PCI Compliance
Security Awareness Program
For
Marine Corps Community Services

Contacts:
Paul Watson
Overview

• What is PCI?
• MCCS Compliance
• PCI DSS Technical Requirements
• MCCS Information Security Policies
• MCCS Common PCI Findings
• Making a Difference at MCCS
• Glossary of Terms
What is PCI?

- PCI stands for Payment Card Industry

- PCI is an umbrella term used for a comprehensive security program to protect credit card information from accidental disclosure
  - PCI SSC – PCI Security Standards Council
  - PCI DSS – PCI Data Security Standard

- Provides protections for all participants in a credit card transaction;
  - Cardholder (Marines, Marine family members, etc.)
  - Merchant (Exchanges, Seven Day Stores, Golf Pro-Shop, Clubs, etc.)
  - Banks/Acquirers (Bank of America)
  - Services Providers (Examples?)
  - Card Brands (Visa, MasterCard, American Express, Discover, JCB)
PCI Data Security Standard

- Represents:
- Merchant and Card industry required data security practices
- Common Acceptance and participation by multiple card brands (5 TODAY)
- Establishes a Single Security Auditing Procedures (SAP)
- **Best Way To Protect Credit Card Information For All MCCS Activities.**

- Best Sources of Reference:
  - for PCI Data Security Standards and Requirements
  - (URL: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org))

- for Business Understanding of Merchant Compliance Requirements
  - (URL: [www.visa.com/cisp](http://www.visa.com/cisp))
Evolution of PCI and Card Brand Security

• Since 2001, Card Brands Security Programs & Enforcement:
  – Visa CISP - largely onsite audit driven
  – MasterCard SDP – primarily scan, questionnaires
  – American Express DSOP - nothing
  – Discover DISC - nothing
  – JCB and Diners – nothing (also original participants in PCI)

• PCI Data Security Standard started in 2004

• PCI Data Security Standard v1.1 – September 2006
  – Common standard of best practices from individual card brand security programs.
  – Retain individual card brand enforcement programs
  – Maintained by the PCI Security Standards Council

• PCI Data Security Standard v1.2 – October 2008
Why PCI Compliance Matters

1. Demonstrates the MCCS’ commitment to protecting our customers confidential data.
2. Indicates stronger controls & processes to assess IT risk and prevent data compromise.
3. Helps to avoid substantial fines and penalties from card industry.
4. Demonstrates compliance for key customers who demand adherence to the PCI DSS.
5. Provides better protection for Marines and Marine family members.

Source: Visa – July 2006
Payment Card Industry Overview

Acquirer
(BofA/Chase)

and/or

Issuer

is a member of

MasterCard

is a member of

VISA

may or may not be the same as

Merchant
(MCCS Activities)

Service Providers

uses payment card to purchase goods or services from

Cardholder
(Marine)

issues cards to
PCI Data Security Standard Applies to Who?

- Anyone who “Stores, Processes or Transmits” cardholder data Must comply with the PCI DSS
- **Including:**
  - Members (Banks & Acquirers – Bank of America, Chase Paymentech)
  - Merchants (MCCS – Exchanges, Seven Day Stores, Clubs, etc.)
  - Service Providers (Examples?)
  - Network Components (Modems, Wireless Routers, Firewalls, etc.)
  - Servers (In store controller/management systems)
  - Applications (Point of Sale (POS) Software – Triversity, HSI, EPOS, etc.)

that connect to cardholder data environments.
What does PCI protect?

- The cardholder’s identity and confidential data, including:
  - Magnetic stripe (track 1 and track 2 data)
  - Card Verification Values (CVC, CVV2 – 3 or 4 digit codes printed on back or front of card)
  - Payment Account Numbers (PAN)
  - Personal Identification Numbers (PIN)
  - Passwords
  - Card expiration dates
  - Personal data
    - Name
    - Address
    - Email
Card Compromises have a Ripple Effect

- MCCS
- Data Breach
- Families, Partners, Vendors
- Paymentech
- Visa / MC
- Direct Impacts
- Indirect Impacts
- MCCS Partners
- Competitors
- Potential Legislation
Why? What’s at risk?

