PAYMENT CARD MERCHANT ANNUAL TRAINING

SESSION 1: Tuesday, November 25 2014 MDCL 3023 (9-11)
SESSION 2: Friday, November 28 DSB 505 (9:30-11:30)
OBJECTIVES

• Updates since 2013 training
• Better understand payment card risk
• Better able to identify fraud
• Know proper card handling process
• Know when/who to report an incident
• Understand best practices
1. Welcome (PCI Committee Introduction) – Nancy
2. Housekeeping /Updates – Heidi
3. People Soft Impact – Deposits – Heidi
4. Other Deposit Tips – Heidi
5. SAQ – Questionnaire Changes and Merchant Responsibilities – Richard
6. Risks & Remediation – Richard
7. Fraud Prevention – Richard
8. Incident Identification & Reporting – Richard
10. Fee Changes – Nancy
PCI Steering Committee

Deidre Henne (Co-Chair) – AVP Administration & CFO
John Kearney (Co-Chair) – CIO
Theresa Cooke – Manager, Student Accounts & Cashiers
Nancy Gray – Director, Financial Services
Heidi van Bodegom – Supervisor, Financial Reporting
John McKay – Director, University Advancement Services
Rocco Piro – Director IT, Faculty of Health Sciences
Tawnya Smith – Chief Internal Auditor
Mike Sowerby – IT Manager, Student Affairs
Richard Godsmark – Director IT, University Technology Services
HOUSE KEEPING

1. Sign-in Sheet

2. Presentation Notes

3. Reminder to contact Financial Services upon staff turnover

4. Ensure all staff involved in payment processing for your area are aware of policies/procedures/training

http://www.mcmaster.ca/bms/BMS_FS_Payment_Card.htm
## Updates

- **Growth in Merchants**
  - 2011: 70 Merchants
  - 2012: 80 Merchants
  - 2014: 85 Merchants

- **Interac Online**
  - Fiscal 2012: $19.7 million
  - Fiscal 2013: $23.4 million
  - Fiscal 2014: $32.5 million
Updates — cont.

• Virtual Terminals that have the XP Operating System are required to be upgraded to a supported version as of 8\textsuperscript{th} April 2014 due to Microsoft no longer provide support or updates for XP. IT Security worked with Merchants to upgrade systems to maintain compliance.

• Hand-held terminals need to be upgraded before the end of December 2014 as required by Moneris. Moneris will be working with Merchants to replace units over the next few months.

• The implementation of physical tethers to secure hand-held devices will follow the replacement schedule.
PEOPLESOF# IMPACT – DEPOSITS

• Ensure that you are using the Deposit Entry – Moneris – Quick guide instructions for deposits
• separate deposit entries for Visa, MC, Interac and Amex do not have more than one ID # receipt for each credit card type
• The Payment ID needs to include your 3-digit merchant code followed by the method of payment (002-Visa, 002-MC, 002-Amex and 002-Debit)
• The Accounting Date has to agree with the date of the Moneris transaction and the Control Data dates (Received and Entered dates) should all be the same dates as the Accounting Date
• The deposit and the direct journal should be entered as close to the date of the transaction as possible
Note that the Mosaic team is working on automating Moneris deposits which will eliminate some of the current manual procedures. A communication will be sent out to the community in advance of any changes.
OTHER DEPOSIT TIPS

• Ensure that your control currency matches the CIBC bank code – the control currency default has been USD until recently → it is important that bank 001 is selected for CAD deposits and bank 002 is selected for USD deposits

• Only use bank 001 (CAD) or bank 002 (USD) – if cash or cheques are received in another foreign currency, please contact Student Accounts & Cashiers

• When preparing cash and cheque deposits for the bank, prepare one deposit slip for each accounting date (Note: this should be the date that you are taking the funds to the Cashiers Office) → do not combine multiple accounting dates together especially during month-end close and a new working month

• Do not combine cash/cheque deposits together with multiple business units
OTHER DEPOSIT TIPS – CONT.

- With Direct Journals, use the description line to document details of the deposit.
- The **Accounting Date** should ALWAYS be the date that you are making the deposit to the bank – **Received** and **Entered** dates should all be the same dates as the **Accounting** Date.
- 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.
GOOD NEWS!

Self Assessment Questionnaires in their current form are no longer required to be completed by departments/faculties involved with payment card processing.

A simpler and more business focused questionnaire has been developed and is to be completed by department/faculty after completion of training by all staff handling payment cards.

