

Payment Card Update Training & Awareness

Nov 2023





McMaster University recognizes and acknowledges that it is located on the traditional territories of the Mississauga and Haudenosaunee nations, and within the lands protected by the “Dish With One Spoon” wampum agreement.



Agenda



- | | |
|-------------------------------|--------|
| 1. Committee Introduction | Saad |
| 2. Announcements | Saad |
| 3. Chargebacks & Charges | Saad |
| 4. Mosaic Deposits | Dianna |
| 5. PCI Training and Awareness | Greg |

PCI Steering Committee

- Gayleen Gray (co-chair), AVP & CTO
- Lilian Scime (co-chair), Interim CFO
- Lou Mitton, Controller, FA
- Tracy Dallaire, Director Information Security, UTS
- Steven Barei, Information Systems Manager, HCS
- James Dietrich, Project Analyst, CSU
- Alina Vorobeitchik, Manager Advancement Records, UA
- Dianna Creamer, Senior Manager Accounts Receivable, AR - FA
- Herman Poon, Manager Information Systems, HS
- Jon Jones, Assistant Director, Finance and Operations, MCE
- Len Hostin, Senior Manager Internal Audit, AAS (ex-officio)
- Greg Atkinson, Manager of Information Technology, UTS
- Saad Khan, Manager Financial Reporting, A&FR - FA

Announcements



- Attendance
- Ensure all staff involved in payment processing for your area are aware of policies
- Presentations available on PCI website:
<https://financial-affairs.mcmaster.ca/services/banking-ecommerce/pci-dss-overview/>
- Reminder to advise of staff turnover (Mosaic and Moneris IDs)

POS training

- Training video on avenue-to-learn (15 minutes)
- All POS staff must take this training
- How to access POS training



Moneris Checkout

Project completed Security Features

Pay with your digital wallet for faster checkout
or enter details manually



_____ or _____

Cardholder Name

Card Number MMY CW

 CAD Total **\$10.25**

Cancel

- CVV
- AVS
- 3D-Secure 2.0
- Auto Decision by Moneris

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:	Dec 4, 2023
Deadline to respond:	Dec 11, 2023
Response shared with merchants:	Dec 22, 2023
Results shared with PCI-DSS Committee:	Jan 19, 2024

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
- Checkout, confirm if the merchant has:
 - Data Preload (built-in)
 - CVV and Auto decision by Moneris
 - AVS
 - 3DS
 - Any other security controls

GROWTH OF CARD SALES AT MCMASTER



Fiscal years	Merchants	Sales \$
2017	64	83.7 million
2018	64	86.9 million
2019	66	88.4 million
2020	69	92.4 million
2021	66	72.7 million
2022	59	80.8 million
2023	62	88.1 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 '21/22		Fiscal '22/23	
	\$ Value	Count	\$ Value	Count
Adjustment reversal	2,320.02	19	8,906.32	15
Declined	1,556.83	5	8,219.60	10
Closed - not disputed	20,887.11	21	252,762.24	327
Total	24,763.96	45	269,888.16	352

Moneris Login and Merchant Direct Reports

<https://www.moneris.com/>

Chargeback tips:

<https://www.moneris.com/en/insights/posts/product-education/chargeback-101-everything-you-need-to-know>



Helpful resources

- Personal Protection Equipment
<https://financial-affairs.mcmaster.ca/services/banking-ecommerce/pci-dss-overview/#tab-content-procedural-tools>
- “How to” videos and guides
 - Process purchase or refund
 - Void a transaction
 - Pre-authorize a transaction
 - Add recurring transactions
 - Set up devices and many more<https://www.moneris.com/en/Support/Devices/Moneris-Gateway#MRC>

Mosaic Deposits

Accounts Receivable Office Hours

In person service is available every Friday from 10:00 AM to 1:00 PM. Cheque deposits can be left anytime in the drop box outside Gilmour Hall, Room 109 (New AR Office). Cash deposits should be delivered to GH-109 during office hours on Fridays. Cash left in the drop box is done at your own risk. Contact: macpay@mcmaster.ca

Cash Deposits are accepted for retail operations.
All other payments received will be applied to a MacBill Invoice.
The university is a cashless organization.

NON STUDENT DEPOSITS – TIPS

Moneris deposits in MonAmex

- Moneris deposits into Account Receivable are automated
- Information on process Moneris deposit: Mosaic Home, Support and Documentation, How to Guides, Cash Receipts – Direct journal Documentation

MACBILL TRAINING MATERIALS

- Mosaic Work
- Finance Training tile



- Travel and Expenses
- Non-PO Voucher
- MacBill External Billing
- MacBuy Procurement
- Hyperion
- Recycle bin

MACBILL PAYMENT METHODS:

Pay Corporate Account



Online Banking

PAYMENTS FROM
A **CANADIAN** BANK ACCOUNT

Set up Online Banking from
your Canadian financial
institution's website/app.



Credit Card Payment

PAYMENTS BY CREDIT CARD

*If you do not have a Canadian
phone number, please enter
905-525-9140 in the Telephone
field.*

Other Deposits – TIPS

Non MacBill Invoiced payments (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

The screenshot shows the Mosaic News website interface. The top navigation bar includes 'Mosaic Home' and 'Mosaic News'. The main content area features a news article with the following details:

- Publication Home** > **Mosaic Public News**
- Missing Money? Find your unclaimed payments here**
- Source** Financial Services
- Modified** 02/21/2018 11:23AM
- View unclaimed payments in excel**
- [Click here](#) to download the list of unclaimed payments

The left sidebar contains a list of other news items, including 'Reconciling What? Indigenous Relations in Canada', 'Improvement to Workflow in T & E Module', 'MacBill Project Update – June 4, 2018', 'June P-card transactions posted', 'MacBill Project Update – May 2018', 'AP01- Revised Guidelines', 'Useful Year-end Queries in Accounts Payable WorkCenter', 'MacBill - April Update', and 'MacBill – Mosaic Billing and Accounts Receivable'. The Windows taskbar is visible at the bottom of the screenshot.

