Payment Card Update Training & Awareness

Nov 12 2019
Nov 21 2019

AGENDA

1. Committee Introduction (Lou)
2. Housekeeping (Saad)
3. Chargebacks & Changes (Saad)
4. Mosaic Deposits (Dianna)
5. PCI Training and Awareness (Paul)

PCI STEERING COMMITTEE

- Dee Henne (co-chair), AVP Admin & CFO
- Gayleen Gray (co-chair), AVP & CTO
- Nancy Gray, Executive Director, Strategic Projects, FA
- Lou Mitton, Controller, FA
- Richard Godsmark, Director, Technology, UTS
- Steven Barei, Information Systems Manager, Housing & Conference Services
- Tracy Mestdagh, Interim Director of IT, Faculty of Health Sciences
- Karen McQuigge, Director, Alumni Advancement, UA
- Dianna Creamer, Manager, Student Accounts and Cashiers
- Elizabeth Zelek, Manager, Financial Affairs Business Office
- Wendy Brunner, Manager, Finance and Administration, CCE
- Tawnya Smith, Chief Internal Auditor (ex-officio)
- Paul Muir, Information Security Officer, UTS
- Saad Khan, Manager Financial Reporting, Financial Affairs

HOUSEKEEPING

- Sign-in Sheet
- Presentations available on PCI website: **https://financial-affairs.mcmaster.ca/app/uploads/2018/07/Policy-for-the-Acceptance-of-Payment-Cards-and-E-Commerce-Payments-October-2019.pdf**
- Reminder to advise of staff turnover (Mosaic and Moneris IDs) - Attestation discussed later.
- Ensure all staff involved in payment processing for your area are aware of policies and that the training is available on PCI-DSS website
- Cashiers training

MERCHANT ATTESTATION

PCI-DSS Compliance Steering Committee requires all Moneris Merchants and PayPal accounts to confirm their Compliance with Payment Card and Ecommerce Policies.

Timelines:

Request to attest:	Nov 11, 2019
Deadline to respond:	Dec 6, 2019
Response shared with merchants:	Dec 20, 2019
Results shared with PCI-DSS Committee:	Jan 16, 2020

Details of Attestation

Gather and/or update information

- Merchant name and number
- Name and email address of:
  - Day-to-day contact person
  - Signing Authority
  - Ultimate responsible person
- Chartfield for revenues and fees
- Store ID
- Frequency of reconciliation between Moneris/PayPal and Mosaic
- URL for eCommerce merchants
- Feedbacks

Confirmations to comply with PCI-DSS

- physical or logical changes to procedures or technology
- collection and destruction of card information
- Number of people involved with Payment processing
- Their (above) names and recent training dates
- Number of POI devices with locations
- For hosted pay page, confirm if the merchant has:
  - Data Preload
  - CVV and AVS requirement
  - logging for each transaction, including transaction timestamp, customer session ID and customer IP address
  - Any other security controls

GROWTH OF CARD SALES AT MCMASTER

Fiscal years	Merchants	Sales $
2013	53	27.7 million
2014	54	31.5 million
2015	59	33.9 million
2016	64	64.3 million
2017	64	83.7 million
2018	64	86.9 million
2019	66	88.4 million

The above stats cover Moneris merchants only, however PCI Committee covers other payment processors.

CHARGEBACKS

- Timelines – **Merchant gets a maximum of 10 days to respond (PayPal 20 days)**
- Cost – **$15 per chargeback (PayPal $20)**
- Chargebacks in past two years

	Fiscal '18/19		Fiscal '17/18	
	$	#	$	#
Adjustment reversal	1,136.15	4	6,311.53	15
Declined	879.00	5	2,297.00	7
Closed – not disputed	22,757.70	10	18,500.08	12
Total	24,772.81	19	27,108.61	34

Moneris Login and Merchant Direct Reports
https://www.moneris.com/

Mosaic Deposits

NON STUDENT DEPOSITS – **TIPS**

Moneris deposits in MonAmex

- Complete Moneris deposits by 1:00pm on the 2nd business day of the month.
- Do not change any information in the uploaded Moneris deposits. It is an automated bank account and any alteration decreases the performance of auto reconciliation.
- Information on process Moneris deposit: Mosaic Home, Support and Documentation, How to Guides, Cash Receipts – Direct journal Documentation

