Merchant Services [1]

There is a range of acceptable options to take credit card payments:

- Point of Sale Devices
- E-Commerce (online accounts)
- Point of Sale Devices/*Point to Point Encrypted Devices (P2PE)*

Credit Card Merchant Accounts

Please contact Alisha.Palas@cu.edu [2] for more information.

Process to open a merchant account to accept credit card payments

In order to accept payment cards in return for their goods/services, departments (merchants) must complete a Merchant Application and return it to the Office of the Treasurer. Currently, the University of Colorado accepts VISA, MasterCard, and Discover cards. Upon request, Departments may also accept American Express.

Any department accepting payment cards must designate an individual (staff or faculty member) within that department who will have primary authority and responsibility for payment card transaction processing.

After the merchant application has been received, the application will be reviewed and approved by the DFA or Department Head (if applicable), Campus Controller (or delegate), Campus Internal Security Assessor, and Treasurer's Office.

If the Merchant is using a third-party service provider, the Department will need to go through the contracting process with the PSC prior to opening the merchant account. During this time, the Campus Internal Security Assessor will also review the contract, add any additional data security language and may ask for the third party's Attestation of Compliance.

The primary contact for the merchant department and any employee who will be involved with the merchant account must complete and pass a PCI-DSS online course offered within the CU Skillsoft portal.

After all approvals have been received, the Office of the Treasurer will request that a new merchant account be created with the acquiring bank, currently Wells Fargo.

Annually, all merchants must complete a Self-Assessment Questionnaire which requires attending training and working with the Campus Internal Security Assessor.

Please contact Alisha.Palas@cu.edu [3], 303-837-2135, for more information.

Should our department request a Credit Card Merchant Account?

The following business practices should be in place BEFORE a unit decides whether to accept credit card payments.

- Is the department currently employing good business practices for handling non-credit card payments?
- Do cash / check deposit handling procedures conform to the campus's cash control policies and procedures?
- Are transactions, cash/check deposit handling, and reconciliation duties performed with proper segregation of duties? If not, what supervisory controls are in place to ensure proper oversight?
- Are refund transactions properly controlled?
- Are refunds approved by a supervisory before funds are returned to the payee?
- Are refund transactions properly documented and accounted for?
- Does staff understand the necessary accounting flows for transactions, and are they properly posted?
- Are detailed financial statements and reports reconciled timely?
- Does the unit have the financial resources to reconcile deposits daily?
- Are the unit's speedtypes managed in a fiscally sound manner?
- Are document retention and destruction policies in place and followed?
- Are documents securely destroyed when their retention time is completed?
- Does the unit have paper shredding capability for record destruction for paper containing cardholder information? Cross-shredding or secure data destruction services are required.
- Does the unit understand the Treasury policy that requires only paid University staff (not volunteers) process all payments, including credit card transactions? (Paid student staff qualify.)
- Does the unit understand that it is prohibited from storing cardholder data in any electronic form whatsoever?
- Does the unit understand that they must respond to and report any incident that involves cardholder data?
- Does the unit have a training program for new staff, or staff accepting new payment processing responsibilities that include card payments?
- Does the unit have the IT staff and security knowledge to create and maintain a secure online payment website, if applicable?
- Has the unit consulted with their campus IT security team regarding their security obligations for processing credit card payments?
- Will the unit be responsible timely to chargebacks and disputes, (within 14 days of notification of dispute)?
- Does the unit understand that the primary contact for the merchant account and the

fiscal principal are responsible to attend yearly PCI training in addition to completing all other yearly PCI compliance requirements?

Fraud Flags

Things to Watch For to Reduce Credit Card Fraud

Why care about fraud? Fraud raises the cost of doing business for all card merchants and financial institutions in the payment card system. The organizational unit is financially responsible for the costs associated with the merchant account, including fines passed down from the card brands for fraudulent activity.

Start by ensuring that all staff understand:

1. Your department's typical customer profile (i.e. student at the campus, specific faculty group, general public within Colorado, International)

2. Your department's typical market area (i.e. Denver, Boulder, Metro Denver, within Colorado, USA only, International)

3. With your market area, customer profile, and typical transaction defined, ask yourself the following questions about each transaction:

Is it from the typical customer?
Is it from an address in the defined market area? Is it a typical ticket size?
Is it from a normal source (online, in-person, via mail or telephone)?
Is the order for a normal number of items / services / amount? Is more than one card being used to make this purchase?
Are multiple transactions being made with similar card numbers in a sequence?

