University of Victoria | Accounting Services

Merchant Payment Card Processing Guidelines

The following is intended to provide guidance that departments or units can use to help develop specific procedures for their department or unit. If you have questions, please contact Accounting Services – banking@uvic.ca

CREDIT CARD PAYMENTS ARE NOT ACCEPTED FOR STUDENT TUITION FEE PAYMENTS

Only UVic departments, centres and agencies that have applied for a Merchant account through Accounting Services can process payment cards. Available payment options include INTERAC®, Visa®, MasterCard®, Visa Debit®, American Express® , China Union Pay ®.

All staff that process payment card information for their department or unit, must have adequate training to ensure they understand current Payment Card Industry (PCI) Standards.

This document covers the following:

- Glossary of Terms
- Merchant Accounts
- Processing Payments
- Managers Responsibility
- Fraud Prevention

Glossary of Terms

PIN	Personal Identification Number
PED	Payment Entry Device
Card Present	A card holder is present with the payment card that can be swiped or inserted in the PED and a PIN entered
Hosted Payment Page	A merchant specific Moneris web page where customers enter payment card information for online purchases
Self Service	A card holder can select goods, services and enter payment card information through payment page online
Virtual Payment Terminal (VPT)	It is a computer with a special security configuration that allows UVic employees to safely enter customer payment card information received via telephone, mail, or fax (MOTO[1]) in a PCI compliant manner. It is an institutional decision to process payment card information received via telephone, mail, or fax using Virtual Payment Terminals to manage risk of PCI non-compliance. VPT service catalogue.
Staff Assisted	A card holder mails or phones in to request goods or service and provides payment card information, UVic employee enters the information and destroys the payment card information
Vault	Allows you to securely register and store customer payment card account

[1] Mail Order, Telephone Order payments

	information on Moneris secure servers. Can be used in conjunction with a payment page or independently.
MOTO	Mail Order, Telephone Order payments
Data Loss Prevention (DLP)	Security software that monitors activity on computers (virtual payment terminal) used to process customer payment card information.

Merchant Accounts

New

This process must be used for first time new merchant account requests or adding a new service to an existing merchant (i.e. new payment card type, equipment, adding virtual payment terminal or payment page). Requests for new merchant accounts should be made **at least three weeks** prior to the time when you are expecting to collect payments.

Note: If you require support from UVIC Systems for payment page development, PED installation, etc. that request should be made at the same time or earlier.

1. Review the options for accepting payment cards and determine the right method of accepting payment for your Unit, Department http://www.uvic.ca/vpfo/accounting/assets/docs/banking/resources/payment-card-process-options.pdf
2. Complete the Payment Processing Application Form including all approvals https://www.uvic.ca/vpfo/accounting/assets/docs/banking/merchant-request-payment-card-acceptance.pdf
3. Email the completed form to banking@uvic.ca or fax to 250-853-3814
4. If additional information or approval is required for the request you will be contacted by Banking in Treasury Services
5. You will receive notification from Banking in Treasury Services that the merchant number, services and equipment (if applicable) have been received

Changes

Changes to existing merchant account set up that impact devices/equipment or banking services must be communicated to Accounting Services. These include:

- PED replacement, returns
- Payment page changes impacting PCI compliance or banking information
- New contact person or account holder
- Removal of any service

1. To request a change to your merchant account set up compose an email that includes:
    a. Subject line: 'Chg Request Merchant Name & Number'
    b. Body: Description of change being requested
2. Send email to banking@uvic.ca
3. If additional information or approval is required for the request you will be contacted by Banking in Accounting Services, otherwise you'll be notified of request completion

Payment Card Processing Set Up

Terminal Troubleshooting

When a device/equipment malfunctions follow the steps below to resolve.

- The two most common problems/solutions
    - Cables
        - Are they connected?
        - All of them?
    - Power Source
        - Is the unit turned on?
        - Is the unit connected to the power source?
        - Does the power source have the appropriate characteristics (i.e. voltage, current, etc.)?