MacBill Moneris Card payments

Information on process Moneris deposit:

- Mosaic Home
- Support and Documentation
- How to Guides
- MACBILL-Accounts Receivable Documentation

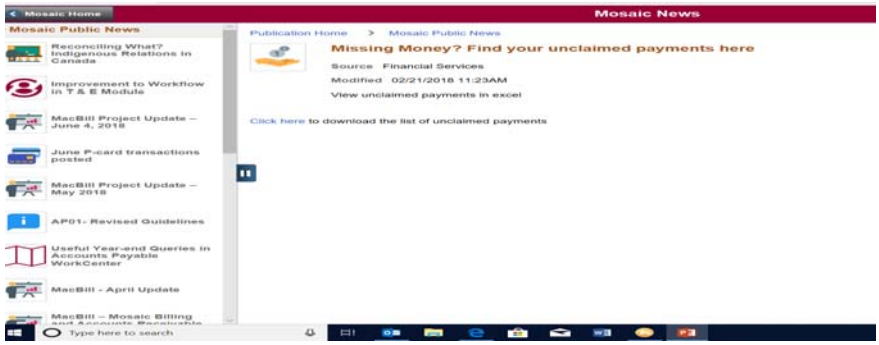
Other Deposits – **TIPS**

Cash, cheque, wire & EFT deposits in the CDN and US accounts:

MR3

Missing payments – UNCLAIMED PAYMENTS

Mosaic, Mosaic News, Missing Money? Find your unclaimed payments here



STUDENT DEPOSITS – **TIPS**

- To reconcile Campus Solutions Moneris transactions daily:
  - Three way daily balancing reconciliation
    - From Moneris daily transactions to departmental CS/SFA, in purpose of finding any student transactions that are paid but not post to mosaic
    - From CS/SFA to Moneris, in purpose of finding any student CS entries that are not balanced to Moneris or not balanced to your department Receivable chartfield.
    - From Moneris to the bank to ensure all moneris payments are deposited that are recorded in CS/SFA
- Reconciliation Tool: Mosaic>Campus Solutions>Student Financials>Charges and Payments>Electronic transactions>Electronic payments>Moneris Reconciliation

McMaster University

PCI Training and Awareness

McMaster University

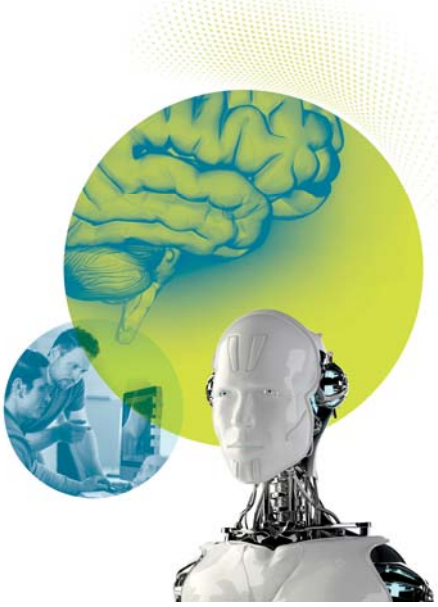
Payment Card (PCI)

Training & Awareness

2019 Annual Training

PCI Training & Awareness

Contents



Payment Card Risk

What is the risk of accepting credit cards?

At what cost?

Compliance

- McMaster is required to demonstrate compliance to the PCI Data Security Standard (PCI-DSS).
- Penalties for non-compliance may include increased processing fees – affecting all merchants.

Fraud

- Fraudulent activity may result in financial loss, reputational damage and a disruption to normal business activities.

Breach

- A compromise to the computers and systems that are used by McMaster merchants to process credit card payments may result in financial loss, financial penalties, reputational damage and a disruption to normal business activities.