4. That you should always obtain an authorization for the full amount at the time of purchase.

5. That if express or overnight shipping is requested, it could be a fraudulent transaction.

6. Always ask yourself:

Does the customer appear nervous or display unusual behavior?
Does the customer repeatedly come back to make additional purchases?
Does the customer tell you she is having trouble with the card and give you a "special" authorization number to call?
Does the card appear to be altered in any way? (Number not embossed, number worn, damaged hologram, no magnetic stripe on the back, altered signature panel, the terminal displays a different card number than is embossed on the card, etc.)
Is there anything suspicious about the circumstance of this transaction?

Note that a "yes" answer to any one of these questions (that is, a single red flag) does not necessarily indicate a fraudulent transaction. However, the more yes answers / red flags, the higher the probability that the transaction is fraudulent.

7. Do NOT:

Process the transaction if the authorization process returns a decline.
Process the transaction if all the information necessary to complete the transaction is incomplete
Disturb the customer or attempt to make an arrest or assault the customer
Process your own transactions – good internal controls require that employees do not handle their own payment transactions
Allow volunteers or other non-university staff or students to process card transactions.

8. Understand that there are fraud screening protections for online accounts; some are free and some are available for a minimal extra cost, including:

Maximum or minimum amount of purchase
Number of transactions for a single customer within a defined time span
Number of items/services purchased per session
Number of simultaneous sessions from particular IP addresses
Address verification service which compares address submitted on the order to the address billing address
Enhanced card code verification to validate the cardholder 3 or 4 digit security code

Payment Card Processing Best Practices

1) Define your Customers, Market Area, and Typical Transaction

Knowing to whom you provide your products and services, where you provide them, and what a typical transaction looks like is very important in reducing fraud. It also assists you in defining internal controls.

2) Require Good Internal Controls

Require that payment processing happen with good internal controls. This means that the tasks of processing the payment, batching the daily transactions, and reconciling financial statements be distributed between different people. If this is not possible, please consult with your campus controller or finance office for advice on how to implement sufficient internal controls to ensure that opportunities for error and fraud are reduced as much as possible. In no case should an employee ever process their own card transaction (payment or refund).

3) Specify a Security Policy

Each merchant is required to have a security policy, whether you process card payments manually, over the phone, through your web site, or use a third party processor to handle everything. You policy should cover at a minimum the following points:

Perform an annual risk / threat assessment or review
Specify standardized processing procedures that keep cardholder data secure?
Specify whether or not remote access / processing is allowed, under what circumstances, and how it will be secured
Include employee security awareness program (all employees have security training upon hire and annually)
Require employees to acknowledge at least annually that they have read, understood, and

accept the security policies
Screen employees handling any type of payment
Address use of third parties to handle / process cardholder data
Include PCIDSS security language in all contracts with vendors; monitor that vendor has maintained PCIDSS compliance
Implement an incident response plan

NEVER store cardholder data in spreadsheet, word processing, database, or other software.

4) Specify a Refund Policy

Your customers must be informed of your Refund Policy.

You can have a "No Refunds" policy.
Your refund policy must be disclosed to your customers, via signs in your physical location if you process card-present transactions, on your web site, or in your mailing materials.
Refunds must be processed against the original card presented for payment and for the full amount of the original purchase; they cannot be paid in check, unless the window for credit card refund has passed.
Refunds should be approved by a supervisor, and this approval should be documented along with the refund documentation

5) Specify a Privacy Policy for Your Web Page

Your privacy policy must incorporate CU's existing privacy policies.

Any information that you collect online to facilitate payments must be disclosed in your web site privacy policy / statement.

Tell your customers what data you collect, why you collect it, how you will use it, and when you will delete it from your records

6) Establish and Maintain a Records Retention and Destruction Policy

The State Archivist and the CU Office of University Controller (System) have established normal record retention timeframes for particular documents and your policy should follow those timeframes. In addition, the Payment Card Associations also have record retention timeframes pertaining specifically to payment card transactions. The records retention policy for CU can be found here: https://www.cu.edu/ope/aps/2006 [4]

The advice of the Treasurer’s office is to physically retain paper records for the minimum time necessary to document disputes and chargebacks. If a dispute or chargeback arises later, you can reconstruct the transaction from your receipt documentation or from the online ClientLine portal.

It is extremely important to destroy records (by cross-shredding or other secure destruction technique) when no longer needed or within retention policy.

7) Keep Cardholder data safe.