- Data breaches can lead to significant adverse consequences

- **For Marine Corps Community Services:**
  - Unwanted media attention – i.e. DSW, TJX, Hannafords
  - Lost revenue and/or financial damages
  - Lost time and distractions to Marines and their families
  - Litigation
  - Substantial VISA and MasterCard penalties

- **For the cardholder:**
  - Identity theft
  - Unauthorized charges to their credit or debit card account
  - Damage to their personal credit rating
  - Financial losses
Cost of a Data Breach

Studies estimate the 2007 Cost of a Data Breach at:
• $197* per compromised credit card record.
• an average total per-incident cost of - $6.3 million*

What does this mean to MCCS?
• A single MCCS command can conduct up to 650,000 transactions per year or more.
• Card breaches often take 12 - 18 months to be identified
• All cards used during that period could be compromised or at risk.
• Total cost to MCCS for a breach at a single base can potentially be up to $128 Million. (650,000 X $197)

Fines per Incident:
• VISA – Up to $500,000
• MC – Often $25 per card = up to $16,250,000

* Source: Ponemon Institute's 2007 Cost of a Data Breach Report
Non-Compliance Fines and Enforcement

- **Compliance is enforced** by MCCS’ banks and fines start from the Card Brands (Visa / MC)
- i.e. The security program has teeth!

- **VISA CISP Compliance Fines & Penalties** (One brand example)
  - Fines the responsible bank
    - Typically $5,000-$25,000 per month per merchant
  - Bank passes fines on to merchant (MCCS)
  - Bank imposes restrictions on merchant (MCCS)
MCCS Goal - - Utopia: Safe Harbor

- **Safe harbor provides merchants protection from fines in the event that they or one of their service providers experiences a data compromise.**

- **To attain safe harbor status MCCS must:**
  - Validate compliance with a third party QSA annually
  - Maintain full PCI compliance at all times
  - Demonstrate that prior to a compromise, all PCI compliance validation requirements were fully met.
MCCS Compliance – Visa & MC

VISA and MasterCard Requirements

• **Level One** (> 6 mil single card brand transactions/yr):
  – Includes all types of payment card transactions (debit, credit, phone, etc.)
  ✓ Annual on-site PCI data security assessment (SAP/ROC)
  ✓ Quarterly network vulnerability scans
• PCI DSS
• Technical Requirements
PCI Data Security Standard (DSS)

- The Digital Dozen
  - 12 PCI DSS requirements
- 6 Control Objectives
- 226 Detailed security focused sub(requirements)
PCI DSS Control Objectives

1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Monitor and test networks regularly
6. Maintain an information security policy
The PCI DSS Digital Dozen

1. Install & Maintain a Secure Firewall Configuration
2. Maintain System Configuration Standards
3. Protect Stored Cardholder Data
4. Encrypt Transmission of Cardholder Data Across Open, Public Networks
5. Use and Regularly Update Anti-virus Software or Programs
6. Develop & Maintain Secure Systems & Applications
7. Restrict Access to Cardholder Data By Business Need to Know
8. Assign Unique IDs and Implement Strong Password Controls
9. Restrict Physical Access to Cardholder Data
10. Track and Monitor All Access to Network Resources and Cardholder Data
11. Regularly Test Security Systems & Processes
12. Maintain an Information Security Policy
226 Sub Requirements

• Detailed in the PCI Data Security Standard

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

8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
  • Password
  • Token devices (for example, SecureID, certificates, or public key)
  • Biometrics

8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users
What to Do if You Suspect a Compromise

• **Identification**
  1. Is a secured area found unlocked and confidential information missing?
  2. Have you noticed new unidentifiable equipment in the POS area?
  3. Do security logs alert you to suspicious activities?

