



Credit Card Compliance

Informational Meeting

March 1, 2006

8:30 a.m.

Regina Herrington

Willis Marti



Agenda

- Introduction
- CIS Network Security – Willis Marti
- Business Environment Controls – Regina Herrington
- Questions/Answers

Merchant Levels (as of 3/1/06)

Merchant Level	Description
1	Merchant processing over 6 million transactions per year regardless of processing method or any merchant that has suffered a hack or attack that resulted in an account data compromise
2	Merchant processing 150,000 to 6,000,000 Visa or MasterCard e-commerce transactions per year
3	Merchant processing 20,000 to 150,000 Visa or MasterCard e-commerce transactions per year
4	Any merchant processing fewer than 20,000 Visa or MasterCard e-commerce transactions per year, and all other merchants processing up to 6 million transactions per year

** These levels are expected to change,
but VISA has not sent out official information yet. **

Validation Requirements

Level	Validation Action	Validated By	Due Date
1	<ul style="list-style-type: none"> ■ Annual On-Site Security Audit and ■ Quarterly Network Scan 	<ul style="list-style-type: none"> ■ Independent Security Assessor or Internal Audit ■ Qualified Independent Scan Vendor 	9/30/04
2 and 3	<ul style="list-style-type: none"> ■ Annual Self-Assessment Questionnaire and ■ Quarterly Network Scan 	<ul style="list-style-type: none"> ■ Merchant ■ Qualified Independent Scan Vendor 	6/30/05
4	<ul style="list-style-type: none"> ■ Annual Self-Assessment Questionnaire (Recommended) and ■ Quarterly Network Scan (Recommended) 	<ul style="list-style-type: none"> ■ Merchant ■ Qualified Independent Scan Vendor 	3/31/06

*Level 4 merchants must comply with CISP; however, compliance validation for merchants in this category will be determined at the acquirer's discretion.



Global Payment's Requirements

*Level 4 merchants must comply with CISP; however, compliance validation for merchants in this category will be determined at the acquirer's discretion (Global Payments).

- Must be compliant with CISP
- Must complete Annual Self-Assessment Questionnaire
- Due Date of March 31, 2006



Compliance Plan

- Complete Self-Assessment Questionnaire
- Identify any weak or missing controls
- Correct and/or implement controls
- Revise, Sign and Submit Completed, Compliant, Self-Assessment Questionnaire



University Breaches

- Georgia Tech – March 10, 2002
 - Undetermined number of employee financial records and university credit card numbers
- University of Georgia – January 2004
 - Applications
 - Nearly 20,000 students at risk
- Stanford University – May 11, 2005
 - Career Development Center
 - Nearly 10,000 people at risk
- University of Iowa – May 18, 2005
 - Bookstore
 - 30,000 people at risk



Penalties

- Fines
 - Members are subject to fines, up to \$500,000 per incident, for any merchant that is compromised and not CISP-compliant at the time of the incident
- Automatic “upgrade” to Level 1 if breached



Who needs to comply?

- EVERYONE that processes credit card payments
 - Terminal processing
 - Software processing
 - Other methods
- EPay/AggiE-Pay customers do not need to fill out questionnaire. Regina and Carlos have taken care of them on a system wide basis.



Payment Card Industry 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



Self-Assessment Questionnaire

YES – The merchant is compliant with the self-assessment portion of the PCI Data Security Standard.

NO – The merchant is not considered compliant. To reach compliance, the risk(s) must be resolved and the self-assessment must be retaken to demonstrate compliance.

If current processes require the answer to a question to be “no,” procedures must be changed to comply with the control. Do not turn in a questionnaire with “no” as a response. Please call us so that we can help turn the “no” into a “yes” by March 31, 2006.



Self-Assessment Questionnaire

N/A – If the question is not applicable to the payment processing method, please mark “n/a” and write a brief explanation.

For example: If all transactions for a particular merchant number are processed through a terminal, the answer to many questions will be “n/a” and the explanation will be “processed with terminal.”

** If there is not a “n/a” box but “n/a” would be your answer, add a “n/a” option. Do not check “yes” to show compliance when “n/a” is really correct.