1. Contact your IT support staff
2. IT support staff attends location and troubleshoots issue using Moneris Guide
3. If issue is not resolved the IT support staff member calls Moneris Customer Service Center at 1866-319-7450
4. If issue is not resolved on the phone, Moneris will dispatch their Technician and provide a Reference Number and estimated arrival time
5. IT support staff emails banking@uvic.ca to notify them a Technician will be on site, Ref # and estimated arrival
6. When Technician arrives, IT support staff confirms they are the Moneris rep and assist in troubleshooting
7. Reset administrative or managerial passwords, and if necessary, reset any customized settings
8. If the device is replaced the Technician attends Accounting Services front counter in ASB to notify them of the serial number replaced and new device serial number
9. Banking staff updates the UVic Payment Card Tracking & Inventory spreadsheet

PED Replacement

Processing Payments

Card Present – Processing a payment using a PED

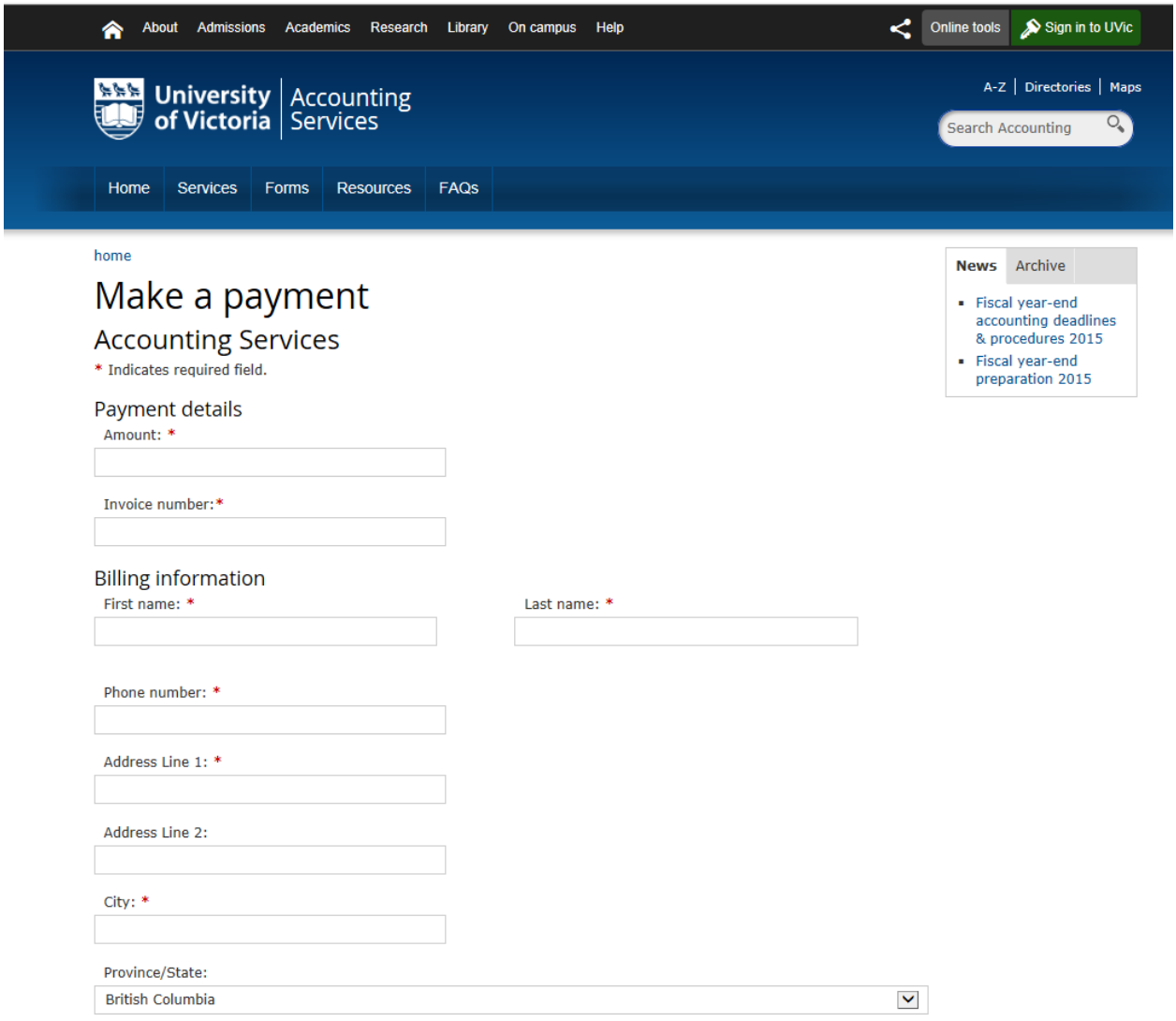
When the card holder is making a transaction in person, the following steps should be followed.