Compliance

The Policy for Acceptance of Payment Cards and Non-Cash Payments

- Recent updates related to e-commerce processing
- ***No electronic cardholder data storage

PCI-DSS self assessment questionnaire v3.2.1

- Current version makes multi-factor authentication a requirement for non
- McMaster University responsible for six (6) device type SAQs

E-commerce (2 types)

- Web based merchants using hosted pay page or hosted tokenization

Point-of-Purchase (2 types)

- Face-to-face transactions using handheld devices
- May be integrated to a Point-of-Sale system

Virtual Terminals (2 types)

- Purpose built systems for processing card not present (CNP) transactions
- Specialized single purpose hardware/software solutions.

E-commerce

Risks of accepting online payments

Compliance

- Merchants using the e-commerce site to enter in credit card information on behalf of end-users.
  - Merchant is responsible for correctly separating e-commerce and virtual terminal functionality. This may mean a dedicated system is required!

Fraud

- Card Validation and Distributed Guessing attacks against the merchant's hosted pay page.
  - Merchant is responsible for ensuring that the e-select account is properly configured in compliance with The Policy for Acceptance of Payment Cards and Non-Cash Payments. This includes session logging requirements, Data Preload, CVV and AVS.

Breach

- E-commerce site that are vulnerable to attack due to unpatched servers or poorly coded websites.
  - Merchant is responsible for ensuring the website and supporting software are up to date and configured securely.

McMaster University

Virtual Terminals

Risks associated with manually entered transactions

Compliance

- Merchant manually enters CNP transactions using the same computer that is used for email and web surfing
  - Emerging Risk: Windows 7 end-of-life! January 14, 2020. Upgrade you C-VT's as soon as possible.

Breach

- Merchant manually enters CNP transactions on a computer that is running software that is not up to date, does not have appropriate security software, is not configured securely, and/or has malicious software installed.
  - Use a hand-held merchant terminal for CNP payment processing. This will transfer the majority of PCI-DSS compliance responsibility to the Moneris – recommended!
  - Merchant is responsible for correctly separating day-to-day business activities and virtual terminal functionality. This may mean a dedicated system is required!

McMaster University

Windows 7 End-of-Support

Emerging risk for merchants who use Virtual Terminal

- Windows 7 Operating system reaches End-Of Support on January 14, 2020
- All Virtual Terminals using Windows 7 will be out of compliance January 15, 2020
- Options:
  - ❖ Decommission: for merchants who no longer process phone or mail-in orders.
  - ❖ Replace with Handheld: for merchants for whom the volume of phone or mail-in orders is low.
  - ❖ Upgrade: for merchants whose virtual terminal hardware is relatively newer.
  - ❖ Replace: for merchants with aging virtual terminal hardware.

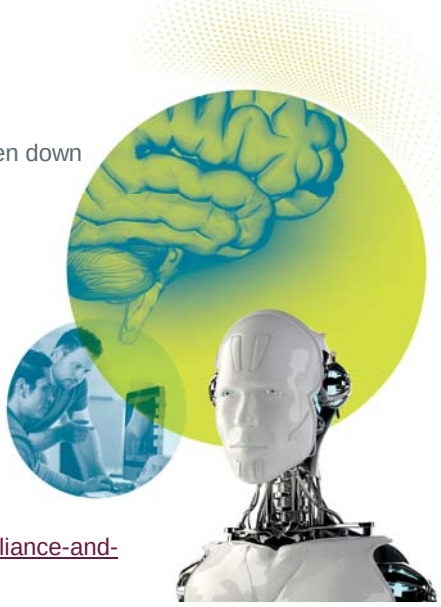
Action MUST be taken before January 14, 2020. Please contact IT Security for support.

