Memo

To: Managers, Supervisors & Staff in York University Card Processing Units

From: Trudy Pound-Curtis, AVP Finance and CFO
         Aldo DiMarcantonio, Comptroller
         Laurie M. Lawson, Treasurer

Date: January 22, 2008

Subject: Payment Card Processing Controls and Compliance

Scope

This applies to all units that accept payments by credit card (Visa and Mastercard), charge card (Amex, PCards), and debit cards (Interac), whether at point-of-sale terminals, integrated retail systems, web-based card-present and card-not-present sites, and eCommerce applications.

Card processing units are referred to as merchants. Merchants have been authorized by Treasury to transact using equipment and web code interfaces provided by card processor firms including Moneris and First Data. Card processor firms act as an intermediary link to the underlying bank-sponsored credit card companies Visa and Mastercard, and to Interac. American Express merchant capability may also be linked to Moneris for card processing.

Card Processing Risks

Supervisors of areas are advised that card processing, like cash handling, involves risks to the University. Fraud is a significant risk and may be attempted by external or internal parties. The Supervisor’s greatest protection to prevent or counter fraud is to systematically and consistently employ controls and compliance checks in their every day unit operations and to work cooperatively with the Finance section to manage allocation and reconciliation processes for revenues.

Due to the ongoing risk of credit card fraud at York University, we are reminding areas of the basic controls and procedures. The most significant risk arises when a unit fails to ensure that a minimum of two persons are involved with the handling, supervision and recording of transactions involving credit and debit cards*. We specifically underscore that a unit’s refund processes require systematic staff supervision, two-person minimum refund approval processes, and ongoing management review of refund volumes and potentially unusual patterns.

* The handling of cash and deposits similarly requires strict processes and controls.
Unit managers should make use of on-line monitoring tools to verify and audit transactions. If your unit is not yet set up to access your merchant activity, via Moneris’ eSelectPlus or Merchant Direct and American Express On-Line Monitoring System (OMS), please contact Treasury to arrange set up with this management tool (see contacts below).

Unit Controls

1. **Processing Transactions and Reconciling Revenues:** There must be a separation of duties among staff processing credit and debit transactions and staff reconciling and recording those activities. In other words, the individual processing credit and debit transactions must be supervised and monitored by another individual whose primary responsibility is the reconciling and recording of transactions. This second individual should not have capabilities to process credit/debit card transactions and should have sufficient training to properly monitor usual credit and debit transactions.

2. **Recording Revenues:** Activity/transactions must be recorded on a timely basis (ideally daily in units with high volume, but as a minimum weekly) and submitted electronically in journal format to General Accounting.

3. **Handling Refunds and Credits:** Each unit is responsible for ensuring that ALL refunds and credits are consistently approved and authorized by a supervisor to prevent the processing of improper refunds and credits.
   - a. The refund process must involve a minimum of two persons. One person processes refunds (duty of the clerk), and the other approves (duty of the supervisor) those refunds.
   - b. The refund process must be evidenced by approval signatures by the supervisor for each refund transaction processed. The unit must retain the refund transaction records, ensuring controlled and limited access of authorized persons only.
   - c. Front line clerks processing transactions should not have the ability to modify transactions. Where business reasons require such capability, access to this capability must only be granted with proper supervision. For example, clerks should not have the ability to void or otherwise correct sales, without proper secondary approval.
   - d. Credit/debit card refunds must only be processed to the credit/debit card refund which was originally charged. Deviation from this procedure should only be undertaken with appropriate management approval.
   - e. Refunds and credit procedures should only be approved where the customer presents a receipt, that provides evidence a particular charge was processed by the unit. The receipt should then be marked to indicate that a particular transaction was refunded by the unit to prevent duplicate refunds being processed against a particular charge.
   - f. Managers should regularly review credits, refunds, and voids to ensure compliance with proper procedures. The review should include a survey, and if warranted an investigation, of high risk transactions. High risk transactions include: multiple refunds to the same individual; multiple refunds processed to the same credit card; multiple refunds processed to the same debit card; unusual number of voids or refunds processed by a particular clerk or at a particular site.

4. **Protection of Confidential Information:** Records of credit/debit card transactions that include payee and card number data must be kept in a highly secure site with controlled and limited access. Ensure your unit’s systems have card masking (client receipt cannot show card number except last 4 digits). Provide clients with an environment where they can shield their transaction from the view of other customers.
5. **Protection of Card Processing Equipment**: The unit’s manager is responsible for ensuring the safekeeping and protection of Moneris equipment, user IDs and passcodes. IDs and passcodes must not be shared. Only authorized staff should have access to the credit card terminals and records. Equipment must be kept out of reach of the public and protected from potential tampering by skimmers. Both Visa and Mastercard publish extensive tips on how to protect from fraud attacks.

6. **Management Review**: A unit’s management is responsible for reviewing and approving all activity, reports and reconciliations on a regular monthly basis. Any concerns should be raised to the attention of the Treasurer or the Comptroller.

7. **Services**: All requests for the following must be directed to the York University Treasury Department:

- New merchant accounts (Visa, Mastercard and Interac via Moneris; American Express)
- Change in service type (e.g., POS fixed or mobile, eSelectPlus, eCommerce, integrated systems)
- Enrolling for Merchant Direct (Moneris) and OMS (Amex)
- Refund limit adjustments
- Equipment upgrades
- Temporary equipment requirements
- Assistance with card processing service-related problems
- Inquiries concerning card processing security, new technology and EMV chip readiness

Treasury will manage the inquiries with the supplier contacts at Moneris, American Express, First Data, Chase Paymentech, etc.

Your attention to these matters is greatly appreciated. Our community’s ongoing vigilance against fraud will serve to protect the University and its many customers.

### Contacts

**York University Treasury Department**

- Michael Humpage  416-736-2100 ext. 22201  mhumpage@yorku.ca
- Gulsevil Horzum  416-736-2100 ext. 22729  horzumg@yorku.ca
- Laurie Lawson  416-736-5539/ext. 55539  llawson@yorku.ca

**York University Comptroller’s Department, General Accounting** (processing journals to GL)

- Mike Morris  416-736-2100 ext. 22000  morrism@yorku.ca
- Bonnie Barbayanis  416-736-2100 ext. 22006  barbayb@yorku.ca

**Moneris Help Line**  416-319-7450

**American Express**  1-800-268-9877