- For “chip and PIN” transactions follow the prompts on the terminal & have the card holder enter their PIN
- China Union Pay cards require a signature for all transactions even if a PIN is entered
- Compare name on card to sales receipt
- Compare signature on card to the one on sales receipt
- Compare last four numbers on the card to the numbers that appear on the sales receipt
- After the transaction has been processed through the PED device, destroy the portion of any forms or other documentation that contain credit card information. Hard copy storage of credit card information is not permitted
- For non-chip enabled cards, check the card for security features i.e. holograms, CVD on the back of the card, card brand logo appears, signature panel exists and is signed, numbers on the front are embossed, the first 4 digits of the card number are repeated below the first four embossed digits

Self-Service Payments

Units can collect payments through a payment page that allows merchants clients to enter their credit card information directly for goods and services. Units must reconcile these payments and manage refunds, voids, etc.

Payment pages are required to meet Payment Card Industry data security standards. As such, UVic Systems methodology must be followed for implementation of payment pages.



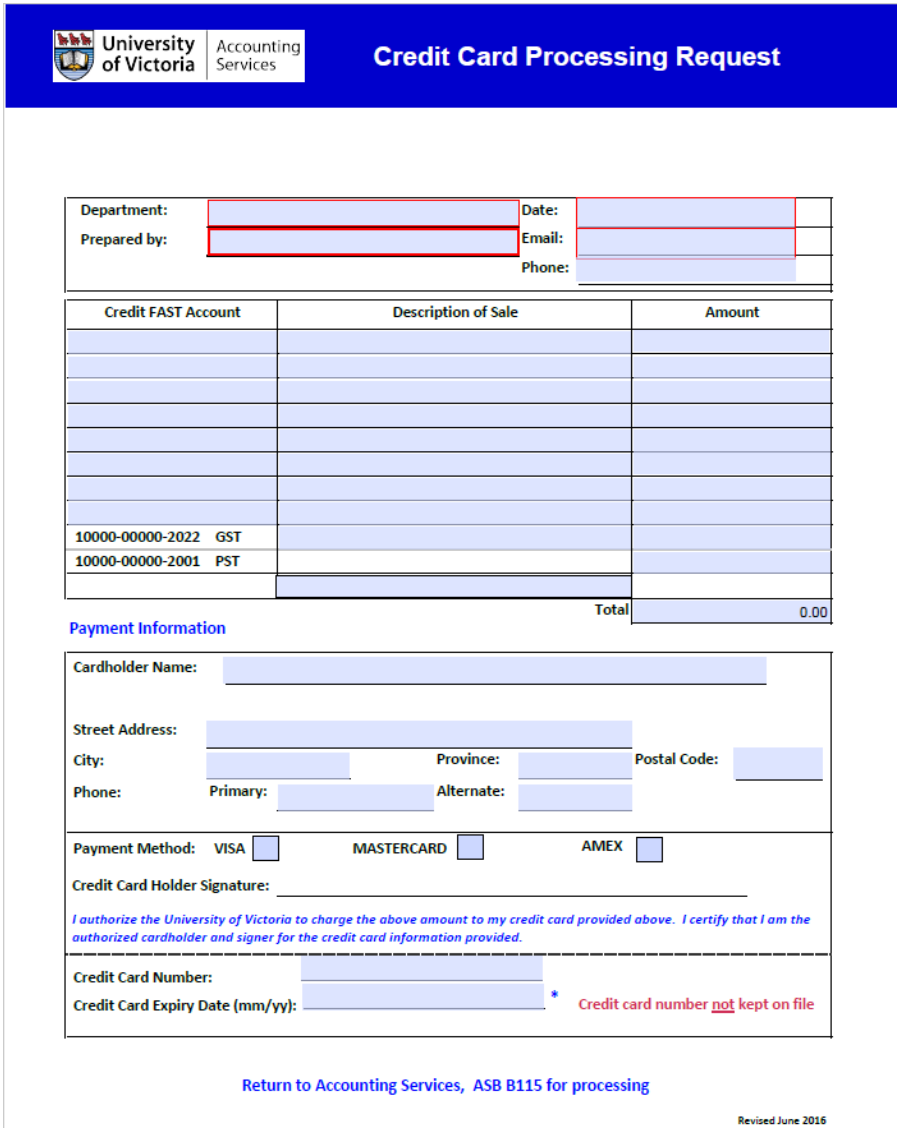
[E-Commerce Resources for Merchants]

