA)



VERIFIED
by **VISA**



Smart Cards in Other Authentication Applications

- Becoming more common in Enterprise employee identification schemes
 - Crossing over into authenticating users to network
- Cards contain certificate with user information
 - Certificate signed by “Issuing authority” and verified during authentication process
 - Securely stored on card, protected by PIN
- Dual interface cards (contact and contactless) facilitate use of smart cards for physical and logical access
- “Federation” of credential would allow extending use of certificate outside the Issuing Enterprise

In Summary

- Security for payment systems needs to be approached from a holistic point of view
- User authentication is a critical requirement
 - No prevalent methodology has been adopted
 - New standards may simplify interoperability
- Smart cards offer many benefits for security, flexibility and ubiquity
 - New form factors facilitate their use and interface with a growing range of applications



Smart Card
Alliance



Securing the Payment Environment

Sally Ramadan
Director, Payment Card
First Data Corporation





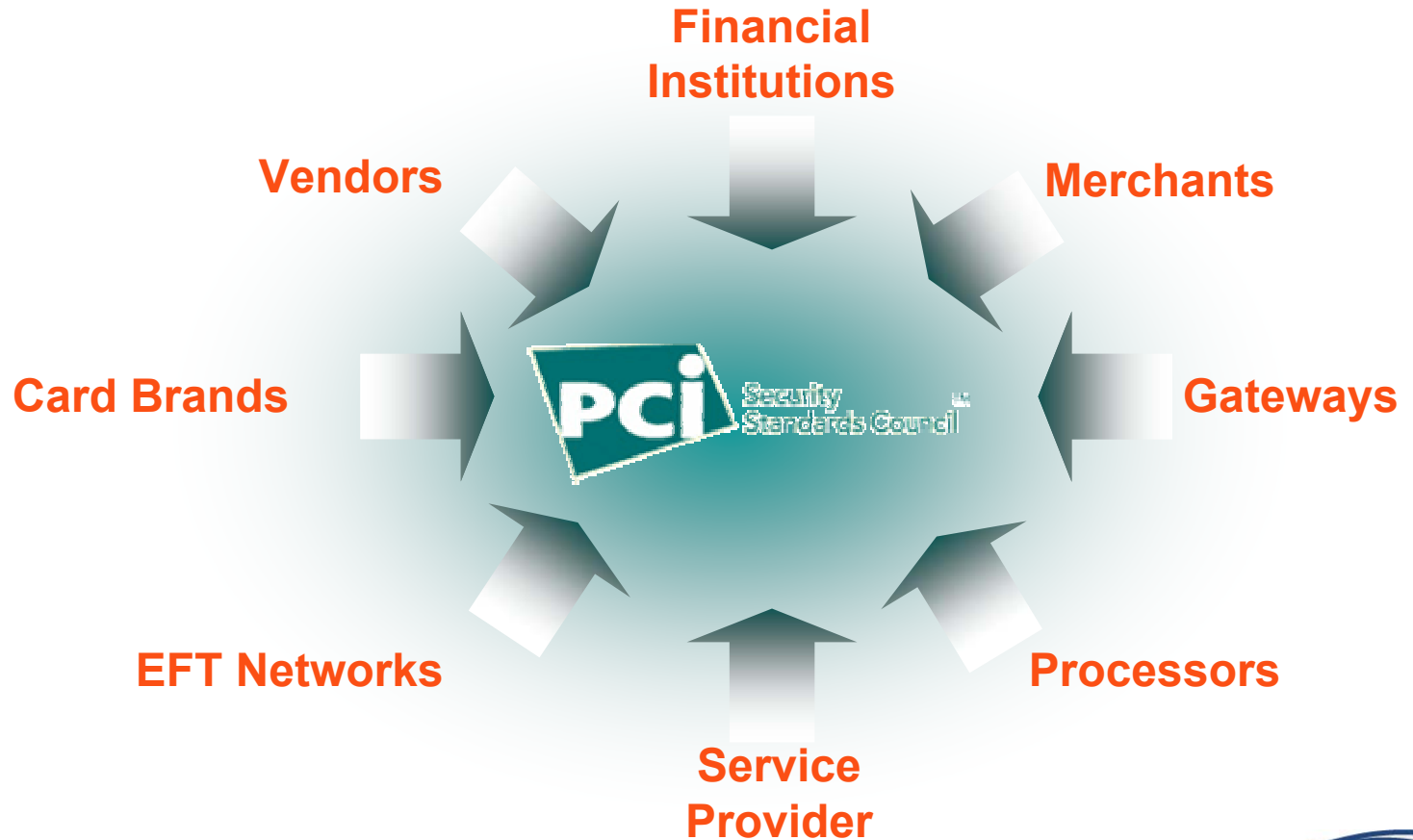
Smart Card
Alliance

The information contained herein and stated by the speaker is provided as a courtesy and is for general informational purposes only. This presentation is not intended to be a complete description of all applicable policies and procedures. The matters referenced are subject to change. Individual circumstances may vary. The information contained herein includes, among other things, a compilation of documents received from third parties. First Data shall not be responsible for any inaccurate or incomplete information. Nothing contained in this presentation is intended to supplement, amend or modify any applicable contract, rule or regulation.