McMaster University

Fraud Prevention

The basics of fraud prevention can be broken down into two sections:

- Card-Present (face-to-face)
- Card-Not-Present (Mail order/telephone/Internet)



Resources

https://www.moneris.com/en/Support/Compliance-and-Security/Protecting-Against-Fraud

McMaster University

Fraud Prevention
Card-Present (face-to-face)

The 3 C's of Card-Present Fraud Prevention

- **Customer behaviour:** Keep an eye on customers who appear nervous or are making an unusual purchase from your business (such as several high-priced electronic items at a convenience store).
- **Card Entry & Handling:** If customers have Chip & PIN on their card, be aware of the number of times they are attempting to enter their PIN or re-inserting their card to try again. If they do not have Chip & PIN on their card, be sure to validate the date, hologram, security code, and signature panel on their credit cards.
- **Card Acceptance:** Always follow proper card acceptance procedures and use the secure Chip & PIN method whenever possible. For manual transactions, always take an imprint of the card.

Fraud Prevention
Card-Not-Present (Mail order/telephone/Internet)

The 3 E's of Card-Not-Present Fraud Prevention:

- **Expensive**: Take notice of purchases that include high-priced items or large quantities of the same item.
- **Express**: Be wary of customers who request express, next-day delivery.
- **Extra cards**: Watch for customers who make purchases using multiple credit cards.

McMaster example

Person places order online for an event and then contacts you, either by phone or email, to cancel their attendance; and then asks for refund to different payment card… big warning flag!

Reference: Twelve Potential Signs of Card Not Present (CNP) Fraud Guide

Other Considerations

There are two additional aspects that need to be considered with respect to credit card processing security:

- Device security; physical security of handheld.
- Proper Handling of credit card information.

McMaster University

Other Considerations

Device Security

Are physical and/or logical controls in place to restrict access?

- Hand held devices that capture payment card data via direct physical interaction with the cardholder are protected against tampering and substitution? Stickers? Tethers? Secure location?
- Devices are periodically inspected to look for tampering or substitution. Daily or at least weekly.
- Merchant is responsible the installation and use of tethers.

Be aware of suspicious behavior and report tampering or substitution of devices

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
  - Reference: PCI Protecting the POS – Merchant Best Practices
  - Reference: Merchant Best Practice to Prevent Skimming
  - Use Moneris checklists as a guide.

McMaster University

Other Considerations
Proper Handling

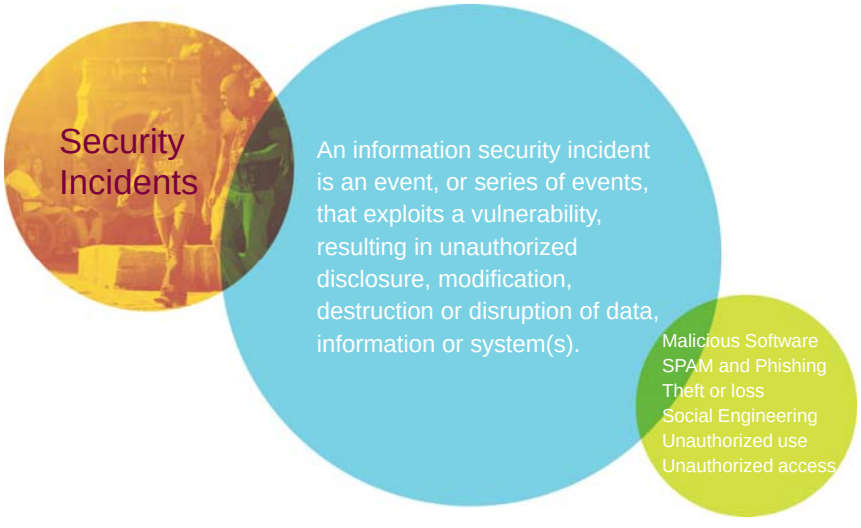
Don't store Credit Card (CC) information if not necessary

- The CC# masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full CC#.
- Hardcopy materials no longer required are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. Use Confidential Waster bins.
- All media that is kept is physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

Restrict access to cardholder data by business need to know

- Access to system components and cardholder data limited to only those individuals whose jobs require such access.
- Access is restricted to least privileges necessary to perform job responsibilities.

Remember - No sending CC information over email or USB....!



Security Incidents
Incident Identification

When is it a payment card, or PCI incident?

Any breach or compromise that **potentially** exposes payment card data to unauthorized individuals.