Staff Assisted Payments (MOTO) - Phone

a) Over the phone orders must be processed through a Virtual Payment Terminal which electronically transmits card holder data to Moneris. If cardholder data is taken over the phone, the employee must immediately record the information into an approved Virtual Payment Terminal workstation while the cardholder is on the phone. If you are unsure if your workstation is approved for use of as a Virtual Payment Terminal, contact your manager, Desktop Support staff, Computer Help Desk or the infosec team. There is a sticker on the computer stating 'PCI Security Compliant Computer'. **Do not logon to Moneris to process payments on any other computer.**
b) An employee who has completed appropriate training is responsible for processing transactions at an approved workstation.
c) If the payment is for an Accounts Receivable invoice ensure the **customers quote the GR123456 reference. Otherwise, assign a reference e.g. R23 04012012 (23rd receipt on April 1st, 2012). Providing a reference maintains the audit trail back to the originating document.** Do not write down any cardholder information to maintain compliance with PCI standards.
d) In the event that a customer leaves unsolicited cardholder data on a voicemail, return the call of the customer asking them to provide payment through acceptable means and delete the voicemail immediately.
e) Never request or accept credit card information by email.

Staff Assisted Payments - Mail

a) Only forms approved by Accounting Services may be used to collect credit card information. All forms that collect credit card information should be designed in such a way that the customer's credit card information can easily be removed after processing. Customers must be instructed not to submit forms through email. The form below is an example of where credit card information should be located on forms.



University of Victoria | Accounting Services

Credit Card Processing Request

Department: Date:
Prepared by: Email:
Phone:

Credit FAST Account	Description of Sale	Amount
10000-00000-2022 GST		
10000-00000-2001 PST		
	Total	0.00

Payment Information

Cardholder Name:

Street Address:
City: Province: Postal Code:
Phone: Primary: Alternate:

Payment Method: VISA ☐ MASTERCARD ☐ AMEX ☐

Credit Card Holder Signature:

I authorize the University of Victoria to charge the above amount to my credit card provided above. I certify that I am the authorized cardholder and signer for the credit card information provided.

Credit Card Number:
Credit Card Expiry Date (mm/yy): *

Credit card number not kept on file

Return to Accounting Services, ASB B115 for processing

Revised June 2016

b) These forms are only to be used by departments for one-off payments. Payments of a recurring nature are to be processed by other approved methods.
c) Immediately after payment authorization, cardholder data must be removed from the form and shredded. The remaining portion of the form should be retained.
d) Workstations where cardholder data is received by mail must always be attended by employees when the data is being processed, recorded, or are otherwise accessible. Standard lock-out procedures for a workstation must be followed when an employee has to leave their workstation
e) If mail appears to have been opened or tampered with, employees must report this suspected activity to the Accounting Services – banking@uvic.ca .

