Payment Card (PCI) Update
Training & Awareness

2017/2018

AGENDA

1. Committee Introduction (Nancy)
2. Housekeeping (Diana)
3. Mosaic Deposits (Lynne/Saad)
4. Chargebacks & Changes (Diana)
5. PCI Training and Awareness (Richard/Paul)
PCI STEERING COMMITTEE

- Dee Henne (co-chair), AVP Admin & CFO
- John Kearney (co-chair), CIO
- Nancy Gray, Director of Finance
- Richard Godsmark, Director, Technology (UTS)
- Marta Prancho, Systems Analyst (Housing)
- Rocco Piro, Director of IT, FHS
- Karen McQuigge, Director, Alumni Advancement
- Lynne Bennett, Manager, Student Accounts and Cashiers
- Wendy Brunner, Manager Finance and Administration (CCE)
- Elizabeth Zelek, Manager, Financial Affairs Business Office
- Tawnya Smith, Internal Auditor (ex – officio)
- Paul Muir, UTS Information Security Officer (ex-Officio)
- Diana Parker, Project Manager, Ofc Vice-President (Administration)

HOUSEKEEPING

- Sign-in Sheet
- Presentations available on PCI website
- Reminder to advise of staff turnover (unique Moneris and Mosaic IDs)
- Ensure all staff involved in payment processing for your area are aware of policies and training available
  
  [http://www.mcmaster.ca/bms/BMS_FS_Payment_Card.htm](http://www.mcmaster.ca/bms/BMS_FS_Payment_Card.htm)
### Growth of PCI at McMaster

<table>
<thead>
<tr>
<th>Growth in Merchants</th>
<th>Growth in Sales $</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011 70 Merchants</td>
<td>Fiscal 2013 $19.7 million</td>
</tr>
<tr>
<td>2012 80 Merchants</td>
<td>Fiscal 2014 $23.4 million</td>
</tr>
<tr>
<td>2014 85 Merchants</td>
<td>Fiscal 2015 $32.5 million</td>
</tr>
<tr>
<td><strong>2017 56 Merchants</strong></td>
<td><strong>Fiscal 2016 $64.3 million</strong></td>
</tr>
<tr>
<td></td>
<td>Fiscal 2017 $ ?</td>
</tr>
</tbody>
</table>

### Bank Reconciliation

- Disbursement accounts
- Deposit accounts
MONTH-END
YEAR-END PROCEDURE:

Cash and cheques physically received in the new month MUST be posted to the current month – it is not appropriate to enter the deposit for the previous month (even if it’s open) – the amount should be set up as an Accounts Receivable instead

NON-STUDENT DEPOSITS - TIPS

Cash & cheque deposits in the CDN and US accounts:
• Only use appropriate bank for USD currency transactions
• Deposit slips should contain a summary of deposits entered with the same accounting date. That accounting date should also be entered on the deposit slip.
• If possible, use multiple payment option instead of individual deposit entry.
• The physical deposit should be delivered to SAC soon after creating the actual deposit entry in PeopleSoft.
• One Business Unit per one deposit slip.
• If the amount of the posted deposit is correct and there is a need to correct just the accounting part (chartfield string) in a Direct Journal, it should be done through GL JE.
• With Direct Journals, use the description line to document details of the deposit
**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.

---

**STUDENT DEPOSITS - TIPS**

- Payments: When users find that a quick post is missing a student deposit they usually create or request SAC to create a manual entry:
  - In the line description please add MHP references and transaction dates
- Refunds: For both quick and manual posts when the users find the need to refund, they usually create or request SAC to create a manual refund:
  - In the line description please add MHP references and transaction dates
**CHARGEBACKS**

- Timelines and Merchant responsibilities
- Cost of chargebacks
- How to reduce chargebacks

Moneris Login and Merchant Direct Reports
[https://www.moneris.com/](https://www.moneris.com/)

---

**Reducing Chargebacks**

- 1. Use a clear payment descriptor
- 2. Have clear policies (no refunds, etc)
- 3. Get it in writing (require acknowledgement)
- 4. Deal with customer service promptly
- 5. Keep good records
- 6. Learn to spot warning signs of fraud
- 7. Train employees
- 8. Fight back when it makes sense.
CHANGES TO CHARGEBACKS

• MasterCard introducing new Standards (effective October 2017)
• Visa chargebacks now split in two streams
  • Authorization or Fraud disputes
  • Consumer disputes
• Impact? – Shortened Time to Respond!
  - but for some, fewer to require responses

CHANGES TO MASTERCARD – PREAUTHORIZED TRANSACTIONS

• Changes to MasterCard standards.
  • (effective May 2017)
• IF you use pre-Authorization to put a hold, the transaction must be completed or reversed within 30 days; otherwise penalty fees will apply to the Merchant.
• Additional penalties apply if the settlement amt differs from the authorized amount.
PCI TRAINING & AWARENESS

• Payment Card Risk 12
  o Risks & Remediation 13
  o Risks for e-commerce 14
  o Remediation for e-commerce 15
  o Risks for Virtual Terminals 16
  o Remediation for Virtual Terminals 17

• Fraud Prevention 18
  o Face-to-face Transactions 19
  o Mail Order/Telephone Order and Internet Fraud 20

• Other Considerations 21
  o Device Security 22
  o Proper Handling 23

CONTENTS – CONT.