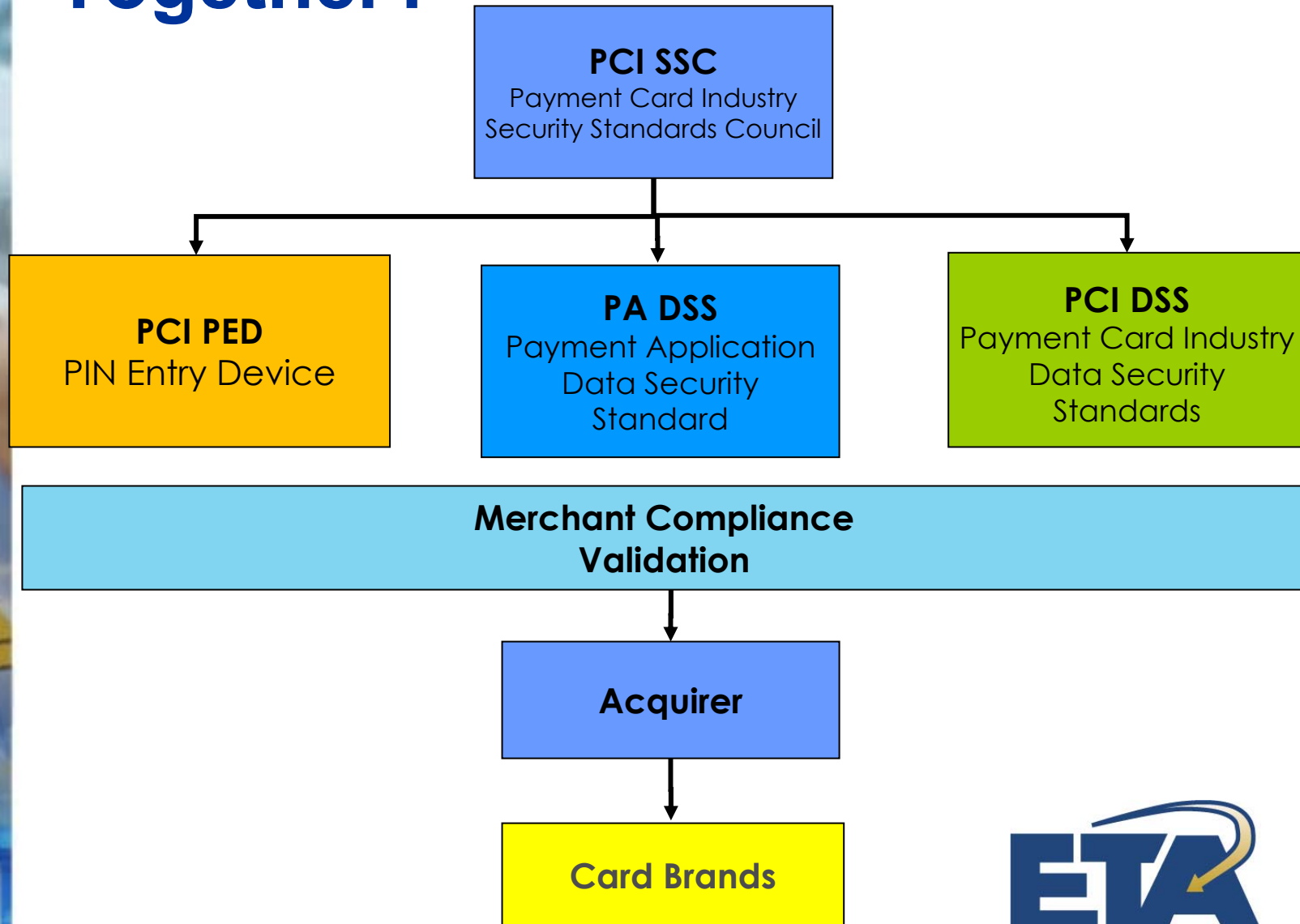


Payment Card Industry Security Standards Council





How Do All the Standards Fit Together?