• **Reporting**
  1. Immediately inform your manager of the compromise. If unavailable, inform the Information Security Manager or IT Point of Contact for your Command.
  2. Determine if there is an ongoing threat to customer account information or MCCS network data. Notify the IT\Network Manager immediately.
MCCS – Common PCI Findings

• Compiled from onsite PCI assessments performed at 12 bases

• Most common non-technical findings:
  – Management of visitors; badged, authorized, escorted
  – Security of paper credit card receipts and reports
  – Password security
  – Maintaining logs
  – Keeping lockable items locked
Challenge Visitors

- PEDs are now being attacked
- Attackers are becoming more sophisticated and bold with their attacks.
- Employees need to be vigilant of visitors; wearing proper badges; properly authorized to be working in area.
- Do not be afraid to question them.

Vigilance can prevent attacks such as these.
Kiosk False Front & Hidden Camera

Camera hidden inside pamphlet holder next to ATM at the University of Texas campus

Unauthorized personnel install these devices.

Source: http://www.utexas.edu/police/alerts/atm_scam/
Visitor Logging

• Logs serve a purpose:
• Require visitor logs for all areas storing or processing cardholder data
• Enforce the signing of logs by all visitors
• Retain logs for at least a year
Paper Receipt Security and Retention

• Paper receipts should be stored:
  – In rooms or closets with secured locks
  – In containers marked
    • “FOUO” (For Official Use Only)
    • with storage and retention dates

• Containers contents should be:
  – Inventoried
  – Periodically reviewed against inventory lists
Records Warehousing

Records Warehousing
Best Practices

The ultimate in records security
Password Security

• Passwords should be secure and protected:
• Minimum of 7 characters
• Alpha, numeric, and special characters – U$mC@1S#1
• Do not use common names or words that can be found in the dictionary
• Do not write down or keep passwords in a public place where they may be discovered (Insert picture of post-it note on a monitor)
Physical Security

• Clear desk – Do not leave papers or reports containing cardholder data on desktops or areas accessible by customers.
• Lock all doors, cabinets or draws securing receipts or other papers holding card data.
• Don’t leave passwords on post-its or viewable at desks.
• Do not promote or allow “tail-gating.”
• Ensure customer receipts and cardholder data are not accessible by those that are not authorized.
Making a Difference at MCCS

• If you accept a customer’s credit card for payment, here are some ways you can help to meet PCI DSS compliance:

1. Protect your customer’s cardholder data at all times.
2. Don’t write down or share customer account information.
3. Don’t ask a customer for their CVC or CVV2 when the customer is present to authenticate their own card.
4. If your department uses AVS, do ask a customer to confirm their zip code and address.
5. Be sure to protect merchant receipt copies that have customer payment card account numbers on them.
Making a Difference at MCCS

• If you work in an office that processes payment card transactions, here are some ways you can help to meet PCI DSS compliance:

1. Don’t share card data over the phone or with those who are not authorized to have such information.
2. If you work in an area that requires use of payment card data, do not take card data home or leave it on your desk unattended or overnight. (Clean Desk Policy)
3. Use computers for acceptable business purposes only. Do not load personal music, files, or applications or access your personal email. (Acceptable Use Policy)
4. Be sure to change your passwords regularly.
5. Learn how to construct a strong computer password.
6. Do not share your passwords with others, even your manager or MCCS IT personnel.
7. Don’t leave computers on and unattended. Log out and/or use locked screen savers.
8. Maintain a segregation of duties between development, testing/QA, and production.
9. Be aware of data retention requirements for payment card receipts and related transactions.
10. Read your MCCS Information Security Policy and attend your annual security awareness training.
If you work in MCCS IT areas, here are some ways you can help to meet PCI DSS compliance:

1. Never store magnetic stripe, CVC2 or PIN data after authorization.
2. Payment card Primary Account Numbers (called PAN) should always be stored encrypted using strong encryption algorithms such as 3DES and AES.
3. Full PANs should be masked when displayed.
4. Payment cardholder data should always be encrypted during transmission over public networks, i.e. wireless or the internet.
5. Access to databases where payment card and other sensitive data resides should be restricted to those with a business need to know.
6. Ensure the use of anti-virus software including automatic updates and periodic scans.
7. Do not share your user IDs or passwords.
8. Don’t use administrator accounts to perform regular user tasks.
9. Ensure that all non-console administrative access is encrypted. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.
10. Restrict physical access to payment card data or systems storing card data.
11. Protect and manage backup media. Store media securely, log removal of media, transfer securely, and destroy securely according to the MCCS data retention policy.
12. Attend annual security awareness training.
Making a Difference – HR and Training

