So you want to take credit cards?

Additional documentation can be found at the Amherst Campus eCommerce Website:
http://www.umass.edu/afsystems/basic-page/ecommerce/95

UMass/Amherst has several ways you can take credit cards to process payments for your department revenue operations. The requirements can be complex depending on how you choose to process the credit card payments but the information below should help you review your options and determine what documentation may be required. The campus eCommerce Manager will need to approve both taking credit cards and your choice of method; the Budget Office needs to approve your revenue activity and the fees you charge. Please contact the campus eCommerce Manager in Administrative Systems at 545-2119 *before* you sign any contract or begin taking credit cards.

Start thinking of your needs and options well before your need to take the credit cards since contracts with vendors need to be reviewed by the campus eCommerce Manager and Procurement, even if no purchase order will be sent to the vendor. In addition, most methods require a review of a transaction by a qualified security assessor (QSA) to verify that no credit card information is inadvertently being stored or inappropriately transmitted before you can offer credit card as a method of payment for your customers; the typical cost for this review is $2,500 and is borne by the department. The University has a contract with a vendor, Compass ITC to do these reviews. You will also need to make sure that the appropriate finance office, such as the Budget Office or Controller's Office, has authorized your area to take in revenue.

All credit card processing has costs associated with it. There fees that are charged to you, the merchant department, from the University's bank, Fifth Third or from a third party vendor. A description of typical fees can be found on the eCommerce website, but a rough estimate is that between 2.5% and 3% of your sales will be charged as fees.

Annually you will also be required to fill out a self-assessment questionnaire (SAQ) attesting to your compliance with credit card processing rules & regulations which the campus sends to the Treasurer's Office for submission to Fifth Third bank. Even if you do not have a merchant id with the University's bank, if you accept credit cards, you must submit an SAQ. Examples of SAQs can be found on the eCommerce website.

Determining which option you will use or under which option your vendor or application falls can be confusing. Any questions concerning credit cards or assistance determining which requirements you fall under, please contact the eCommerce Manager in Administrative Systems, 413-545-2119.

Are your customers typically present in person?

Consider a point of sale terminal (POS terminal), sometimes referred to as a 'swipe machine.' Customers pay by swiping their credit card through the terminal. There are wired and wireless options; Contact the Ecommerce manager for most up to date pricing.

Note: You should never accept credit card information in an email or over a web page that will, in turn, be manually entered into a POS terminal; not should you allow customers to leave their credit card information on a voicemail.

Requirements

- Phone line unless wirelss
- Merchant ID
- POS terminal

Are your customers typically not present and you wish to have them pay online?

You have several options available for taking credit card payments:

- You have programming expertise available in your department and have, or will have, a custom developed web site that captures the information you need for the purchase ex: a shopping cart or workshop registration details and payment amounts.
    - Use the University's preferred payment processor, *CyberSource,* to process the credit card payments. This will require setup and knowledge of scripting to transfer purchase information to CyberSource. The customer enters all credit card information at the CyberSource site and submits it for processing of the payment.

      Requirements
        - Merchant ID
        - Fifth/Third "Add Location Request" form
        - Cybersource Setup Document
        - Credit card data flow diagram
        - If hosted off campus, the hosting datacenter will also need to provide their PCI attestation of compliance
        - If hosted on campus, you must provide your server IP for quarterly scans – an initial scan will be done to determine any security risks
        - Scan by Qualified Security Assessor is required
            - Will include a review of secure coding practices

- You have a website up and running but do not have programming expertise to write scripts to connect to CyberSource. You may or may not have a web page collecting registration information.
    - Use *Commerce Manager* – Commerce Manager can be set up to link from your webpage to process credit cards quickly. Commerce Manager can also capture basic information for a merchant department to use for registrations or other needs. Contact Patty Roper in Administrative Systems to determine if this option is right for your area.
        - No Scan by Qualified Security Assessor, is needed.

- You do not have the programming expertise in your department but have found a vendor or software application which will manage the setup and collection of data. The vendor or software application allows you to utilize CyberSource so you may have to do some scripting to connect CyberSource to the vendor application – this varies from vendor to vendor.

  Requirements
    - Merchant ID
    - Fifth Third "Add Location Request" form
    - Third Party Processing Charge Cards Checklist
    - Cybersource Setup Document
    - Forward copy of contract for review
    - Contracts must contain appropriate PCI required language.
    - Credit Card Data Flow Diagram – flow chart of the payment process.
    - Vendor must provide adequate proof of Payment Card Industry (PCI) Compliance –

Certification of Compliance or an Attestation of Compliance signed by a Qualified Security Assessor or the acquiring bank of the vendor and must provide this annually
- Scan by Qualified Security Assessor.
- If a payment application, the version being installed must be listed on the PA-DSS list. https://www.pcisecuritystandards.org/security_standards/vpa/
- If software as a service, in the cloud – any place not on campus, the datacenter will also need to provide their PCI attestation of compliance

- You do not have the programming expertise in your department but have found a vendor or software application which will manage the setup and collection of data. The vendor uses their own payment processor so no programming needed to be done by the department. *Note*: the payment processor must be able to use the University's bank and merchant ids or a justification as to why not will need to be submitted and sent to the Treasurer's Office.

  Requirements
  - Merchant ID
  - Third Party Processing Charge Cards Checklist
  - Forward copy of contract for review
    - Contracts must contain appropriate PCI required language.
  - Credit Card Data Flow Diagram – flow chart of the payment process.
  - Vendor must provide adequate proof of Payment Card Industry (PCI) Compliance – Certification of Compliance or an Attestation of Compliance signed by a Qualified Security Assessor or the acquiring bank of the vendor
  - Scan by Qualified Security Assessor.
  - If a payment application, the version being installed must be listed on the PA-DSS list. https://www.pcisecuritystandards.org/security_standards/vpa/

- You do not have the programming expertise in your office but have found a vendor or software application which will manage the setup and collection of data for your purchases. Typically these types of applications have a lot of features, are more complex in their functionality and have their own contract with a payment processor. For example, Ucard, Campus Center Hotel, ticketing software for athletics or performances.

  Requirements
  - Merchant ID
  - Fifth Third "Add Location Request" form
  - Third Party Processing Charge Cards Checklist
  - Forward copy of contract for review
    - Contracts must contain appropriate PCI required language.
  - Credit Card Data Flow Diagram - flow chart of the payment process.
  - Vendor must provide adequate proof of Payment Card Industry (PCI) Compliance – Certification of Compliance or an Attestation of Compliance signed by a Qualified Security Assessor or the acquiring bank of the vendor
  - Scan by Qualified Security Assessor
  - If a payment application, the version being installed must be listed on the PA-DSS list. https://www.pcisecuritystandards.org/security_standards/vpa/

Any time you use a third party software vendor, you need to determine if the vendor is a Service Provider and listed on Visa's PCI DSS Validated Service Providers (http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf

or is a Payment Application and listed on the Payment Card Industry (PCI) List of Validated Payment Application: https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

Your vendor should be able to tell you if they are a Service Provider or a Payment Application. A 'rule of thumb' is that a Service Provider is not directly involved in the processing, storage or transmission of cardholder data, is a hosting provider and other entities whereas a Payment Application vendor develops payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and these payment applications are sold, distributed, or licensed to third parties.

Last updated	Date
Patty Roper	3/1/15