DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3044 CATLIN AVENUE
QUANTICO, VIRGINIA 22134-5103

IN REPLY REFER TO

1700
MR

AUG 15 2016

From: Commandant of the Marine Corps

Subj: MANDATORY ANNUAL PAYMENT CARD INDUSTRY SECURITY AWARENESS TRAINING FOR MARINE CORPS COMMUNITY SERVICES EMPLOYEES

Ref: (a) Payment Card Industry Data Security Standards
(b) MCO P1700.27B w/Ch 1
(c) MCO P12000.11A

Encl: (1) Electronic Payment Card Industry Security Awareness Training Course

1. Situation. In accordance with the references, this memorandum establishes an annual Payment Card Industry (PCI) Security Awareness Training requirement for all Marine Corps Community Services (MCCS) employees (including appropriated fund, nonappropriated fund, military, and contractors) with access to MCCS facilities, systems, and/or records. Currently, only MCCS employees directly involved in processing customer credit card information are required to complete this annual training, which is now being expanded to all MCCS employees to comply with PCI business requirements and to raise awareness of proper procedures for handling sensitive data. In order to maintain certification to process credit card transactions, MCCS is required to provide documentation during our annual PCI compliance audit showing that employees are required to complete annual PCI Security Awareness Training and that training has been completed. Noncompliance with PCI standards/business requirements could result in data breaches and have significant adverse consequences for both MCCS operations and our customers, including identity theft, damaged credit ratings, multi-million dollar charges and fines, litigation, unwanted media attention, and loss of our ability to process credit card transactions.

2. Mission. To protect the financial information of Marines and their families, comply with PCI standards/business requirements, and raise awareness of our employees' responsibility to protect sensitive information.

3. Execution.

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. As required by reference (a), all MCCS employees and new hires (including appropriated fund, nonappropriated fund, military, and contractors) with access to MCCS facilities, systems, and/or records will complete annual PCI Security Awareness Training.

(2) Concept of Operation. The PCI Security Awareness Training will be incorporated into annual training requirements to educate MCCS employees on PCI requirements, types of sensitive data, and physical security controls and processes.

b. Subordinate Element Missions

(1) Training Branch, CMC (MRT), will:

(a) Develop and publish the electronic courseware for PCI Security Awareness Training in ETHOS and require a certificate for course completion be submitted into employees' training transcripts. PCI Security Awareness Training course materials are provided in the enclosure.

(b) Update the list of mandatory, annual training requirements for all MCCS employees and new hires to include PCI Security Awareness Training.

(c) Continue to monitor compliance with annual training requirements and elevate any systemic issues to the respective Commander and MCCS Director.

(2) Commanding Generals. Commanding Generals will help communicate changes and ensure that installations implement annual MCCS PCI Security Awareness Training.

(3) Regional/Installation Commanders. Regional/installation commanders will ensure regional and installation MCCS Directors implement annual MCCS PCI Security Awareness Training.

(4) MCCS Directors/Installation Human Resources-Training Directors. MCCS Directors/Installation Human Resources-Training Directors will ensure that all MCCS employees and new hires complete MCCS PCI Security Awareness Training annually and that certificates of completion are uploaded into ETHOS.

4. Administration and Logistics. Forward recommended changes to annual training requirements to CMC (MRT).

5. Command and Signal

a. Command. This LOI is applicable to those Commanders and staff responsible for the operation of MCCS programs.

b. Signal. This LOI is effective on the date signed.

CINDY WHITMAN LACY

Distribution:

COMMARFORCOM
CG MCCDC
CG TECOM
COMMCICOM
CG MCIPAC
CG MCIWEST
CG MCIEAST
CG MCRD/WRR
CG MCAGCC
CG MCRD/ERR
CO Camp Allen
CO H&S BN HQMC
CO MARBKS 8TH & I
CO MCAS Beaufort
CO MCAS Cherry Point
CO MCAS Iwakuni
CO MCAS Miramar
CO MCAS New River
CO MCAS Yuma
CO MCB Hawaii
CO MCB Quantico
CO MCLB Albany
CO MCLB Barstow

