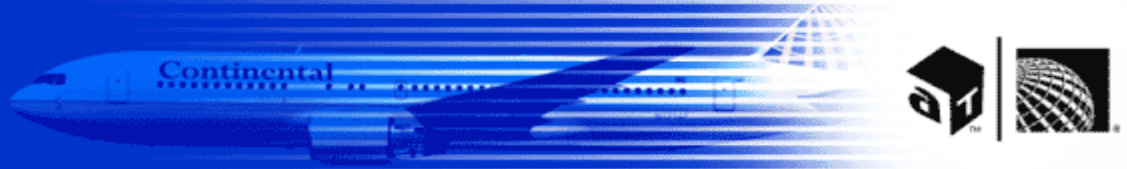




# Payment Card Industry (PCI)

## **Interop Las Vegas 2006**

André Gold  
Director – Information Security  
Continental Airlines, Inc.



## All About Me....

- Current Role and Responsibilities
- IT experience
- Industry Memberships
- Emerging Technologies Participation



# Credit Card Landscape



SDP



CISP

PCI



Data Security  
Guidelines



DSS  
(Data Security)



# Payment Card Industry

**Purpose** – To protect your business, your customers, and the integrity of the payment system

**Scope** – any system(s) or system components(s) where cardholder data is processed, stored, or transmitted, as well as a company's e-commerce and wireless LAN environments





# 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



# Build and Maintain a Secure Network

1. Install & Maintain a firewall configuration to protect data
  - 1.1.2 A **current** network **diagram** with **all** connections to cardholder data, including any wireless networks
  - 1.1.7 Justification and documentation for any **risky** protocols allowed
- 1.3 Build a firewall configuration that restricts connections **between** systems storing cardholder **data** and **wireless** networks



# Build and Maintain a Secure Network

## 1.3 Build a firewall configuration

- 1.3.9 Installation of perimeter **firewalls** between any **wireless** networks and the payment card environment
- 1.3.10 Installation of **personal** firewall software on any mobile and/or employee-owned **computers**



# Build and Maintain a Secure Network

2. Do not use **vendor-supplied** defaults for system **passwords** and other security **parameters**
  - 2.2.2 Disable all **unnecessary** and insecure services & protocols
  - 2.3 **Encrypt** all non-console administrative **access**



# Protect Cardholder Data

## 3. Protect stored data

3.2.2 Do not **store** the care-validation code

3.2.3 Do not store the **PIN** Verification Value

3.4 **Render** sensitive cardholder data unreadable in storage

3.6.6 **Split** knowledge and dual control of keys



## Protect Cardholder Data

4. Encrypt transmission of cardholder data and sensitive information across public networks



## Protect Cardholder Data

4. Encrypt transmission of cardholder data and sensitive information across public networks
- 

## Maintain a Vulnerability Management Program

5. Use and regularly update **anti-virus** software



# Maintain a Vulnerability Management Program

- 6. Develop and maintain secure systems and applications
  - 6.1.1 Install **relevant** security patches within one month
  - 6.2 **Update** your standards
  - 6.3.4 Production data **are not** used for testing or development
  - 6.3.7 Review custom code **prior** to production release
  - 6.5 **Develop** software and applications **based** on secure coding guidelines.



## Implement Strong Access Control Measures

7. Restrict access to data by business **need-to** know
8. Assign a unique ID to each person with computer access
  - 8.3 Implement **2-factor** auth for **remote** access to the network by employees, administrators, and 3<sup>rd</sup> parties
  - 8.4 Encrypt **all** passwords during **transmission** and **storage**, on all system components.



## Implement Strong Access Control Measures

9. Restrict physical access to cardholder data
  - 9.1.1 Use **cameras** to monitor sensitive areas
  - 9.1.2 Restrict physical access to **publicly** accessible network jacks
  - 9.1.10 **Destroy** media containing cardholder information when it is no longer needed for business or legal reasons



# Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

10.5.4 Copy logs for **wireless** networks on to a log server

10.6 Review logs for all system components at least **daily**

10.7 **Retain** your audit trail history – *“an audit history usually covers a period of at least one year”*



# Regularly Monitor and Test Networks

## 11. Regularly test security systems and process

11.2 Run internal and external network vulnerability scans **quarterly**

11.3 Perform penetration testing at least **once** a year

11.5 Deploy file **integrity** monitoring to alert personnel to unauthorized modification of **critical** system or content files, and perform critical file comparisons at least **daily**