PIN Entry Devices

- Applies to manufacturers of Pin Entry Devices
- Objective is to standardize device security requirements, testing methodologies, and approval processes
- Security requirements pertain to physical and logical security characteristics
- Merchants must use PEDs from the certified list
- As of January 2008, there are 276 compliant devices provided by 88 vendors





PA-Data Security Standard

- Applies to software vendors who develop payment applications that process, store, or transmit cardholder data as part of authorization or settlement process
- Focus is to prevent the storage of sensitive cardholder data (i.e. full magnetic stripe data, CVV, CVV2 or PIN data)
- Merchants must use PA-DSS compliant applications
- If not compliant, merchants must upgrade to new PA-DSS compliant version and/or obtain patch to ensure sensitive cardholder data is not stored subsequent to an authorization





PCI Data Security Standard

Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored data4. 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 software6. 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-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. 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



Acquirer Responsibilities

- Acquirers are responsible for determining the compliance validation levels of their merchants and notifying merchants of their compliance validation requirements
- Acquirers must report the compliance status of each merchant to MasterCard and Visa on a continuous basis
- Acquirers are responsible for on-going communication to merchants on rules changes, fine notices, validation deadlines, etc.
- Acquirers must ensure that merchant validation documentation demonstrates that the merchant has achieved full compliance and maintains their compliance each year



Merchant Responsibilities

- A merchant is responsible for engaging a certified vendor to perform assessment
- A merchant is responsible for remediating all non-compliant findings and vulnerabilities identified based on results of Network Scan, Audit or Self-Assessment Questionnaire
- A merchant must submit supporting validation documentation to their acquirer demonstrating full compliance. If not fully compliant, merchant must provide a detailed remediation plan with timelines for compliance. Acquirer may submit to Visa request for extension on behalf of merchant



Why Comply with the PCI DSS?

- The payment brands continually monitor cases of account data compromise. These compromises cover the full spectrum of organizations, from the very small to very large merchants and service providers
- A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations, including:
 - Regulatory notification requirements
 - Loss or reputation
 - Loss of customers
 - Potential financial liabilities (e.g., regulatory & other fees/fines)
 - Litigation

Common PCI DSS Violations

Investigations after compromises consistently show common PCI DSS violations, including but not limited to:

- Storage of magnetic stripe data (Req 3.2)
- Inadequate access controls due to improperly installed merchant POS systems, allowing hackers in via paths intended for POS vendors
- Default system settings & passwords not changed when system was set up (Req 2.1)
- Unnecessary and vulnerable services not removed or fixed when system was set up (Req 2.2.2)
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Req 6.5)
- Missing and outdated security patches (Req 6.1)
- Lack of logging (Req 10)
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems)
- Lack of segmentation in a network, making cardholder data easily accessible through weaknesses in other parts of the network

Recommended Reading

PCI Security Standards Council Website contains all published documents www.pcisecuritystandards.org

- PCI Data Security Standard v1.2 (released October 2008)
- PCI Security Audit Procedures
- PCI Security Scanning Procedures
- PCI Self-Assessment Questionnaire
- Qualified Security Assessor (QSA) Validation Requirements
- Approved Scanning Vendor (ASV) Technical and Operational Requirements
- ASV Validation Requirements
- Feedback Forms

MasterCard Website: www.mastercard.com/sdp

Visa Website: www.visa.com/cisp





**Smart Card
Alliance**



Conclusions

Randy Vanderhoof

Executive Director, Smart Card Alliance



Wrap Up and Conclusions

- **Security touches every part of the payments ecosystem**
 - Issuers and acquirers have different needs
 - Regulator role protects consumers
- **Smart cards add security by ..**
 - Ensuring one cardholder identity exists
 - Binding authentication rules defined by the issuer and accepted by the merchant for that identity
 - Adapting to different payment transaction environments
- **PCI rules define best practices in the absence of card-centric POS to acquirer security**
 - Bridges gap for what is needed today
 - Adds foundation for more security in the future



**Smart Card
Alliance**



Q&A

**Randy Vanderhoof (moderating)
Executive Director, Smart Card Alliance**





Smart Card
Alliance



Electronic Transactions Association

<http://www.electran.org>

Rori Ferensic, Electronic Transactions Association

rferensic@electran.org

Smart Card Alliance

<http://www.smartcardalliance.org>

Randy Vanderhoof, Smart Card Alliance

rvanderhoof@smartcardalliance.org

THALES

Jose Diaz, Thales Information Systems Security

jose.diaz@thalessec.com

 **First Data™**

Sally Ramadan, First Data Corporation

sally.ramadan@firstdata.com