MCCS MCICOM
MCCS MCIEAST, MCB Lejeune
MCCS MCIWEST, MCB Pendleton
MCCS MCIPAC, MCB Butler
AC/S MCCS MCRD/WRR
AC/S MCCS MCAGCC
MCCS Dir Camp Allen
MCCS Dir HQBN HH
MCCS Dir MARBKS 8th & I
MCCS Dir MARFORCOM
MCCS Dir MARFORPAC
MCCS Dir MARFORRES
MCCS Dir MCAS Cherry Point
MCCS Dir MCAS Iwakuni
MCCS Dir MCAS Miramar
MCCS Dir MCAS Yuma
MCCS Dir MCB Camp Lejeune, New River
MCCS Dir MCB Camp Pendleton, Barstow
MCCS Dir MCB Hawaii
MCCS Dir MCB Quantico
MCCS Dir MCLB Albany
MCCS Dir South Carolina

PCI Security Awareness Training
for
Marine Corps Community Services

Local PCI POC:
Gabrielle Bowie
Enterprise Cybersecurity and Compliance
703-432-2920
gabrielle.e.bowie@usmc-mccs.org

Overview

- What is PCI
- MCCS Compliance
- PCI DSS Technical Requirements
- MCCS Information Security Policies
- MCCS Common PCI Findings
- Making a Difference at MCCS

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 or malicious 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, Chase)
  - Card Brands (Visa, MasterCard, American Express, Discover,)

PCI Data Security Standard

Represents:

- Merchant and card industry required data security to include technical and operational requirements.
- Common acceptance and participation by multiple card brands.
- Establishes a single Security Auditing Procedure (SAP).
- “Best Practices” with respect to protecting credit card information for all MCCS activities.

Best sources of reference:

PCI Data Security Standards and Requirements -

- (URL: www.pcisecuritystandards.org)

Business Understanding of Merchant Compliance Requirements -

- (URL: www.visa.com/cisp)

Evolution of PCI and Card Brand Security

Since 2001, Card Brands Security Programs & Enforcement:

- Visa Cardholder Information Security Program - largely onsite audit driven
- MasterCard Site Data Protection Program– primarily scan, questionnaires
- American Express Data Security Operating Policy – no enforcement
- Discover Information Security & Compliance _ no enforcement
- Japan Credit Bureau (JCB) and Diners – no enforcement (original participants in PCI)

PCI Data Security Standard started in 2004

- Maintained by the PCI Security Standards Council

Why PCI Compliance Matters

1. Demonstrates MCCS' commitment to protecting our customers card holder data.
2. Standardizes controls and processes to assess risk and prevent data compromise.
3. Helps avoid fines and penalties from the credit card industry (assessed by card brands – Visa, MasterCard etc.).
4. Demonstrates our commitment to compliance for key vendors who demand adherence to the PCI DSS (Bank of America).
5. Provides better protection for Marines and Marine family members.

PCI Data Security Standard Applies to Who?

All entities that "***Store, Process or Transmit"*** cardholder data must comply with the PCI DSS.

