

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

PCI Security Standard

CS 4950/5950
Homeland Security &
Cybersecurity

Lesson 26
PCI Data Security Standard

Rick White, Ph.D.
University of Colorado, Colorado
Springs



1
Esc


1

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Credit Card Transactions

- Stage 1: Authorization
- Stage 2: Batching
- Stage 3: Clearing
- Stage 4: Funding



2
Esc

2

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Stage 1: Authorization

- Customer Initiates Purchase
- Merchant Requests Authorization
- Request Sent to Processor
- Forwarded to Card Network
- Authorized by Issuing Bank
- Forwarded to Acquiring Bank
- Returned to Merchant
- Customer Purchase Completed

CUSTOMER
The cardholder initiates a purchase.

MERCHANT
The merchant processes the credit card information and requests authorization.

PAYMENT GATEWAY
The payment gateway routes information to the processor.

PROCESSOR
The processor submits the authorization request to the card network.

CARD NETWORK
The card network submits the authorization request to the issuer.

CUSTOMER
The cardholder receives the purchased items or services.

MERCHANT
The merchant accepts the transaction.

ACQUIRER
The acquiring bank forwards the authorization response to the merchant.

CARD NETWORK
The card network forwards the authorization response to the acquiring bank.

ISSUER
The issuer approves the transaction.

3
Esc

3

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Stage 2: Batching

- Merchant Collects Authorizations
- Forwards All to Acquiring Bank

MERCHANT
The merchant's daily sales accumulate in a batch.

ACQUIRER
The merchant sends the batch of transactions to the acquiring bank for payment.

4
Esc

4

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Stage 3: Clearing

- a) Authorizations Sent to Issuers
- b) Issuers Debit Accounts
- c) Payment Sent to Card Networks
- d) Card Networks Transfer Funds
- e) Payment Sent to Acquiring Bank

The diagram illustrates the clearing process. It shows an acquirer bank on the left and an issuer bank on the right, both connected to a central card network. The acquirer bank submits a batch to the card network. The card network distributes the batch to the issuer's issuing bank. The issuing bank charges the cardholder and routes the payment through the card network. The card network then submits the requested amount to the acquirer bank, which receives payment from the card network.

5 Esc

5

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Stage 4: Funding

- a) Deposit to Merchant's Account
- b) Final Payment is Less Fees

The diagram illustrates the funding process. It shows an acquirer bank on the left and a merchant on the right. The acquirer bank deposits the payments in the merchant's account. The merchant receives the payment, minus fees assessed by the network, issuer, and acquirer.

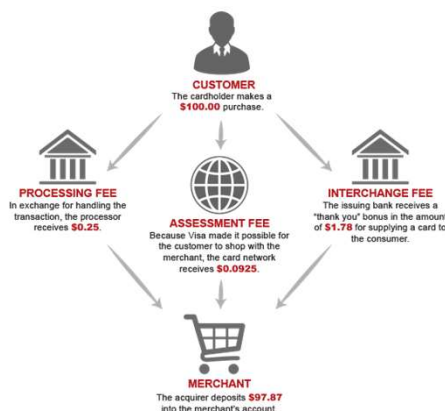
6 Esc

6



Payment Processing Fees

- Issuing Bank receives Interchange Fee, a “Thank You” for supplying the card to the customer.
- Acquiring Bank receives a Processing Fee for handling the transaction.
- Bank Card Network receives an Assessment Fee for facilitating the transaction.
- Final merchant payment is less than what customer paid.



7

Esc

7



PCI DSS

- Risky merchant behavior makes credit cards and associated information vulnerable to theft
- The card-processing ecosystem is rife with potential vulnerabilities:
 - Sales Register
 - PCs and Servers
 - Wireless Hotspots
 - Web Applications
- **The Payment Card Industry (PCI) Data Security Standard (DSS) was designed to reduce vulnerabilities and protect cardholder data.**

Risky Merchant Behavior

81% store credit card numbers

73% store credit card expiration dates

71% store credit card verification codes

57% store customer data


16% store other personal data

When asked why he robbed banks, Willie Sutton reportedly answered “that’s where the money is.”