Here are some examples of **best practices** which will help your team to protect cardholder data:

Learn your department's merchant security policy, and make sure that you know how to apply the rules on the job.
Under no circumstances should credit/debit card information be obtained or transmitted via email.
No cardholder information is allowed to be stored electronically on any device (e.g. computer hard drives, external storage media, etc.). This includes reports from hosted credit card processing vendors. Redacted or masked information can be stored electronically.
Access to cardholder information must be limited to those individuals whose job requires access.
Any paper documents that contain cardholder information (IF the business process is approved by the Office of the Treasurer), must be treated as confidential and must be cross-shredded immediately upon receiving authorization from the bank.
Technology changes that affect payment card systems are required to be approved by the Office of the Treasurer and your campus information security team prior to being implemented.
Any new systems/software that process payment cards are required to be approved by the Office of the Treasurer and your campus information security team prior to being purchased.
Use and regularly update anti-virus software.
Do not use vendor-supplied defaults for systems passwords and other security parameters

Equipment Security Measurers

- Look for false scanners attached to devices, also known as skimmers. Skimmers can be placed over the card reader and look very similar to the original device. Look and feel for any parts that come loose easily.
- Keep an inventory of all devices used for payments, noting their serial numbers, makes, models, and any other identifying information.
- Routinely check the serial number and other characteristics of your devices to be sure that you are using the right one. An approved device could easily be switched for a false one, so it is important to be vigilant.
- Apply tamper-evident security tape over any parts of a device that can be opened. Even if the terminal can't be opened, security tape helps you recognize your terminals and create awareness of the devices.
- Keep card terminals in a secure area where unauthorized people are unable to access.

Payment Card Industry (PCI) Data Security Standard (DSS)

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. The payment card brands (Visa, MasterCard, Discover, American Express, and JCB) have collaborated to create a single set of industry requirements, called the PCI DSS, for consumer data protection. The PCI Data Security Standard aligns the security standards to create streamlined requirements, compliance criteria, and validation processes.

University of Colorado departments who accept credit and debit cards for payment are

responsible for ensuring all card information is received and maintained in a secure manner in accordance with the payment card industry standards. Individual departments will be held accountable if monetary sanctions and/or card acceptance restrictions are imposed as a result of a breach in PCI compliance.

Below is a high-level overview of the PCI DSS, consisting of 6 goals and 12 requirements:

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain network security controls.

Requirement 2: Apply secure configurations to all system components.

Protect Account Data

Requirement 3: Protect stored account data.

Requirement 4: Protect cardholder data with strong cryptography during transmission over open public networks.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems and networks from malicious software.

Requirement 6: Develop and maintain secure systems and software.

Implement Strong Access Control Measures

Requirement 7: Restrict access to system components and cardholder data by business need to know.

Requirement 8: Identify users and authenticate access to system components.

Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

Requirement 10: Log and monitor all access to system components and cardholder data.

Requirement 11: Test security of systems and networks regularly.

Maintain an Information Security Policy

Requirement 12: Support information security with organizational policies and programs.

For more information, consult the PCI website: https://www.pcisecuritystandards.org/ [5]

Reporting a Security Concern or Breach

CU departments and their third party service providers processing credit and debit card transactions must follow ALL of the PCI-DSS requirements: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_se...

[6]

Immediately Report all suspected or known security breaches to the System Administration Office of Information Security, security@cu.edu [7], the Treasurer's Office (treas.all@cu.edu [8]) and your campus information security team.

Boulder: security@colorado.edu [9]
Denver: UCD-OIT-RAC@ucdenver.edu [10]
UCCS: security@uccs.edu [11]
System Administration: security@cu.edu [7]

Approved third party vendors and approval process

Third Party Service Providers

A third-party service provider is a business entity directly involved in the processing, storage, or transmission of transaction data or cardholder data on behalf of the university. They also include companies or organizations that provide services that control or could impact the security of cardholder data, or manage system components – such as routers, firewalls, databases, physical security, and/or servers – in their cardholder data environmentCDE. When an entity is processing, storing or transmitting cardholder data on behalf of the university, or they have access to university's cardholder data, they are a service provider.

The use of a third party service provider does not relieve the CU merchant of ultimate responsibility for its own PCI DSS compliance, or exempt the university from accountability and obligation for ensuring that its cardholder data and Cardholder Data Environment are secure.

Cvent - Cvent is eComm's online event management platform. CU departmental staff can build forms for both simple and complex events. The CU Office of the Treasurer has authorized Cvent as an approved vendor to accept secure credit card payments. You can easily customize the design of your event form and website, even if you don't know HTML. For more information about the program and instructions on how to contact your campus leadership team, go to https://www.cu.edu/ecomm [12].

Touchnet Information Systems, Inc. - CU Online Store, provided by TouchNet, is managed by the Treasurer's Office and is available for department use. Storefronts allow departments to collect credit card payments online. More information can be found at www.cu.edu/store [13]. All questions and requests for additional information can be directed to onlinestore@cu.edu [14].