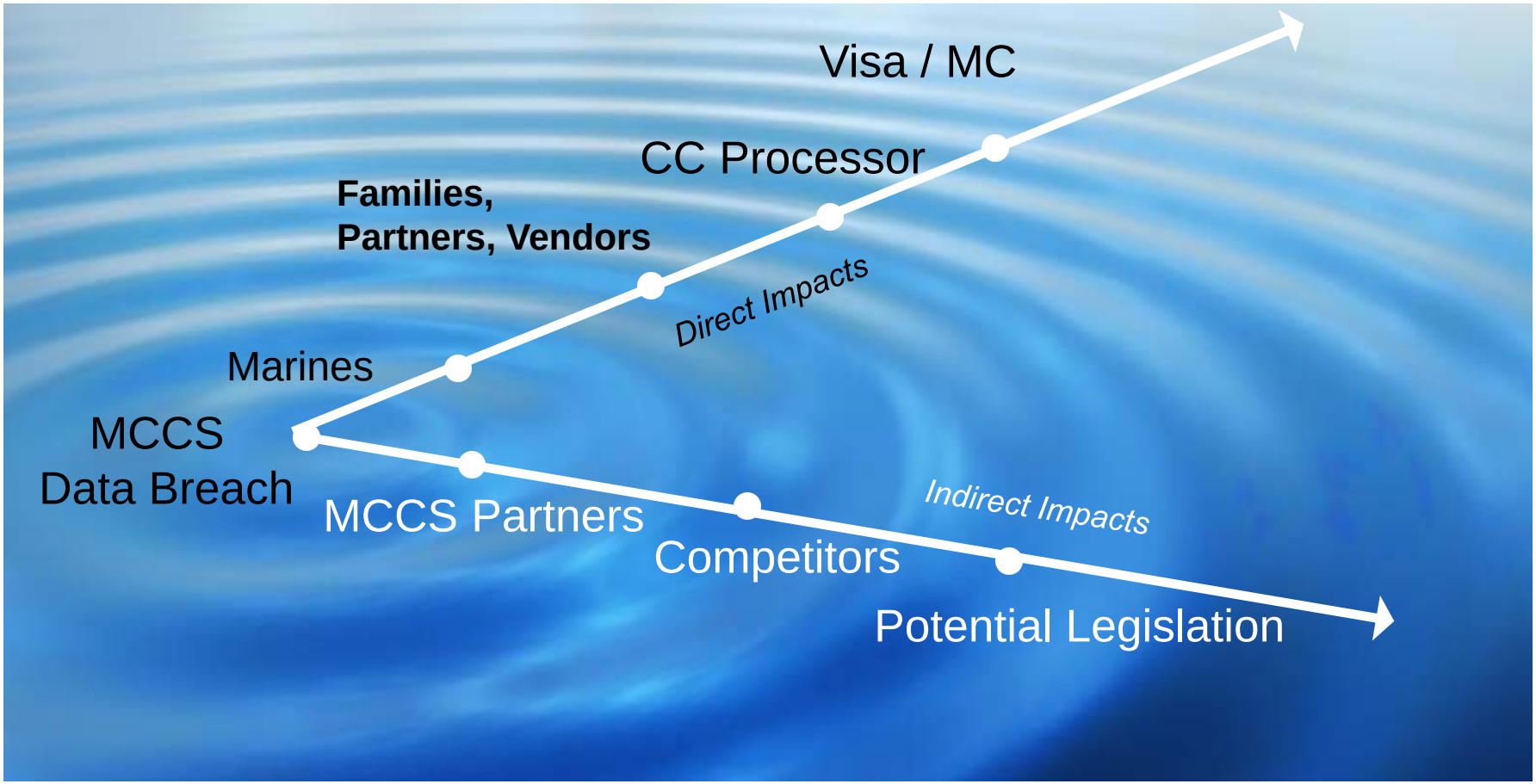
- Members (Banks & Acquirers – Bank of America, Chase)
- Merchants (MCCS – Exchanges, Seven Day Stores, Clubs, etc.)
- Network Components (Routers, Firewalls, etc.)
- Servers (In store controller/management systems)
- Applications (Point of Sale (POS) Software – HIS, HSI, RPOS, etc.)

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 the 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



Why? What's at Risk?

Data breaches can lead to significant adverse consequences.

Marine Corps Community Services:

- Unwanted media attention – i.e. TJ Max, Target, Michaels, PF Chang
- Lost revenue and/or financial damages
- Lost time and distractions to Marines and their families
- Litigation
- Substantial VISA and MasterCard penalties
- Ultimately loss of revenue as no longer able to take credit cards

For the cardholder:

- Identity theft
- Unauthorized charges to their credit or debit card
- Damage to their personal credit rating
- Financial losses

Cost of a Data Breach

Studies estimate the 2012 *Cost of a Data Breach*:

- **$204*** per compromised credit card record
- An average total per-incident cost of - **$6.75 million***

What does this mean to MCCS?

- 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 Command can potentially be up to **$133 Million.** (650,000 average transactions X $204)

Fines per Incident:

- Up to **$500,000***

* Source: Ponemon Institute's 2012 Cost of a Data Breach Report

What if MCCS is not in compliance?

MCCS maintains a commitment to protect customer's card holder data. Compliance is enforced by MCCS' banks and any fines asserted start from the Card Brands (Visa / MC).