8

Esc

8




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

PCI Scope


- PCI DSS applies to ALL agencies who store, process, or transmit cardholder data.
- PCI DSS is administered by the PCI Security Standards Council founded by major credit card companies.
- Agencies must comply with PCI or risk heavy fines or losing the ability to process credit card payments.**



PCI Security Standards Council, LLC
401 Edgewater Place
Suite 600
Wakefield, MA USA 01880

9
Esc

9

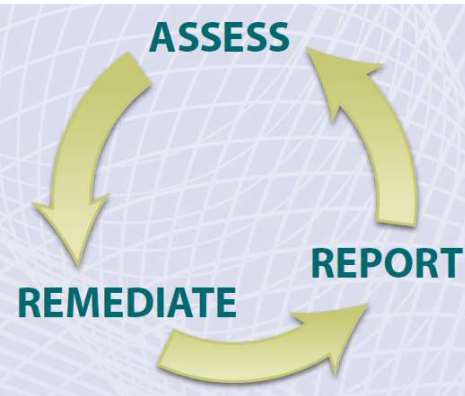


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

PCI Process

- Assess
 - Identify Cardholder Data
 - Inventory Payment IT Assets
 - Assess Vulnerabilities
- Remediate
 - Fix Vulnerabilities
 - Minimize Cardholder Data
- Report
 - Remediation Records
 - Compliance Reports

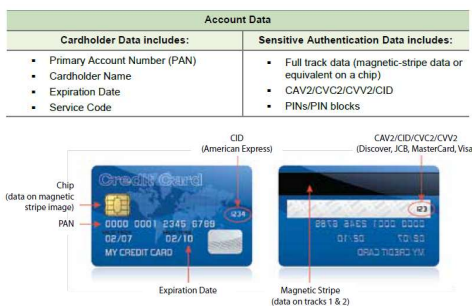


10
Esc

10

**Step 1: Assessment**

- a) Scope Applicability
 - Anything that transacts or stores credit card data is included in PCI DSS
- b) Scope Assessment
 - For smaller installations, assess entire suite
 - For larger installations, assess a sample suite
- c) Conduct assessment using PCI test procedures for each of the 12 DSS requirements



11

Esc

11


**PCI Data Security Standards**

Goals	Requirements
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. 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 cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. 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 data 11. 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 for all personnel

12

Esc

12



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

PCI Test Procedures


Requirement 1: Install & Maintain Firewall Configuration

PCI DSS Requirements	Testing Procedures	Guidance
1.1 Establish and implement firewall and router configuration standards that include the following:	1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: <ul style="list-style-type: none"> Network connections and Changes to firewall and router configurations 1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.

...

13
Esc

13



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity


Step 2: Remediation

a) Option 1: Fix Problem

- Install system or process necessary to satisfy DSS requirement


b) Option 2: Compensating Control

- Sometimes requirements can't be met due to legitimate technical or business constraints
- A Compensating Control is a "Work Around" approved by a Qualified Security Assessor



14
Esc

14









University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Step 3: Reporting

- a) Reporting requirements are established by merchants' card processing agency
- b) Smaller merchants may only need to complete and submit a Self-Assessment Questionnaire (SAQ)
- c) Larger merchants may need to complete a full Report on Compliance (ROC)
- d) Reports must also include an Attestation of Compliance (AOC)
- e) Merchants must submit reports to be certified PCI compliant


What is PCI Compliance?

					
Secure Network	Data Protection	Risk Management	Access Control	Monitoring	Maintenance
maintain firewall to protect consumer data	protect and encrypt cardholder data transmissions	maintain secure systems by targeting vulnerabilities	restrict access to cardholder data by a need-to-know basis	regularly monitor networks and track access to resources	maintain a policy that addresses security

15

Esc

15




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



16

Esc

16