IT Security with Financial Services will then complete one SAQ representing the entire university for PCI compliance.
more business… less tech talk….

- Login into IPACS [https://ipacs.mcmaster.ca](https://ipacs.mcmaster.ca)
- Select Self Service option and continue
- Click Service Catalog (at top of page)
- Select **PCI-DSS Compliance** from **Category** and then **Payment Card Merchant Questionnaire** from main window.

Sign in after this training session and complete for your area. Remember that all staff handling credit cards must review this training and review the [Fraud Prevention Program Reference Guide](https://ipacs.mcmaster.ca) provided by Moneris.
RISKS & REMEDIATION

What is the risk of accepting credit cards?

If not handled well or if a incident occurs:

- Reputational – broken trust
- Financial – penalties & fines

*Both 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…
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.
Risks for e-commerce are:

1. Merchants 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.

3. New vulnerabilities arising on existing systems resulting in new opportunities for attack.
Remediation for e-commerce sites:

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

- Face-to-face transactions
- Mail order/telephone order and Internet fraud

The following slides are R&Ded from the Moneris “Protecting Against Fraud” website @
FACE-TO-FACE TRANSACTIONS

Key areas of focus:

• Suspicious customer behaviour
  
  Fraud prevention begins with keeping your eyes and ears open.

  Signs of suspicious customer behaviour can include:
  
  o Customer has randomly collected merchandise without the usual care
  o Customer may appear nervous or in a hurry
  o Customer may take the card from their pocket instead of their wallet and the signatures may not match
  o Customer makes large, random, expensive purchases

For more tips see pages 2-3 of Fraud Prevention Program Reference Guide
FACE-TO-FACE — cont.

Key areas of focus:

• Card security features

All cards are designed with special security features to deter counterfeiting and alteration. When you are presented with a card, look for the following elements:

  o On the front:
    • Verify the match of print and embossing
    • Embossing
    • Hologram
    • Valid date
    • Compare account numbers

  o On the back:
    • Signature panel
    • Signature

*Check CHIP!

For more tips see pages 5-7 of Fraud Prevention Program Reference Guide
FACE-TO-FACE – CONT.

Key areas of focus:
• Proper processing procedures
  o Check the card's security features
  o Always insert a chip card into the terminal. Only swipe transactions when the chip is not present.
  o For manual transactions, always get an imprint of the card
  o Compare the signature with the back of the card
  o Keep your card reader in proper working order
  o Use Fraud Detection Equipment – counterfeit detection
  o Use Fraud Prevention Equipment – tether, enclosed cases, security stickers….

For tips see pages 8-14 of Fraud Prevention Program Reference Guide
Key areas of focus:

• Code 10 authorizations

  o Code 10 is a universal code that allows you to alert an authorization department of a suspected fraudulent transaction without alarming the customer.
  o Call for a Code 10 when you think a transaction needs a closer look, or when you believe a fraudulent transaction is occurring.
  o If you are at all suspicious, call Moneris at 1-866-802-2637 and follow the prompts for a Code 10.
MAIL ORDER/TELEPHONE ORDER AND INTERNET FRAUD

There is anonymity buying through the mail, over the telephone or online, but here are the steps you can take to help stop credit card fraud.

Watch for:
- Larger than normal purchases
- Orders of "big ticket" items for resale
- Orders shipped Rush or Overnight for quick sale
- Transactions on similar account numbers
- Orders shipped to a single address but made from multiple 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…
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 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)**: high risk transactions.
  - 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

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

OR (905) 525-9140 x28299
If the incident involves a \textit{physical} threat, including theft or tampering with a POS device, then report this immediately to:

\textbf{McMaster Security Services:}
905-525-9140 ext 24281, or 905-522-4135
Dial “88” from any University phone

Then report incident to Moneris:

\textbf{Moneris: 1-866-802-2637 OR 1-866 319-7450}

Then report incident to IT Security:

\textbf{IT Security team: 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 ACTIONS REQUIRED

- 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.

- Complete online questionnaire attesting that the required training has been completed by appropriate staff.

- Review and Update 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, questionnaire, etc.
FEE CHANGES

• the annual ‘PCI Compliance Levy’ base charge of $750 per e-Commerce merchant and $350 per Point of Sale (POS) or Virtual Terminal merchant will remain unchanged

• the annual % levy will increase to 1.25% of sales – note: there will be no change to the maximum of $10,000

• this fee structure will come into effect on May 1, 2015
QUESTIONS?