Virtual Terminal Resources for Merchants

Manager's Responsibility

- Training
    - All employees must be taught necessary policies and procedures that will be necessary for them to complete their tasks and maintain PCI compliance
    - Training must be a continuous process, especially in accordance with changes in regulations, technology and legislation
    - Fraud prevention must be included in employee training sessions
- Post fraud-prevention reminders and materials near registers and in employee areas
- Familiarity with external regulations
    - All employees must be provided with the appropriate materials that outline policies and procedures as dictated by external organizations. These include but are not limited to the merchant agreement, VISA data security standards and MasterCard's Site Data Protection Program
- Access controls
    - Each employee must have access control determined according to the UVic Information Security Policy
- Supervision
    - Changes to Policies/Procedures
        - Every employee should be aware of any and all changes to policies and procedures. The responsibility lies with either a manager or supervisor to provide the appropriate outline of those changes and the implications for different employees
    - Review level of access
        - Supervisors and managers must review level of access that is appropriate for different levels of the hierarchy within an organization, as well as for particular positions, projects or tasks
    - Individual access privileges
        - In addition to generalized review of levels of access, managers must review the appropriate level of access for individuals and their current needs to complete tasks and projects
    - Review policies and procedures
        - Managers must review policies and procedures at least annually to ensure that their operating unit is complying to all necessary regulations including PCI
    - Managers are required to assess employee performance with respect to use of confidential and sensitive data. Further training may be required if their handling of data is not in compliance to policies, procedures, and regulations
    - Any changes to business processes involving payment processing should be done in consultation with and vetted by Treasury Services.
    - Security and Privacy obligations
        - Managers should refer to the University's Information Security and Protection of Privacy policies.

RACI Matrix

R= Responsible A= Accountable C = Consulted I = Informed

	Merchant	Accounting Services	UVIC Online	Desktop Support Services
PED Inventory	R	A		C
Payment Page Maintenance	A C	I	R	I
Payment Card Ongoing Training	R A	I		
Reporting & DCR's	R A	I		

Fraud Prevention

Signs of Credit Card Fraud: Card Present transactions (chip and non-chip)

- Signature on sales receipt doesn't match the signature on the card
- Altered or missing security features
- Signature bar appears to have been altered
- The last four digits on the authorization slip does not match the last four digits listed on the card
- Customers seems nervous or rushes the transaction
- Customer does not give the purchase adequate thought (e.g. asks no questions for high ticket items, pays no attention to size, colour, or number of items purchased, etc.)
- If you are uncertain, consult your supervisor

Authorization Responses

- When authorizing credit cards there will be four authorization responses with separate sets of actions to take for each response
- Response: Approved
  - Action: Ask the customer to sign the sales receipt
- Response: Declined
  - Return the card to customer and ask for another payment method
- Response: Pick Up
  - Keep the card if you can do so peacefully
- Response: No Match
  - Swipe the card and re-key the last four digits. If "no match" response appears again, keep the card if you can do so peacefully. Call the credit card company and request a Code 10 authorization which is a manual override request. The credit card contact numbers should be placed in a location visible to the employees processing credit cards.

How to Handle Suspected Fraudulent Credit Cards

- Keep the card and merchandise behind the counter and in your possession
- Contact the authorization centre and request a Code 10 authorization:
    - For VISA Cards:
        - VISA Voice Authorization Number – unique to each merchant account number and is only used to call in for manual over-ride requests
        - Number on the back of a customer's credit card
        - National VISA assistance centre
        - 1-800-VISA-911
    - For MasterCards:
        - Voice Authorization Number – unique to each merchant account number and is only used to call in for manual over-ride requests
        - Number on the back of the customer's credit card
        - National MasterCard assistance centre
        - 1-800-MC-ASSIST
    - For AMEX:
        - Number on the back of a customer's credit card
        - 1-800-268-9824
    - For INTERAC:
        - Primary Account Number (PAN) generated
        - IOfair@interac.ca or 416-869-8804
    - Moneris Customer Service Centre – UVic's payment card processor
        - Customer Service Help Desk for China Union Pay
        - 1-866-319-7450
- Provide all necessary information that the operator will require to confirm your identity and merchant status
- Answer all questions asked by the operator calmly and with a "yes" or "no" response
- If the operator authorizes the transaction, you may complete the sale
- If the operator does not authorize the transaction, follow all instructions that the operator provides as long as you deem it to be safe and retain the card
- Do not put yourself in any danger in order to apprehend a suspect or in attempt to retain the card
- If you feel you are in an unsafe situation to request a Code 10 Authorization, note as much information as possible and place the call to the authorization centre after the suspect has left. Provide as much detail as you can remember in order to verify the authenticity of the credit card.
- If the card is retained after being deemed fraudulent, cut off the bottom left corner to show that it is voided, but do NOT damage the magnetic strip or chip
- Fill out an incident report detailing the suspect's description and date and time of the transaction
- Contact Accounting Services – Banking, Campus Security and the Police
- If you have retained the card, minimize handling of the card to preserve fingerprints and place into an envelope in a secure location.
- Follow any further instructions given by the authorization centre
- Please be patient when calling an authorization centre, extra care is given during these procedures to ensure that the card is truly fraudulent. In addition, often merchants call for a Code 10 Authorization when they only require a call centre authorization, which will take up the available lines for verifying the legitimacy of Code 10 Authorizations.