- If you work in MCCS HR areas, here are some ways you can help to meet PCI DSS compliance:
  1. Ensure that new employees are properly screened and background checks are performed appropriate to their job responsibilities.
  2. Inform employees and managers of their obligation to read and understand Information Security Policies.
  3. Ensure that new employees are informed of MCCS Acceptable Use Policies for IT equipment and customer information.
  4. Ensure that new employees attend IT training including how to change their passwords and how to use and protect customer data.
  5. Ensure that managers provide new employees with IT systems access appropriate to their job responsibilities. (business need to know)
  6. Inform IT in a timely manner about employee terminations so their user IDs, network and systems access privileges may be removed.
  7. Execute periodic security awareness communication programs such as emails, notices, posters, etc.
If you work in MCCS Finance or Purchasing, here are some ways you can help meet PCI DSS compliance:

1. Store receipts, statements and any other financial data containing cardholder information in a locked file drawer, safe or other designated secure area.
2. If payment card Primary Account Number (called PAN) is downloaded from banks or card brand websites, data should always be stored encrypted. This applies to Excel spreadsheets, Word and PDF documents.
3. Restrict access to PANs to only those individuals in the accounting and finance departments with a business need to know.
4. Storage and inventory of transaction and card receipts should be minimized to only that which is required for business purposes. (i.e. 18 months)
5. Storage areas containing payment card data must be monitored with video cameras and a card access system that provides an audit trail of each individual entry.
6. Maintain accurate and complete logs of all archived or stored data including accounting boxes with card data and receipts stored securely offsite.
7. Do not share passwords.
8. Never send card account numbers via email or in any other unsecured manner.
9. Attend annual security awareness training.
Making a Difference - Facilities

- If you work in MCCS Facilities, here are some ways you can help to meet PCI DSS compliance:

  1. Maintain physical locks and access controls on storage areas – these are key to protecting cardholder information.
  2. Cardholder receipts and other accounting data that has full payment card Primary Account Numbers (called PAN) should only be accessible only to those with authorized access.
  3. Re-consider shared access by other departments.
  4. Avoid open windows and access points that could lead to theft of data.
  5. Operate and maintain video surveillance equipment for secure data areas.
  6. Maintain a visitor log that indicates accountability for who accesses areas where sensitive information is stored, transmitted or processed.
  7. Retain video recordings for at least 90 days and visitor logs for at least one year in the event of a data compromise.
  8. Attend annual security awareness training.
Making a Difference – Legal, Purchasing, Marketing and Internal Operations

- If you work at MCCS in Purchasing, Legal, Marketing or Internal Operations, here are some ways you can help to meet PCI DSS compliance:
  1. Make sure MCCS contractual agreements for third-parties that store, transmit and/or process MCCS cardholder data have appropriate PCI and security language as identified in Req 12.8.
  2. Practice vendor due diligence and management.
  3. Ask your vendors how they comply with the PCI DSS.
  4. Develop secure mechanisms for sharing card data. (Ask MCCS IT)
  5. Review ongoing PCI compliance requirements for all third-parties.
  6. Develop contract practices to ensure MCCS vendors maintain ongoing PCI compliance, how they inform you and what happens if they don’t meet those requirements.
  7. Attend annual security awareness training.
Where to Get More Information

2. PCI Security Standards Council website (www.pcisecuritystandards.org)
Congratulations!
You have completed your 2012/2013 PCI Security Awareness Training

Complete the form below, print this page and return to Human Resources.

__________________________  ______________________________
Print Name & Date            Command/Office

__________________________  ______________________________
Signature                   Supervisor Signature