Nelnet Campus Commerce - Nelnet is an electronic payment service provider used across the campuses for student bill presentment and student payment processing using Automated Clearing House (ACH) debits, credit cards and debit cards. Nelnet Campus Commerce is available for departments accepting online payments tied to admission applications and program deposits.

Authorize.Net - Authorize.net is a payment gateway provider. It allows departments to accept credit cards from websites and deposit funds automatically into their merchant account. The solution offers fraud protection services, recurring billing subscriptions, and checkout options.

Adding new merchant accounts/vendors: If your department would like to open a merchant account, or contract with a third-party vendor to accept credit card payments, start the process early by contacting the Treasurer's Office and your campus Internal Security Assessor to discuss options. If a third-party vendor has already been vetted and approved by the University, the process will be easier and quicker. If a vendor is not currently under contract with the University of Colorado, please allow 9 months for Payment Card review and contract negotiations after the request has been submitted to the Procurement Service Center.

If a potential third-party vendor processes payment card transactions, the vendor MUST be vetted and approved for PCI compliance, regardless of dollar amount.

University of Colorado Boulder Campus

Agreements with third party vendors must be preapproved in writing by the Campus Controller, Treasurer's Office and IT Security Office prior to execution through the PSC. Departments may be required to use preapproved vendors unless there exists a legitimate business need. All third-party providers must meet the standards set forth by the PCIDSS. In the event that the actual processing of credit card transactions is outsourced, various training and duty requirements will differ as noted below, but the principles are the same. Any requisition that appears to be for the purchase of information communication technology (ICT) goods or services must be reviewed and approved by the ICT program. Please visit the ICT Integrity page for more information about the process and to submit a request for review: http://www.colorado.edu/ictintegrity/ [15].

The Boulder campus Internal Security Assessors can be contacted at pcicompliance@colorado.edu [16].

University of Colorado Denver/Anschutz Medical Campus

In order to protect university confidential and highly confidential data, including PHI, the risk and compliance team assesses the security and practices of all third-party vendor server applications and cloud services. Third party vendor applications include those that process, transmit or store PCI (Payment Card Industry) data.
Third party vendors must:

- Prevent the loss, theft, unauthorized access and/or disclosure of university data
- Destroy data when no longer needed per university data owner instructions
- Have incident response procedures and reporting requirements in case of a breach

For more information about the approved applications and assessment process go to: https://www.cuanschutz.edu/offices/information-security-and-it-compliance [17]

The Denver/Anschutz campus Internal Security Assessor can be reached at UCD-OIT-RAC@ucdenver.edu [10].

University of Colorado Colorado Springs Campus

The UCCS Card Acceptance and Security Policy states that outsourcing agreements to third party vendors must be preapproved in writing by the Campus Controller and Treasurer's Office prior to the execution of any agreement. All Third party providers must meet the standards set forth by the Payment Card Industry Data Security Standard (PCIDSS) and be certified. This certification must be obtained before vendor is contracted and reaffirmed annually.

For more information please visit: https://compliance.uccs.edu/news/credit-card-acceptance-and-security [18]

The campus Internal Security Accessor, Greg Williams, can be contacted at gwillia5@uccs.edu [19]

Accessing Client Line/Business Track Reporting

Signing up for Business Track_.pdf [20]

Groups audience:
Treasurer
Sub Title:
The Office of the Treasurer centrally manages the University of Colorado's relationship with the acquiring bank and is responsible for setting up all online and card present merchant accounts, ordering equipment, and closing merchant accounts.

Links
[1] https://www.cu.edu/treasurer/services/merchant-services [2] mailto:Alisha.Palas@cu.edu
[3] mailto:alisha.palas@cu.edu [4] https://www.cu.edu/ope/aps/2006 [5]
https://www.pcisecuritystandards.org/
[6] https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
[7] mailto:security@cu.edu [8] mailto:treas.all@cu.edu [9] mailto:security@colorado.edu
[10] mailto:UCD-OIT-RAC@ucdenver.edu [11] mailto:security@uccs.edu [12] https://www.cu.edu/ecomm
[13] https://www.cu.edu/store [14] mailto:onlinestore@cu.edu [15] http://www.colorado.edu/ictintegrity/
[16] mailto:pcicompliance@colorado.edu [17] https://www.cuanschutz.edu/offices/information-security-and-it-compliance [18] https://compliance.uccs.edu/news/credit-card-acceptance-and-security
[19] mailto:gwillia5@uccs.edu [20] https://www.cu.edu/doc/signing-business-trackpdf