Payment Card Fraud

- Treat terminals and PEDs like cash
- Check terminals and PEDs for unusual appearance or activity throughout the day
- Lock up terminals and PEDs at closing or when not in use
- Remind customers to protect their PIN upon entry
- Follow card-acceptance procedures: examine security features and compare the signatures on the card and sales receipt
- Consult Campus Security as appropriate to ensure that the location where credit cards are accepted is secure
- Discussions involving credit card information should only be held in an area where the discussion cannot be overhead by others that should not have this information
- Watch out for customers who:
    - Purchase large amounts of merchandise without regard to size, style, colour or price
    - Try to distract or rush you during the transaction
    - Behave strangely just after opening, or at closing (e.g. make large purchases or have an unusual number of people with them)
    - Ask for customer account information over the phone

Protecting your terminal and PED (PIN Entry Device)

- Always be aware of terminal and PED placement and positioning
- Lock unused terminals and PEDs out of sight
- Physically secure terminals and PEDs in idle lanes or check-outs
- Be aware of customers attempting to distract employees away from a terminal or PED
- Be aware of customers attempting to block an employee's view of a terminal or PED
- Place terminal and PED in an area where movement by customers would be easily noticed

Signs of terminal and PED Tampering

- Serial numbers on terminal or PED do not match the original number on record
- Label detailing the serial number has been compromised
- Security stickers have been compromised or do not match originals
- Additional skimmers or magnetic reader hardware have been attached
- A new device appears to be attached to the PED and management has not made you aware of any changes to the PED.
- Terminal connections have changed
- Unfamiliar electronic equipment is located in the area where the PED is located.
- Surrounding area has been altered
- Terminal or PED have been altered in any way, e.g. brand name, colour, etc.

How to Handle Suspected terminal or PED Tampering

- Stop use immediately
- Disconnect the PED from the terminal and power source
- Remove the terminal and PED to a secure area
- Lock terminal and PED in an isolated space (i.e. an area or container that will block wireless signals, such as a safe)
- Contact the payment card processor, Accounting Services – Banking, Campus Security. If Campus Security deems appropriate they will contact the Police.
- Do not disturb the area as it's now considered a crime scene

Common Forms of Credit Card Fraud that You Should Look Out For

- Counterfeit Credit Cards
  - To avoid the acceptance of counterfeit credit cards, employees must verify the authenticity
  - To ensure that the credit card is authentic, the security features of the card should be inspected
  - Compare the information on the card matches the information on the sales receipt – name, signature, and last four digits of PAN (Primary Account Number). Although the signature will most likely be the same, differences may be found in the visible digits of the PAN and the name.
  - To aid in the prevention of copying key credit card information, employees should be aware of and vigilant of modern copying techniques – such as skimming devices and tampered PEDs

- Lost or Stolen Cards
  - To avoid the acceptance of lost or stolen cards, employees should verify that the cardholder and the person presenting the payment card are one and the same
  - To ensure the identity of the cardholder, check the name and signature on both the sales receipt and the card
  - If the situation warrants it (such as signs of alteration to the signature or halos of previous embossed characters), request an additional piece of ID.