Payment Card Merchant Annual Training

Session: April 11th, 2013
Objectives

• Updates since 2012 training
• Understanding PCI Risk
• Fraud prevention training
• Procedures for PCI Incident reporting
AGENDA

1. PCI COMMITTEE
2. HOUSE KEEPING
3. UPDATES
4. SAQ CHANGES
5. RISKS & REMEDIATION
6. MONERIS FRAUD PRESENTATION
7. SECURITY INCIDENT IDENTIFICATION
8. SECURITY INCIDENT REPORTING
9. MERCHANT ACTIONS REQUIRED
PCI STEERING COMMITTEE

Deidre Henne (Co-Chair) – AVP Administration & CFO
John Kearney (Co-Chair) – CIO
Elizabeth Zelek – Acting Manager, Student Accounts & Cashiers
Nancy Gray – Director, Financial Services
Heidi van Bodegom – Acting Supervisor, Financial Reporting
Stacey Farkas – Supervisor, Financial Reporting
John McKay – Director, University Advancement Services
Rocco Piro – Director IT, Faculty of Health Sciences
Tawnya Smith – Senior Manager, Internal Auditor
Mike Sowerby – IT Manager, Student Affairs
Richard Godsmark – UTS Security Officer
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

Survey link - http://www.surveymonkey.com/s/BM7BJFF
UPDATES - VOLUMES

• Growth in Merchants

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchants</td>
<td>65</td>
<td>70</td>
<td>80</td>
</tr>
</tbody>
</table>

Fiscal 2011 $15.6 million
Fiscal 2012 $19.7 million
Fiscal 2013 $23.4 million so far

• Interac Online
UPDATES - MOSAIC

• New PeopleSoft implementation for Financial system scheduled for December 1st
• *New* Billing and Accounts Receivable module
• Payment Card sales transactions will be recorded (in ‘books’) through this module
  o Replaces on-line cashiering
  o Difference between payments received to offset an A/R or Direct sales (i.e. e-commerce)
• Student and Non-Student payments will be handled differently
• Direct upload from Moneris being investigated (eliminate manual intervention)
• Department ‘visits’ to gather information
SAQ CHANGES

GOOD NEWS!

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

A simpler and more business focused PCI audit questionnaire will be developed over the next few months and supplied to each merchant for completion; date to be determined.

IT Security with Financial Services will then complete one SAQ representing the entire university for PCI compliance.
Risks & Remediation

The two most significant PCI risks for McMaster University are poorly or improperly implemented SAQ A and SAQ C-VT solutions; or more commonly known as e-commerce and virtual terminal.

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

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 SAQ A and SAQ C-VT results in a SAQ D classification – or 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

Remediation for e-commerce sites:

- Merchant correctly separating SAQ A and SAQ C-VT 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.

- **NEW!!!** All McMaster based e-commerce sites will be scanned on a weekly basis to monitor potential vulnerabilities and provide an assessment of compliance.
Risks for virtual terminals

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 or 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.

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.
MONERIS FRAUD PREVENTION
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
PCI Security Incident Identification

When is it a 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
EXAMPLES OF PCI SECURITY INCIDENTS

• Skimming: theft of credit card information.
  ➢ Theft or loss, unauthorized access to credit card information

• Malware: infections on PCI 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 PCI system.
  ➢ Unauthorized access to credit card information
SECURITY INCIDENT REPORTING

Upon detection of a PCI related information 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 PCI 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 PCI device, report the incident directly to Moneris.

**Moneris:** 1(866) 319-7450

Report the incident to the IT Security only after it has been reported to Moneris.
SECURITY INCIDENT REPORTING

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

**McMaster Security Services:**

905-525-9140 ext 24281, or 905-522-4135
Dial “88” from any University phone

Report the incident directly to Moneris only after the physical threat has been contained.

**Moneris:** 1(866) 319-7450

Report the incident directly to the IT Security only after it has been reported to Moneris.

**IT Security team:** [c-it-security@mcmaster.ca](mailto:c-it-security@mcmaster.ca)

OR (905) 525-9140 x28299
**Merchant Actions Required**

- Ensure that all staff that handle payment card data review the policies online.
- Add printed materials to your Merchant Binder.
- Review and Update Authorized Access Record.
- Ensure all staff that perform payment processing are aware of the Policy, procedures and this training material.
- Implement Action Plan, if required, in conjunction with appropriate resources to ensure compliance, as identified for C-VT requirement.
QUESTIONS?