• Security Incidents 24
  o Incident Identification 25
  o Payment Card Incidents 26
  o Incident Reporting 27
  o Security Incident Reporting 29

• IT Security Best Practices 30

• Merchant Responsibilities 31

• Resources 32
**PAYMENT CARD RISK**

What is the risk of accepting credit cards?

If not handled well or if a incident occurs:

- Reputational – broken trust
- Financial – penalties & fines
- Business disruption

*Can be significant, given the event!

Example – Target POS breach, 2014

Between Nov. 27 and Dec. 15, 2013, attackers used malware installed on POS systems to steal data on about 40 million debit and credit cards in the U.S., Brazil and Russia – wow!

Result – CIO and CEO resigned, financial damage pending...

---

**RISKS & REMEDIATION**

The two most significant payment card risks for McMaster University are poorly or improperly implemented/maintained e-commerce and virtual terminal solutions.

**E-commerce** are the websites constructed to use the Moneris Hosted Pay-Page so that all transactions are entered by the end-user and the transactions are handled by Moneris.

**Virtual terminals** are web-browser based access to Moneris to authorize payment card transactions, where the merchant (McMaster) manually enters payment card data via a securely connected web browser. This is typically the Moneris eSelect Plus web portal.
Risks for e-commerce are:

1. Merchants (you) using the e-commerce site to enter in credit card information on behalf of end-users. The combination of e-commerce and virtual terminal functionality results in non-compliance!

2. Improper or unsecure coding of new e-commerce sites providing avenues for attack (your developers).

3. New vulnerabilities arising on existing systems resulting in new opportunities for attack.

Remediation for e-commerce sites:

- Merchant (you) correctly separating e-commerce and virtual terminal functionality. This may mean a dedicated system is required! Or could mean a change in business process.

- New sites undergo rigorous security testing by IT Security before being allowed to start accepting credit cards and are then scanned on a weekly basis to monitor potential vulnerabilities and provide an assessment of compliance.

- Merchants are responsible to ensure that their site/s are kept up to date with latest patches and security fixes.
Risks for Virtual Terminals:

1. Merchant (you) uses the same system for email and web surfing for virtual terminal and the system becomes compromised by malware enabling the collection of payment card information by unauthorized individuals.

2. Anti-virus and patching is not performed on a regular basis opening vulnerabilities on the system for potential exploitation.

3. Merchant installs software which happens to be malware, on a virtual terminal system; enabling the system to be compromised.

Remediation for Virtual Terminals:

Two options available:

1. Convert to a hand held merchant terminal; which in turn converts the majority of the responsibility for PCI to Moneris — recommended!

2. Use a dedicated terminal which is locked down appropriately, limits installation of software, has anti-virus installed, is patched automatically and has its logs monitored for unauthorized access.

IT Security can provide the software and also assist with the configuration of the system to achieve a dedicated and secure virtual terminal solution. Merchant supplies the computer system and is responsible to replace when required.
The basics of fraud prevention can be broken down into two sections:

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

The following slides are R&Ded from the Moneris “Easy Tips for Fraud Prevention” @
http://insights.moneris.com/h/i/71440923-easy-tips-for-fraud-prevention

---

**CARD-PRESENT**

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.
CARD-NOT-PRESENT
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…

OTHER CONSIDERATIONS

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

- Device security; physical security of handheld.
- Proper Handling of credit card information.
**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 card are protected against tampering and substitution? Stickers? Tethers? Secure location? Merchant is responsible for ensuring the installation and use of tethers.
- Devices are periodically inspected to look for tampering or substitution. Daily or at least weekly.

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).

**PROPER HANDLING**

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

- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after processing.
- 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 Waste 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

An information security incident is an event, or series of events, that exploits a vulnerability, resulting in unauthorized disclosure, modification, destruction or disruption of data, information or system(s).

Some examples of information security incidents are:

- Malicious Software
- SPAM and Phishing
- Theft or loss
- Social Engineering
- Unauthorized use of computer accounts
- Unauthorized access to computer systems

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
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

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 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 INCIDENT REPORTING

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

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

If the incident involves a *known* act of fraud, or 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](mailto:c-it-security@mcmaster.ca)
OR (905) 525-9140 x28299

---

SECURITY 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](mailto:c-it-security@mcmaster.ca)
OR (905) 525-9140 x28299
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:
http://www.mcmaster.ca/uts/security/ITsecurity/index.html

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

MERCHANT RESPONSIBILITIES

- Ensure all staff that perform payment processing are aware of the polices, procedures and this training material. Also ensure that all staff have reviewed the Moneris Fraud Prevention Reference also provided.

- Review and update Payment Processing Authorized Access Record and provide to Finance. Lists staff who have access to what in relation to payment cards processing.

- Implement Action Plan, if required, in conjunction with appropriate resources to ensure compliance, as identified for Virtual Terminal requirement, tethers, etc.
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 Easy Tips for Fraud Prevention
http://insights.moneris.com/h/i/71440923-easy-tips-for-fraud-prevention

Moneris Fraud Prevention Guidance

Reporting to IT Security