Card Brand

- Fines the responsible bank
- Typically $5,000-$25,000 per month per merchant up to 2% of sales

Bank

- Bank passes fines on to merchant (MCCS)
- Bank imposes restrictions on merchant (MCCS)

MCCS

- Higher fines and fees
- Loss of ability to conduct credit card transactions

What does PCI compliant really mean?

Requirements of the PCI DSS include:

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.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
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.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

MCCS – Common PCI Findings

Most common non-technical findings :

- Management of visitors lacking – need to be badged, authorized, escorted
- Security of paper credit card receipts and reports missing
- Access control to secure areas missing
- Password security poor
- Logs not adequately maintained
- Unencrypted emailing of PAN data
- Keeping items locked

Most common technical findings :

- Shared administrative accounts or passwords
- Missing system logs or video
- Unnecessary access to systems or databases

What to Do if You Suspect a Compromise

Identification

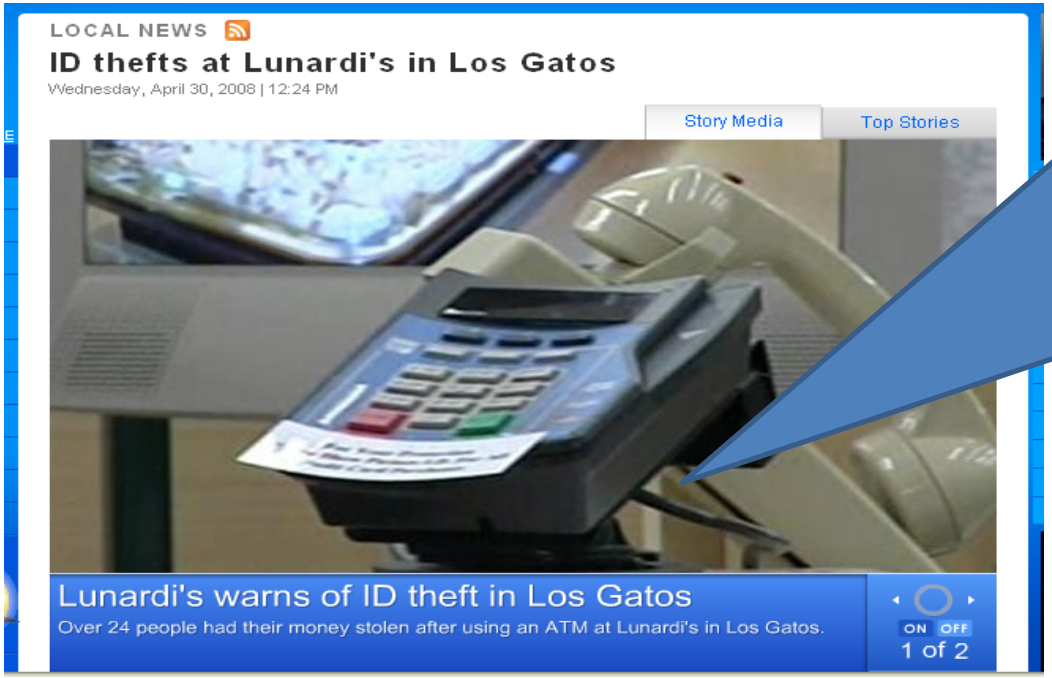
- Is a secured area found unlocked and confidential information missing?
- Have you noticed new unidentifiable equipment in the POS area?
- Do security logs alert you to suspicious activities?

Reporting

- Immediately inform your manager of the compromise. If unavailable, inform the PCI Point of Contact or MIS staff for your Command.
- Determine if there is an ongoing threat to customer account information or MCCS network data. Notify the PCI POC, MIS staff and the HQ Help Desk immediately.

How do we make a difference?
Challenge Visitors.

- Employees need to be vigilant of visitors; wearing proper badges; properly authorized to be working in area; escorted.
- Do not be afraid to question them.
- Beware of illegal hardware and software installations.



Key Logger device installed by unauthorized visitor. Can be used to capture credit card data during transactions

How do we make a difference?

Be Aware.