Self-Assessment Questionnaire

Cover Sheet/Signature Page – This document is to be completed, signed, and then attached to the front of each completed Self Assessment Questionnaire.

1. Send completed questionnaires to:
April Kmiec
TAMU MS 6000
College Station, TX 77843-6000
2. Keep a copy for yourself.



CISP in a Nut Shell

Network Security

Willis Marti

Associate Director – CIS

wmarti@tamu.edu

Ellen Mitchell

Chief Security Analyst – CIS

ellenm@net.tamu.edu



Guidelines

- Computers must be grouped so that there is an “Inside” and an “Outside”.
 - “Inside” are any computers that handle customer information.
 - “Outside” should be everything else.
- Firewalls with NAT must separate any system that stores credit card information.
- No wireless.



More Guidelines

- Minimize communications between “Inside” and “Outside”.
 - Don’t combine office workstations with credit card processing.
 - No email servers or file servers “Inside”.
- Remote administration must be carefully planned and controlled.



Last Guideline

- Databases are **Evil**™.
 - Watch what you store, even “temporarily”.
 - Be wary of report generation requirements.
- Vendor certifications are tricky.
Remember, it must be valid in your environment.



Business Environment Controls

Regina Herrington
Assistant Financial Manager
rmherrington@tamu.edu

April Kmiec
Financial Management Supervisor I
a-kmiec@tamu.edu

Patti Ponzio
Financial Assistant II
pdp@vpfn.tamu.edu



Business Environment Controls

Questionnaire Guidelines

- Complete a questionnaire for each merchant number. If you think you have an exception, please contact April or Regina.
- Provide Organizational Information.
- Provide brief description of how transactions are processed/transmitted and how cardholder data is stored.
- Provide list of all third party providers.
- List Point of Sale (POS) software/hardware in use.



Basic Rule of Thumb

Treat customer credit card information like
you would want yours to be treated



Common questions

- 9.1 Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?
 - Further interpretation: There needs to be at least 2 forms of physical controls. For example, if the credit card information is stored in an office, the office needs to have a lock AND the cabinet that the information is in has to have a lock



Another Common Question

- 9.7 Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?
 - Please utilize the library records retention facility for old information that your office is not looking through on a regular basis.



Another Common Question

- 12.7 Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers?
 - Make sure that procedures are in place for all future employees that deal with credit card information to have security sensitive checks done. This includes student workers AND full time staff. You do not have to go back and have security checks done on current employees.



Whew! I'm done. Now what?

- Constantly monitor compliance
- Stay in compliance
- Re-evaluate questionnaire next year and resubmit
- Re-do every year to ensure constant compliance



Who can help?

- Financial Management Operations
 - Regina Herrington
 - April Kmiec
 - Patti Ponzio
- Computing Information Services
 - Willis Marti
- Departmental IT staff



Any Questions?

Thank you for coming!



Network Security

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

1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?
1.2	If wireless technology is used, is the access to the network limited to authorized devices?
1.3	Do changes to the firewall need authorization and are the changes logged?
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?
1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?
1.7	If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?



Network Security

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

1.8	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?
1.9	Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?
1.10	Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?



Network Security

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2.1	Are vendor default security settings changed on production systems before taking the system into production?
2.2	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?
2.3	If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?
2.4	If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?
2.5	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?
2.6	Are secure, encrypted communications used for remote administration of production systems and applications?



Business Environment Controls

Requirement 3: Protect stored data

3.1	Is sensitive cardholder data securely disposed of when no longer needed? (Business Officer and Departmental IT)
3.2	Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products? (Coordinate with Departmental IT)
3.3	Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products? (Do not keep written or electronic records of these codes.)
3.4	Are all but the last four digits of the account number masked when displaying cardholder data? (Coordinate with Departmental IT)
3.5	Are account numbers (in databases, logs, files, backup media, etc.) stored securely— for example, by means of encryption or truncation? (Coordinate with Departmental IT)
3.6	Are account numbers sanitized before being logged in the audit log? (Coordinate with Departmental IT)



Network Security

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

4.1	Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?
4.2	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?
4.3	If wireless technology is used, is the communication encrypted using WPA, LEAP, VPN, SSI at 128-bit, or WEP?
4.4	If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?
4.5	Is encryption used in the transmission of account numbers via e-mail?



