Payment Card Update Training & Awareness

Nov 13 2018
Nov 15 2018

AGENDA

1. Committee Introduction (Nancy)
2. Housekeeping (Saad)
3. Chargebacks & Changes (Saad)
4. Mosaic Deposits (Dianna)
5. PCI Training and Awareness (Richard/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
- Laurie Ham, Manager, Conference and Event services
- Rocco Piro, Director of IT, Faculty of Health Sciences
- Jeff Chuchman, Associate Director, Advancement Services, 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
- 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
MERCHANT ATTESTATION

The PCI-DSS Compliance Steering Committee has requested that all merchant signing authorities complete an annual attestation. All Moneris Merchants and PayPal accounts will confirm the following:

1. Compliance with the Policy

2. That the account details associated to the Moneris merchants and/or PayPal accounts are up-to-date.

GROWTH OF CARD SALES AT MCMASTER

<table>
<thead>
<tr>
<th>Fiscal years</th>
<th>Merchants</th>
<th>Sales $</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>51</td>
<td>27.0 million</td>
</tr>
<tr>
<td>2013</td>
<td>53</td>
<td>27.7 million</td>
</tr>
<tr>
<td>2014</td>
<td>54</td>
<td>31.5 million</td>
</tr>
<tr>
<td>2015</td>
<td>59</td>
<td>33.9 million</td>
</tr>
<tr>
<td>2016</td>
<td>64</td>
<td>64.3 million</td>
</tr>
<tr>
<td>2017</td>
<td>64</td>
<td>83.7 million</td>
</tr>
<tr>
<td>2018</td>
<td>64</td>
<td>86.9 million</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th></th>
<th>Fiscal ’17/18</th>
<th>Fiscal ’16/17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjustment reversal</td>
<td>6,311.53</td>
<td>8,480.60</td>
</tr>
<tr>
<td>Declined</td>
<td>2,297.00</td>
<td>3,365.68</td>
</tr>
<tr>
<td>Closed – not disputed</td>
<td>18,500.08</td>
<td>5,446.02</td>
</tr>
<tr>
<td>Total</td>
<td>27,108.61</td>
<td>17,292.30</td>
</tr>
</tbody>
</table>

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

## Mosaic Deposits
STUDENT DEPOSITS – TIPS

To reconcile Campus Solutions Moneris transactions daily:

- Two-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.

- Reconciliation Tool:
  - Mosaic>Campus Solutions>Student Financials>Charges and Payments>Electronic transactions>Electronic payments>Moneris Reconciliation

Steps to balance Moneris transactions to Campus:

- Complete the App Engine query run control by filling out the prompts, open the results in an excel format.

<table>
<thead>
<tr>
<th>Prompt Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIRECTIONALITY</td>
<td></td>
</tr>
<tr>
<td>MONEXTRACTED</td>
<td>27/06/19</td>
</tr>
</tbody>
</table>

  Fill out Moneris transaction date here

- To check daily suspended item:
  - Add filter and check column AX for suspended items
  - Example: June 19th has one suspended item "IN MONERIS NOT IN MOSAIC $7,083.99 with unique transaction identifier mhp18169153151p35 for Student ID#400151171

- If there is an exception, investigate the issue and proceed accordingly

- Please do not hesitate to contact Student Account & Cashiers or Financial Service if you have specific reconciliation inquiry
MR2  App Engine will be ready by November 2018 so we need to get a path to Mosaic. - S.Khan
M. Rana, 2018-07-11
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

Other Deposits – TIPS

Cash, cheque, wire & EFT deposits in the CDN and US accounts:
Missing payments – UNCLAIMED PAYMENTS
Mosaic, Mosaic News, Missing Money? Find your unclaimed payments here
MR3 I want to replace this slide with MacBill. - S.KHAN
M. Rana, 2018-07-11
MacBill Moneris Card payments

Information on process Moneris deposit:
• Mosaic Home
• Support and Documentation
• How to Guides
• MACBILL-Accounts Receivable Documentation

Timeline

Phase I – Go live – May 31, 2018
Phase II – Planned – Fall 2018
Phase III – Planned – Winter 2019
McMaster Corporate Visa and MasterCard Payments:

**Step 1:**
https://www.mcmaster.ca/bms/index.htm

**Step 2:**
https://www.mcmaster.ca/bms/BMS_Pay_McMaster.htm
McMaster Corporate Visa and MasterCard Payments:

Step 3:

https://mosaic.mcmaster.ca/pisp/prepprd /EMPLOYEE/ERP$WEBIB_MONERIS.ISC RIPT1.FieldFormula.IScript_Moneris

PCI Training and Awareness
PCI Training & Awareness

Contents

- Payment Card Risk 22
  - Risks & Remediation 23
  - e-commerce 24
  - Virtual Terminals (VT) 26

- Fraud Prevention 28
  - Face-to-face transactions 29
  - Mail Order / Telephone and Internet fraud 30

- Other Considerations 31
  - Device Security 32
  - Proper Handling 33
PCI Training & Awareness
Contents - continued

- Security Incidents 34
  - Incident Identification 35
  - Payment Card Incidents 36
  - Incident Reporting 37
- IT Security Best Practices 41
- Merchant Responsibilities 42
- Resources 43

Payment Card Risk
What is the risk of accepting credit cards?

If not handled well, or if an incident occurs:.
- Reputational – broken trust.
- Financial – penalties & fines.
- Business disruption

Can be significant; given the event!
Example – Target POS breach, 2013
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!

Target Settles 2013 Hacked Customer Data Breach For $18.5 Million
The two most significant payment card risks for McMaster University are poorly or improperly implemented/maintained e-commerce and virtual terminal solutions.

**E-commerce**

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**

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.

---

**e-commerce**

Risks of accepting online payments

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.
**e-commerce**
Remediation steps for payment accepting websites

1. 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. If you are unsure, ask your friendly IT Security team.

2. New sites must 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. Any significant changes to the site must also be checked and so please contact IT Security when major changes have occurred.

3. Merchants are responsible (this means you) to ensure that their site/s are kept up to date with latest patches and security fixes.

---

**Virtual Terminals**
Risks associated with manually entered transactions

1. Merchant (you) uses the same computer system for email and web surfing for manually entered transactions 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 system used for manually entering credit card transactions; enabling the system to be compromised.
**Virtual Terminals**  
Remediation options 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.

---

**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)

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
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!
Other Considerations

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

1. Device security; physical security of handheld.

2. Proper Handling of credit card information.

Other Considerations

Device Security

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

- Handheld 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).
Other Considerations

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
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
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:

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

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
Merchant Responsibilities

- Ensure all staff that perform payment processing are aware of the policies, 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.

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

Open Session:
Questions and Answers
The End