Accepting Credit Cards
Question and Answers

How do I get started if my department wants to start accepting credit cards?

Each department accepting credit cards must be set up within the centralized University banking and accounting environment. That is, campus departments may not set up their own banking relationships for payment card processing and card receipts. The Treasurer’s Office negotiates all banking and card processing relationships on behalf of the entire University. Prior approval to accept payment cards is required by the Campus Controller and the Treasurer’s Office, as well as our bank. For general information about starting the process to accept credit cards and the related fee structure go to http://www.cu.edu/treasury/. Joe Tinucci in the Treasurer’s Office is the initial point of contact at 303-837-2185.

Complete procedures are included in the Credit Card Acceptance policy. The procedures include the necessary documents in demonstrating to the Payment Card Industry that the University’s performed due diligence in implementing the necessary controls and safeguards to protect the cardholder account information.

What are the security and business concerns for accepting payment cards?

It is important that every University employee understand that credit card data must be fully protected, whether in electronic form, on paper, or over the Internet. Website resources are:

- Credit Card Merchant Guide
- Precard Business Practices Checklist
- Payment Card Industry Data Security Standards

General business and security considerations include but are not limited to:

- Never request a cardholder to send their credit card number over the internet – either via email or directly through their browser – except by secure methods approved in writing by the Treasurer’s Office.

- Do not store payment-card information on your PC or on the campus network except by secure methods approved in writing by the Treasurer’s Office and the campus Security Principal. No complete credit card numbers may be stored in hard copy or electronic form without required security measures. Note that if you store card information in any electronic form, the full security requirements apply to not only the system on which the data is held but also to all the other systems to which that machine is connected.
• Ensure that cardholder data printed on paper or received by fax is protected against unauthorized access. Once you have obtained an approval for a card payment, delete cardholder data (blackout credit card numbers – except for the last four digits) or destroy before it is physically disposed.

• Use care when designing paper forms so that the cardholder information can be easily protected while ensuring that the department can obtain whatever other information is necessary to process the transaction. For instance, if creating a paper conference registration form, place the registration information in the top part of the form and the cardholder information at the bottom of the form so it can be cut off and separated from the registration once payment confirmation is obtained.

• If a department is accepting payment card information via telephone, fax, or in person AND is entering that information into any computer system, the full internet security requirements as approved by the Treasurer’s Office must be applied to that data.

• Access to payment card account numbers should be restricted for users on a need-to-know basis.

• Credit card transaction, cash and deposit handling, refunds, and reconcilement duties are performed with proper segregation of duties and on a timely basis (minimum monthly).

• Refunds / credit transactions must be approved by a departmental supervisor and must be properly documented – including the reason for the refund, the approver’s signature, and such other details as may be appropriate.

What are the methods that can be used to process credit card payments?

Each University department must have a means of obtaining an authorization, as well as sending the approved transaction to the card system for processing. Methods include:

Internet

Professionally programming is necessary and many of the Visa / MasterCard requirements are of a technical nature (e.g. data encryption, firewalls, secure cookies) and require programming skills not normally possessed by departmental programmers or student staff. It is important that the Treasurer’s Office ensure that payment card data is not being stored on the University’s network and that approved third party vendors are handling the payment information. Authorized vendors have established secure, state-of-the-art
processing procedures for online transactions; using secure card services that meets the requirements of the PCIDSS data security program.

The Treasurer’s Office and UCD’s Information Technology Department will work with the departments and their software providers to discuss credit card processing, but any labor or expenses associated with implementation are the responsibility of the unit or department owning the system.

**Swipe Terminal** – A Point of Sale credit card terminal is a special-purpose terminal that allows the credit card to be swiped on a machine or the credit card number to be key-punched into the terminal and sent electronically to the credit card processing company. While this method usually requires the purchase of a card swipe terminal, it is more cost effective than other methods for ongoing card payments.

**What fees are associated with accepting credit cards?**

Every transaction incurs a "discount" and “processing” fee to the credit card system. The discount varies with the type of card presented but averages approximately from 1.5% to 3.25%. The processing fee ranges from $0.15 and $0.50 per transaction, depending on the authorization and processing methods (e.g. internet, swipe terminal or manual). In addition to these fees there are also set-up fees. For more information on fees and numerical examples of the fee structures, see the Treasurer’s website.

There will be additional fees if you are handling cardholder information over the Internet, or store cardholder information in electronic form. These fees include, but are not limited to, the account setup fee, the monthly processor charges, security vulnerability scanning fees, and security administration fees. Please see the Treasurer’s web site for additional information.