Debit and/or Credit Card Facility

Financial Service's General Accounting department provides guidance and assistance in setting up a debit or credit card facility to allow university departments to accept payments other than by cash, cheque or wire transfer.

Below is a summary of the issues that need to be considered when setting up such a facility, the processes you need to be aware of in order to avoid any unnecessary delay in getting your debit or credit card facility up and running, and the responsibilities required for ensuring the process runs efficiently thereafter:

1. Considerations before setting up a Debit/Credit Card Facility

Back to List

Many departments have already put in place facilities to accept debit/credit cards via PIN Pads (point of sale (POS) terminals) and through hosted checkout online accounts to accept credit card payments over the internet. Below are a few of the significant factors to consider when looking into the possibility of setting up a new debit/credit card facility:

One-Time Requirement or Ongoing Requirement?

If your requirement for accepting credit card payments is limited to a one-time event or annual event (such as an Annual Conference), the costs of setting up and operating a Merchant account of your own will likely be prohibitive, as the monthly costs associated with having such an account can be significant. In such cases, it is suggested that you select a software solution to help meet the needs for these one-time events. Financial Services, in collaboration with IT Services (ITS) has selected a software solution. Please review the One Time Events – Procedure for Accepting Credit Card Payments document and contact the PCI Coordinator if you have any questions

If your requirement for accepting credit card payments is ongoing in nature, and not associated with a one-time or annual event, then opening a new Merchant Account may be a good option to meet your needs, provided the benefits of doing so would outweigh the related costs to having an active Merchant Account.

Cost/Benefit Analysis

Before proceeding with creating a new Merchant Account, it should be ensured that the benefits of doing so outweigh the associated costs. A major factor in this consideration is the volume of transactions to be processed. A low number of transactions and associated dollar value of those transactions may make the costs associated with having a Merchant Account (such as monthly service charges and the rental of equipment) impractical. The costs of operating a Merchant Account are discussed in more detail in section 3 below.

Another major consideration is PCI DSS Compliance. You will need to complete a self assessment questionnaire (SAQ) on an annual basis, and weekly PIN Pad inspections submitted quarterly if you accept payment using PIN Pads. Information on PCI DSS Compliance is discussed in more detail in section 4 below.

Other Considerations

An additional matter to consider before proceeding with creating a new Merchant is to ensure that there is proper financial staffing in the department with the time and ability to process and record the related transactions as required.

Also, please note that all arrangements to set up a Merchant account must be approved by the Department Head (or delegate) with signing authority over the departmental budget before the account setup can be initiated and ultimately, Financial Services.

Back to List

2. Products Available

There are a number of products available which allow departments to accept debit/credit card payments. Below are the options available, along with their associated advantages and disadvantages, to help decide what product(s) may be the best option for your faculty or department:

- **PIN Pad (Point of Sale (POS) Terminal)**

  A PIN Pad (Point of Sale (POS) terminal) is used to process debit and credit card transactions. These are ideal for businesses or offices where customers regularly make payments for transactions on-site at the point of sale. PIN Pad have the advantage of being relatively easy to set up and use. The primary drawback is that the customer needs to be physically present in order to make the transaction, and therefore transactions can only take place on-site during business hours.

- **Wireless PIN Pad (Point of Sale (POS) Terminal)**

  Wireless PIN Pads (POS terminals) are ideal for businesses that need to process payments on the go. They have the same basic functions of a regular PIN Pad, except that they are not wired-in to one static location. The advantages and disadvantages are consistent with that of the regular PIN Pad, with the exceptions that they have the added benefit of portability, and the drawback of higher monthly fixed costs.

- **Hosted (Online) Check Out**

  By adding a simple link to your website you can accept credit cards and debit cards with your ecommerce checkout.

1. Customers click the 'checkout' or 'buy now' button on your website.
2. The customer is then re-directed to a secure payment page, enters their credit or debit card information and clicks 'buy'.

The major advantage of these accounts is the ease of use for the customer. Transactions can be completed without the customer needing to be physically present, and can be transacted at any time of the day from anywhere in the world (with an internet connection). The main disadvantage to this option is the cost of IT help that may be required to set up the departmental webpage to interface with the online payment portal.

Back to List

3. Applicable Costs

Fixed costs vary depending on the product that is used. The PIN Pad solution has the lowest fixed cost, with Hosted Checkout being slightly more costly and Wireless PIN Pad terminals costing significantly more.

In addition to fixed costs there are also **transactional costs** which vary by volume and are typically (1.5 – 3%) monthly, based on the gross amount of the transactions.