Network Security

Requirement 5: Use and regularly update anti-virus software.

5.1	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?
-----	--



Network Security

Requirement 6: Develop and maintain secure systems and applications.

6.1	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?
6.2	Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?
6.3	If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?
6.4	Are all changes to the production environment and applications formally authorized, planned and logged before being implemented?
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?
6.6	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?



Network Security

Requirement 6 continued: Develop and maintain secure systems and applications.

6.7	Is sensitive cardholder data stored in cookies secured or encrypted?
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?



Business Environment Controls

Requirement 7: Restrict access to data by business need-to-know

7.1	Is access to payment card account numbers restricted for users on a need-to-know basis? (Also applies to Departmental IT)
-----	--

Business Environment Controls

Requirement 8: Assign a unique ID to each person with computer access

8.1	Are all users required to authenticate using, at a minimum, a unique username and password? (Business Officer and Departmental IT)
8.2	If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on? (Network and Departmental IT)
8.3	Are all passwords on network devices and systems encrypted? (Network and Departmental IT)
8.4	When an employee leaves the company, are the employee's user accounts and passwords immediately revoked? (Business Officer and Departmental IT)
8.5	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist? (Business Officer and Departmental IT)
8.6	Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period? (Business Officer and Departmental IT)

Business Environment Controls

Requirement 8 continued: Assign a unique ID to each person with computer access

8.7	Are accounts used by vendors for remote maintenance enabled only during the time needed? (Departmental IT)
8.8	Are group, shared, or generic accounts and passwords prohibited for non-consumer use? (Business Officer and Departmental IT)
8.9	Are non-consumer users required to change their passwords on a pre-defined basis? (Departmental IT)
8.10	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords? (Departmental IT)
8.11	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force? (Departmental IT)



Business Environment Controls

Requirement 9: Restrict physical access to cardholder data

9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility? <i>(Any physical access to data or systems that house cardholder data allows the opportunity to access devices or data, and remove systems or hardcopies, and should be appropriately restricted.)</i> (Business Officer and Departmental IT)
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices? (Network and Departmental IT)
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access? (Business Officer and Departmental IT)
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access? (Business Officer)
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data? (Business Officer and Departmental IT)



Business Environment Controls

Requirement 9: Restrict physical access to cardholder data

9.6	Are all media devices that store cardholder data properly inventoried and securely stored? (Business Officer and Departmental IT)
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)? (Business Officer and Departmental IT)



Network Security

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

10.1	Is all access to cardholder data, including root/administration access, logged?
10.2	Do access control logs contain successful and unsuccessful login attempts and access to audit logs?
10.3	Are all critical system clocks and times synchronized, and do logs include date and time stamp?
10.4	Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?
10.5	Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?



Network Security

Requirement 11: Regularly test security systems and processes.

11.1	If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?
11.3	Is a intrusion detection or intrusion prevention systems used on the network?
11.4	Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures installed?

Business Environment Controls

Requirement 12: Maintain a policy that addresses information security

12.1	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented? (Business Officer and Departmental IT)
12.2	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)? (Business Officer and Departmental IT)
12.3	Are information security policies reviewed at least once a year and updated as needed? (Business Officer and Departmental IT)
12.4	Have the roles and responsibilities for information security been clearly defined within the company? (Business Officer and Departmental IT)
12.5	Is there an up-to-date information security awareness and training program in place for all system users? (Business Officer and Departmental IT)
12.6	Are employees required to sign an agreement verifying they have read and understood the security policies and procedures? (Business Officer and Departmental IT)

Business Environment Controls

Requirement 12 continued: Maintain a policy that addresses information security

12.7	Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers? (Business Officer)
12.8	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards? (Business Officer and Departmental IT)
12.9	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties? (Business Officer and Departmental IT)
12.10	Are security incidents reported to the person responsible for security investigation? (Business Officer and Departmental IT)
12.11	Is there an incident response team ready to be deployed in case of a cardholder data compromise? (Business Officer and Departmental IT)