## Maintain an Information Security Policy

### 12. Maintain a policy that address information security

12.6.2 Require **employees** to **acknowledge** in writing that they have **read** and **understood** the company's security policy and procedures

12.8 **Contractually** require all third parties with access to cardholder data to adhere to PCI requirements

12.8.5 Include **termination** provision that ensures 3<sup>rd</sup> parties will treat cardholder data as confidential



<b>Benefits of compliance</b>	
Everyone	<ul style="list-style-type: none"><li>• Limited risk</li><li>• More confidence in the payment industry</li></ul>
Member	<ul style="list-style-type: none"><li>• Protected reputation</li></ul>
Merchant & Service Provider	<ul style="list-style-type: none"><li>• Competitive edge gained</li><li>• Increased revenue and improved bottom line</li><li>• Positive image maintained</li><li>• Customers are protected</li></ul>
Industry	<ul style="list-style-type: none"><li>• "Good security neighbors"</li></ul>
Consumer	<ul style="list-style-type: none"><li>• Information is safeguarded</li><li>• Identity theft prevention</li></ul>



Merchant Level	Description
1	<ul style="list-style-type: none"><li>•Over 6,000,000 transactions per year.</li><li>•Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</li><li>•Any merchant identified by any other payment card brand as Level 1.</li><li>•Any merchant Visa states so.</li></ul>
2	<ul style="list-style-type: none"><li>•processing 150,000 to 6,000,000 e-commerce transactions per year</li></ul>
3	<ul style="list-style-type: none"><li>•processing 20,000 to 150,000 e-commerce transactions per year.</li></ul>
4	<ul style="list-style-type: none"><li>•Everyone else</li></ul>



## Compliance Basics

Level	Validation Action	Validated By
1	<ul style="list-style-type: none"><li>•Annual On-site Data Assessment</li></ul> <b>AND</b> <ul style="list-style-type: none"><li>•Quarterly Network Scan</li></ul>	<ul style="list-style-type: none"><li>•Data Security Company</li><li>•Internal Audit</li><li>•3rd Party Scan Vendor</li></ul>
2 and 3	<ul style="list-style-type: none"><li>•Annual Questionnaire</li></ul> <b>AND</b> <ul style="list-style-type: none"><li>•Quarterly Network Scan</li></ul>	<ul style="list-style-type: none"><li>•Merchant</li><li>•3rd Party Scan Vendor</li></ul>
4	<ul style="list-style-type: none"><li>•Annual Questionnaire</li></ul> <b>AND</b> <ul style="list-style-type: none"><li>•Quarterly Network Scan</li></ul>	<ul style="list-style-type: none"><li>•Merchant</li><li>•3rd Party Scan Vendor</li></ul>



Service Provider Level	Description
1	All processors (member and Nonmember) and all payment gateways
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually
3	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/transactions annually

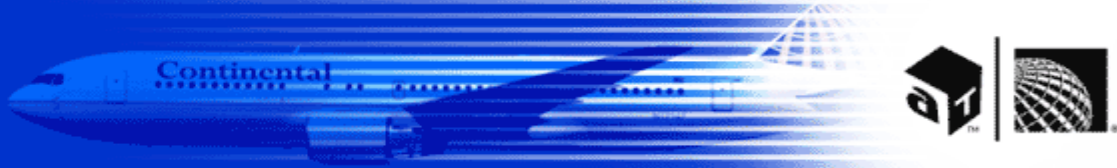


<b>Compliance Basics</b>		
<b>Level</b>	<b>Validation Action</b>	<b>Validated By</b>
1	<ul style="list-style-type: none"><li>•Annual On-site Data Assessment</li><li>•Quarterly Network Scan</li></ul>	<ul style="list-style-type: none"><li>•Data Security Company</li><li>•3rd Party Scan Vendor</li></ul>
2	<ul style="list-style-type: none"><li>•Annual On-site Data Assessment</li><li>•Quarterly Network Scan</li></ul>	<ul style="list-style-type: none"><li>•Data Security Company</li><li>•3rd Party Scan Vendor</li></ul>
3	<ul style="list-style-type: none"><li>•Annual Questionnaire</li><li>•Quarterly Network Scan</li></ul>	<ul style="list-style-type: none"><li>•Service Provider</li><li>•Quarterly Network Scan</li></ul>



# Our TOP 5 PCI Compliance Issues

5. Firewall, Firewalls, and more Firewalls
4. WiFi to LAN Segmentation
3. Encrypt Everything
2. Not enough time nor money
- 1. Credit Card Companies Only Endorse IT**



# Questions



<http://www.visa.com/cisp>