Payment card data includes:

- credit cardholder name, account number and expiry date
- credit card verification or CVV code
- credit card Personal Identification Number (PIN)
- information that is stored on the magnetic stripe
- the card itself

Security Incidents
Payment Card Incidents

Examples:

- Skimming: theft of credit card information.
  - Theft or loss, unauthorized access to credit card information
- Malware: infections on payment card computers.
  - Unauthorized access to credit card information
- SPAM and Phishing: change your online banking password now!
  - Social engineering
- Card not present (CNP): e-commerce.
  - Unauthorized use of credit card information, social engineering
- Hacking: data breach on a payment card system.
  - Unauthorized access to credit card information

Security Incidents
Incident Reporting

Upon detection of a payment card related security incident, merchants and/or staff are instructed to:

DO NOT logoff or power off the affected system.

DO remove the affected system from the network.

DO take note of pertinent information, including:

- the time that the *suspected* incident occurred
- the condition of the affected system
- your merchant number

REPORT the incident using the following guidelines….

Security Incidents
Incident Reporting

If the incident involves a suspected act of tampering with a payment card device, report the incident directly to IT Security:

IT Security: c-it-security@mcmaster.ca
OR (905) 525-9140 x28299

If the incident involves a known act of tampering with a payment card device, report the incident directly to Moneris:

Moneris: 1-866-802-2637 OR 1-866 319-7450

Then report the incident to IT Security:

IT Security: c-it-security@mcmaster.ca
OR (905) 525-9140 x28299

Security Incidents
Incident Reporting

If the incident involves a *physical* threat, including theft or tampering with a POS device, then report this immediately to:

McMaster Security Services:
905-525-9140 ext 24281, or 905-522-4135
Dial "88" from any University phone

Then report incident to Moneris:

Moneris: 1-866-802-2637 OR 1-866 319-7450

Then report incident to IT Security:

IT Security team: c-it-security@mcmaster.ca
OR (905) 525-9140 x28299

University Security
Incident Reporting

The purpose of having University update is to minimize communication gaps between merchants and University Security when a suspected fraud is escalated to University Security. When the incident is escalated to University Security, they issue an incident number. It is recommended that follow ups on investigations should be sent to Joseph Zubek, Senior Manager, Security and Parking Services with the incident number.

Functions:
- Investigate reported cases of known Fraud
- Investigate reported cases of suspected Fraud
- Interview witnesses and record statements
- Collect evidence for Forensic examination to support criminal charges
- Prepare necessary paperwork to submit to the Courts
- Liaise with Hamilton Police Major Fraud Unit when appropriate

IT Security Best Practices

- Enable automatic updates – OS, application, browser, plugins, etc.
- Ensure Anti-virus installed and updated
- Ensure computer firewall turned on
- Treat all incoming messages with suspicion…
- Remember that websites can be bad too!

For guidance on best practices please visit us at: https://informationsecurity.mcmaster.ca/

And make sure you follow us on Twitter - https://twitter.com/McMaster_ITSec

McMaster University

Merchant Responsibilities

General

- Complete the annual attestation of compliance.
- Maintain a training log for all staff that are involved in payment processing.
- Plan for the appropriate resources to ensure compliance.

E-commerce

- Scan your website and server often. Contact IT Security for details.
- Implement session logging, Data Preload, CVV and AVS validation for all transactions.

Point of Purchase

- Merchant is responsible the installation and use of tethers.

Virtual Terminals

- Emerging Risk: Windows 7 end-of-life! January 14, 2020. Upgrade you C-VT's as soon as possible.

Talk to IT Security or Finance representatives if unsure about something. We are here to help!

McMaster University

Resources

McMaster policy and procedure documents
http://www.mcmaster.ca/bms/BMS_FS_Payment_Card.htm

Moneris Login and Merchant Direct Reports
https://www.moneris.com/

Moneris Fraud Prevention Guidance
https://www.moneris.com/support/compliance-and-security/protecting-against-fraud

Reporting to IT Security
https://informationsecurity.mcmaster.ca/topic/information-security-incident-identification-and-reporting/