Kiosk False Front & Hidden Camera

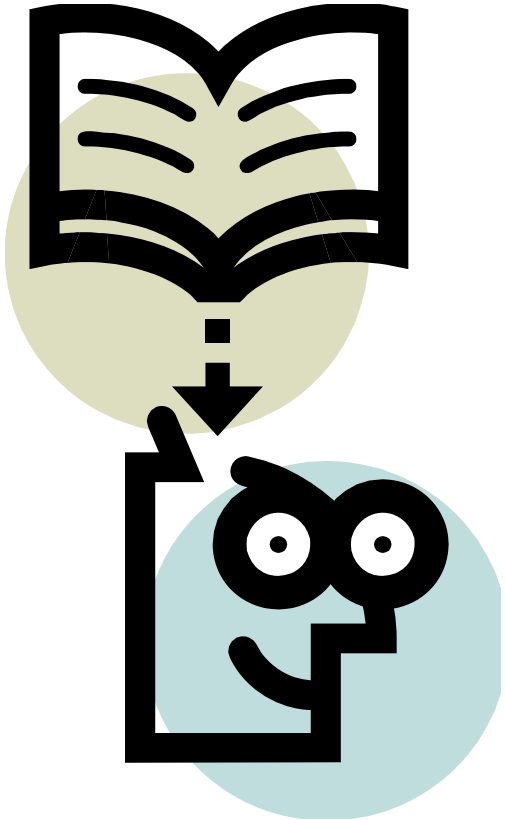
False front (Skimmer) placed over the face of the ATM in Texas.

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

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

How do we make a difference?
Ensure Visitor Logging.

- 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.
- Temporary badge management - ensure all visitors can be identified.



How do we make a difference?

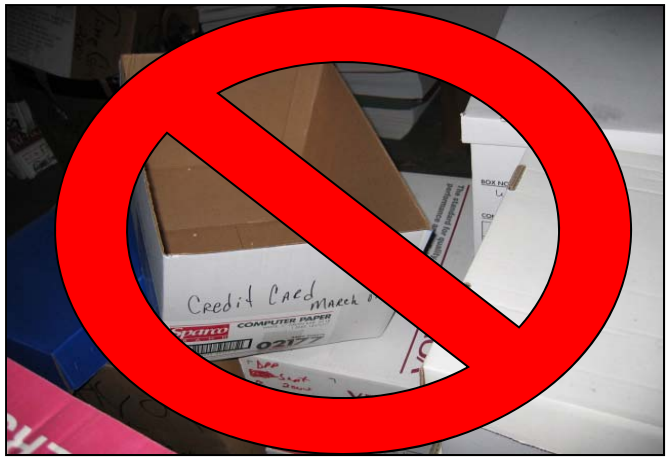
Ensure Proper Receipt Security and Retention.

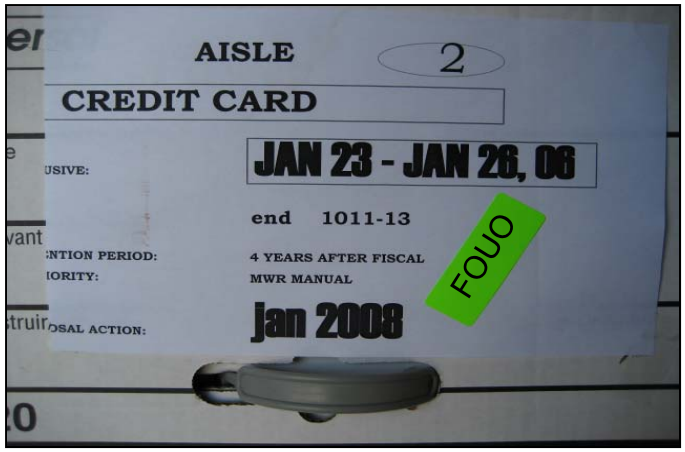
Paper receipts should be stored:

- In rooms or closets with secured locks and cameras
- In containers marked
  - "FOUO" (For Official Use Only)
  - with storage and retention dates

Containers contents should be:

- Inventoried
- Periodically reviewed against inventory lists



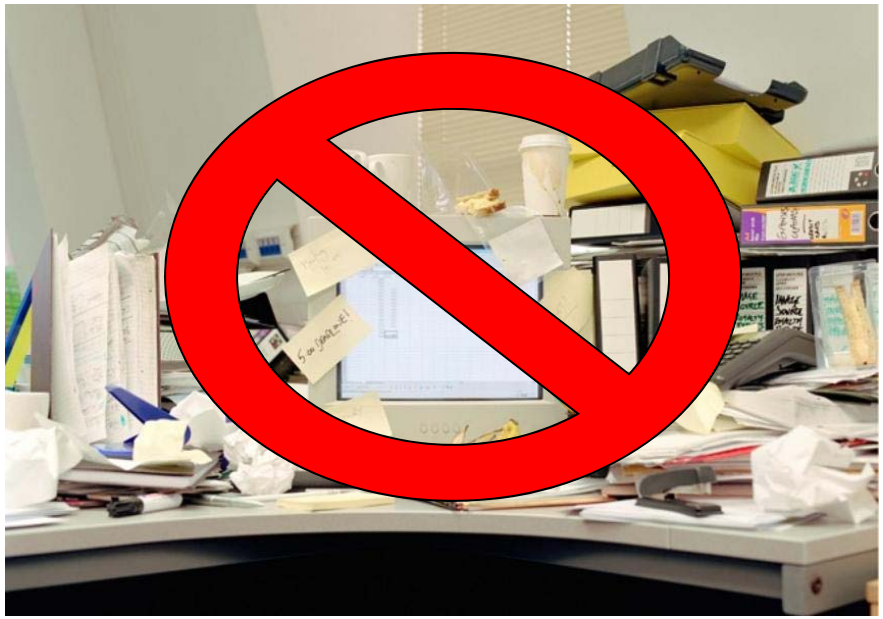


How do we make a difference?
Use Password Security.

- Passwords should be secure and protected and **Never Shared.**
- Minimum of 15 characters, a passphrase is preferred.
- Alpha, numeric, and special characters i.e. 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.
- Use Common Access Card (CAC) whenever possible.

How do we make a difference?
Physical Security.

- Clean 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.



Violators loiter near building entrances that require card key access and follow other employees in. They then enter offices and steal information and property, especially cash and credit cards.

Where to Get More Information

1. Visa Cardholder Information Security website (www.visa.com/cisp)
2. PCI Security Standards Council website (www.pcisecuritystandards.org)
3. Crossroads MCCS Information Security SharePoint site (http://crossroads/default.aspx)

PCI Security Awareness Training

This certifies that I have received training on my credit card data security responsibilities and I understand that I am responsible for safeguarding credit card data that I may have access to incident to performing official duties. I also understand I may be subject to disciplinary action for failure to properly safeguard credit card data, for improperly using or disclosing credit card data, and for failure to report any known or suspected loss of credit card data or the unauthorized disclosure of information.

_____	_____	_____
Name	Employee ID	Date

Making a Difference

Select each box for information

MCCS

IT

HR/Training

Finance/Purchasing

Legal/Marketing/Operations

Facilities

Done

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)
3. Use computers for acceptable business purposes only. (Acceptable Use Policy)
4. Be sure to change your passwords regularly.
5. Learn how to construct a strong computer password or passphrase.
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 locking 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 complete your annual security awareness training.

BACK

Making a Difference in IT

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. Primary Account Numbers should only 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 or VPN 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. Complete annual security awareness training.

BACK

Making a Difference in 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 the Information Security Policies.
3. Ensure that new employees complete the PCI awareness training.
4. Ensure that new employees are informed of MCCS Acceptable Use Policies for IT equipment and customer information.
5. Ensure that new employees attend training including how to change their passwords and how to use and protect customer data.
6. Ensure that managers provide new employees with systems access appropriate to their job responsibilities. (business need to know)
7. Inform IT in a timely manner about employee terminations so their user IDs, network and systems access privileges may be removed.
8. Execute periodic security awareness communication programs such as emails, notices, posters, etc.

BACK

Making a Difference in Finance\Purchasing

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 a Primary Account Number 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 user accounts or passwords.
8. Never send PANs via email or in any other unsecured manner.
9. Complete annual security awareness training.

BACK

Making a Difference in Legal, 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 cardholder data have appropriate PCI and security language.
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.
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. Complete annual security awareness training.

BACK

Making a Difference in 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 should only be accessible 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. Complete annual security awareness training.

BACK