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](#)

PCI Training and Awareness

Payment Card (PCI)

Training & Awareness

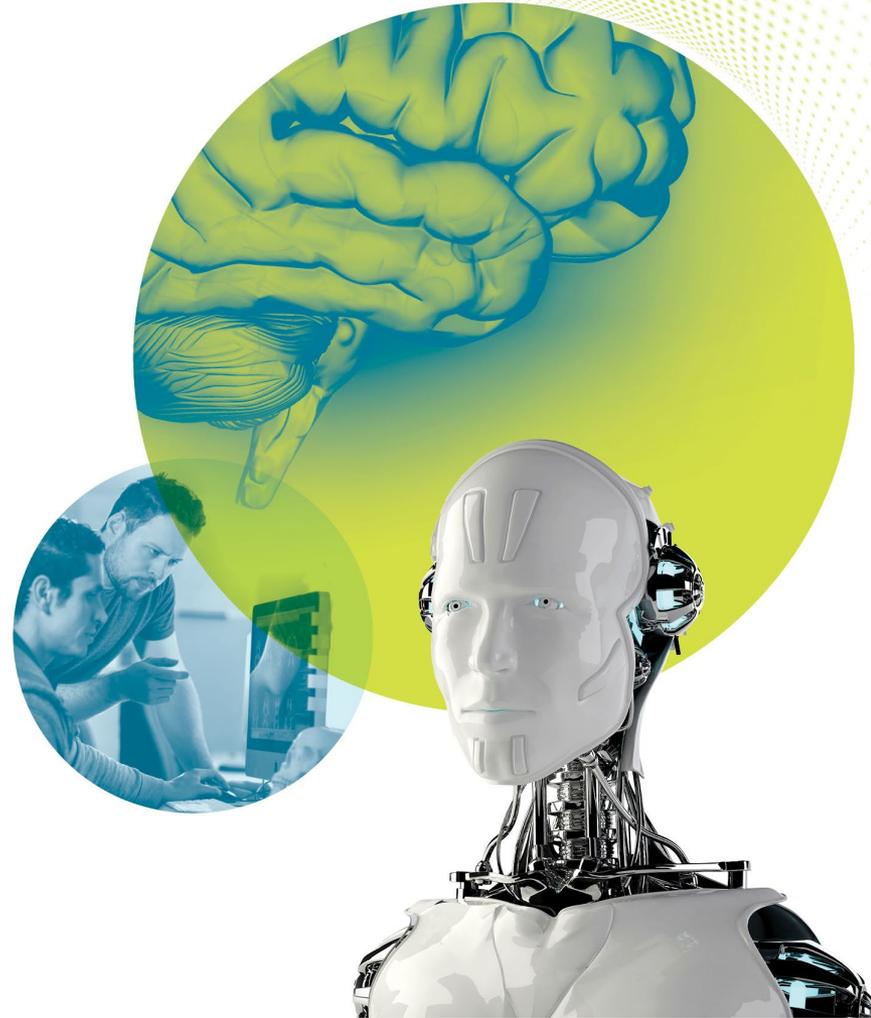
*2019 Annual
Training*



PCI Training & Awareness

Contents

- Payment Card Risk 21
 - Compliance, Ecommerce and Virtual Terminals
- Fraud Prevention 25
 - Card Present and Card not Present transactions
- Other Considerations 28
 - Device Security and Proper Credit card Handling
- Security Incidents 31
 - Incident Identification and reporting
- IT Security Best Practices 38
- Merchant Responsibilities 39
- Resources 40



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, legal action 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 (2023)

PCI-DSS self assessment questionnaire v3.2.1, moving to 4.0 in 2024

- Training on differences is available via A2L

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 & Virtual Terminals

Risks, controls, and additional training

- Introduction a blended approach to PCI-DSS Security Awareness Training:
- Materials for understanding compliance, fraud risk, fraud prevention, incident and breach response, and other considerations are available through McMaster's Information Security Awareness Training in A2L.
- Accompanying Information Security Training is available and recommended.
- Enrollment instructions: **[Information Security Training Program - Information Technology Security \(mcmaster.ca\)](https://informationsecurity.mcmaster.ca/training)** (informationsecurity.mcmaster.ca/training)
- Open drop-in sessions to discuss training materials, ask questions, or provide feedback. Email Atkinson@mcmaster.ca for invitation.
 - Jan 22 2024, 3-4pm
 - Feb 22 2024, 3-4pm
 - March 22 2024, 3-4pm
 - April 22 2024, 3-4pm



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).

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

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.

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

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

- Antivirus software is up to date and running. All files are scanned periodically.
- Setup automatic updates for the best protection and the most convenience.
- Engage System Administrators and IT Staff to ensure that security maintenance roles and responsibilities around e-Commerce systems are covered.
- Maintain vigilance for phishing and train/practice routinely.
- Setup different passwords for every site you access. Use a password manager to help keep them all strong.
- Check your privacy settings on social media and other third party services to make sure you aren't over-sharing, and to know what data 3rd party apps are accessing and how they're using it.
- Download and use the multi-factor authentication app.

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

- Ensure all software is as up-to-date as possible, and that at-risk applications are brought to the attention of system administrators and IT Security.

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

Resources

PCI-DSS Training

<https://informationsecurity.mcmaster.ca/training>

McMaster policy and procedure documents

<https://financial-affairs.mcmaster.ca/resources/>

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/information-security-incidents/>



Q&A