If you require more detailed information on costs of debit/credit card facilities, please send an email to the PCI Coordinator with a request for this information.

4. PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a set of mandatory requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. As such, Queen's University must take steps to ensure that all transactions being processed through associated Merchant Accounts meet this Data Security Standard, and that any/all cardholder data is handled appropriately. Non-compliance with these requirements may include, but are not limited to, potential fines, reputational damage, and the loss of payment card acceptance privileges.

More information PCI DSS can be found online at:

http://www.queensu.ca/financialservices/procedures/payment-card-industry-pci

Alternatively, if you have any questions or concerns regarding PCI DSS Compliance, or any implications it may have on your administration of a Merchant Account, please contact the PCI Coordinator at pcicoordinator@queensu.ca.

5. Setting up a Merchant Account

Back to List

In order to proceed with obtaining debit/credit card facilities, the department must fill out the Requisition Form and send it to Financial Services addressed to:

PCI Coordinator
Financial Services
207 Stuart Street, 3rd Floor

Once the requisition form is reviewed by Financial Services, authorization is provided to the payment processor to set up the debit/credit card facility for the specific product(s) chosen by the department.

The payment processor will then set up the merchant account(s) for your department, and order the PIN Pad where applicable. Also, if an e-commerce solution is required, the payment processor will coordinate with your department to identify specific requirements for the payment gateway. The department may need to get technical support to set up the interface with the online payment portal.

Once the above is completed and the department has followed the payment processor's instructions for setting up the facility, the department can begin to use the merchant account and collect debit/credit card payments.

6. On-going Responsibilities

Back to List

Once the debit/credit card facility is up and running, the following are the on-going responsibilities:

- **Recording Revenue and Monthly Fees – Financial Services responsibility**

  On a monthly basis, Financial Services will record the revenues and fees associated with the merchant account. The entries made to record the revenues will debit the Financial Services bank account, and record the credit to the departmental revenue account provided by the department at the time of account set-up.

  Similarly, the entries made to record the associated fees and chargebacks will credit the Financial Services bank account, and record the debit to the proper departmental expense account. Entries are required to be done monthly before the general ledger closes for the month pertaining to the revenue and/or fees.

- **Internal Controls and Safeguards – Department responsibility**

Back to List

  It is the responsibility of the department to ensure recommended internal controls are in place and information is safeguarded.

There are controls that should be put in place and designed to prevent the loss of assets due to error or misappropriation and to protect customers from misuse of their credit cards or breaches of their confidentiality.

- **Separate**, to the extent possible, **all duties related to data processing of payment card information**. A system of checks and balances should exist where tasks are performed by different individuals in order to assure adequate controls. For example, the same person should not process credit card transactions and perform the monthly merchant statement reconciliation. The same person should not process both transactions and refunds.

  The following duties should be performed by different individuals:
  - payment card refund
  - transaction processing
  - departmental oversight and review

- **University personnel who receive and/or process credit card information must properly safeguard the data.** This applies to all personnel who handle cardholder information during the processing of any transaction, or who retain, store, or dispose of the information. Secure environments include locked drawers, locked file cabinets, file cabinets in locked offices, and safes. Please refer to the Policy for Acceptance of Credit and Debit Cards as well as the Procedures for the Acceptance of Credit and Debits Cards for more information. These documents can be found at: http://www.queensu.ca/financialservices/payment-card-industry-pci

- **Training:** All University Staff who have any association with receiving payments through credit cards are required to sign an Ethics Agreement and complete the PCI DSS Awareness Training on an annual basis. Association with receiving payments through credit cards can include direct handling of credit card, obtaining credit card information over the phone, or payments accepted through third party e-commerce applications.

- **Payment card documentation should be treated much like cash.** It should be maintained in a secure environment limited to a minimum number of dependable, trustworthy and accountable staff.

- **Annual Self Assessment Questionnaires** (SAQ's) must be completed in order to be PCI DSS Compliant

- **Weekly PIN Pad Inspections must be conducted and submitted quarterly** as per the PIN Pad Security Training and Procedures document

To minimize the risk of loss and/or additional expenses that could occur from compromised cardholder information, **Queen's University merchants will NOT retain any of the following information electronically:**

- Credit Card number
- Credit Card expiration date
- Security Code (CVV2 number)

7. Changing or Closing a Merchant Account

Back to List

If the department wants to make changes to a merchant account or if the account is no longer required, it is important to do the following immediately in order to avoid future fees/charges:

- Fill out the Change/Close Form and send to:

  PCI Coordinator
  Financial Services
  207 Stuart Street, 3rd Floor