Published on *University of Colorado* (https://www.cu.edu)

Merchant Services [1]

Merchant Accounts

Merchant Accounts are used to accept payment cards and other forms of payment either online or in-person.

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

There are two acceptable options accept card payments:

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

Process to Open a Merchant Account

In order to accept payment cards departments must complete a Merchant Application and return it to the Office of the Treasurer. Currently, the University of Colorado accepts VISA, MasterCard, Discover and 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. Some departments have PCI DSS training specific to their environments. These trainings should be taken in addition to the Skillsoft training.

After all approvals have been received, the Office of the Treasurer will request a new merchant account 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.

Should our department request a Merchant Account?

Maybe! Here are a few points to consider before requesting a Merchant Account.

- Have you checked if CU Online Store [3] will work for your needs? CU Online Store is managed by Treasury and alleviates many responsibilities from your department for PCI Compliance. The reconciliation process is also much easier!
- Do you have enough staff members to manage all steps with proper separation of duties? Similar to cash handling policies, there should be enough members of your team to separate, at minimum, acceptance and reconciliation responsibilities.
- Are you ready to implement required policies and procedures to accept card payments? Each department is required to have a policy in place for card acceptance. It is required to review this policy at least annually, or any time there are significant changes to the payment environment or responsible parties.
- Do you know what PCI-DSS Compliance is? The Payment Card Industry (PCI) created Data Security Standards(DSS) that lay out minimum data security requirements we must abide by in order to accept card payments. Part of these Standards include yearly attestation and training to ensure we, as a University, are compliant.

For next steps or more information on roles and responsibilities, including PCI Compliance, please contact MerchantServices@cu.edu [2].

Tips to Reduce Fraud

Online Card Acceptance

- Use fraud reduction tools offered by many online gateways or service providers
- Set minimum and maximum transaction amounts, if possible
- Use address verification services
- Use ReCAPTCHA, if available
- Only issue refunds to the original form of payment

In-Person Acceptance

- Check your card devices before each use for evidence of any tampering
- Use Tap-to-Pay whenever possible
- Only issue refunds to the original form of payment

What NOT to Do:

- Do not accept card payments via email
- Do not store card data electronically
- Do not keep paper with written card data
- Do not allow someone to process their own card payment or refund

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 Internal Controls

Require internal controls for payment processing. This means the tasks of processing the payment, batching the daily transactions, and reconciling financial statements should 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 opportunities for error and fraud are reduced as much as possible. In no case should an employee 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. Your policy should include at a minimum:

- Standardized processing procedures to keep cardholder data secure?
- Circumstances under which remote access is granted and how remote access will be secured
- An employee security awareness program (all employees have security training upon hire and annually)
- Requirement that employees acknowledge at least annually that they have read, understood, and accept the security policies
- Requirement that employees should be given the least amount of access necessary to complete their assigned duties
- Details of how a third-party is used and how they impact the cardholder data environment (if applicable)
- PCIDSS security language in all contracts with vendors; monitor that vendor has maintained PCIDSS compliance
- An implement an incident response plan
- Requirement that cardholder data is NEVER stored in a spreadsheet, word document, database, email, or other electronic forms of storage.

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. This includes disclosing a "No Refunds" policy.
- Refunds must be processed against the original card presented for payment Refunds cannot be paid in check, unless the window for credit card refund has passed. Please refer to the Procurement Service Center for the process to issue a refund via check.
- Refunds should be documented and approved by a supervisor.

5) 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].

Paper records should be kept for a minimum amount of time.

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

6) 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 you know how to apply the rules on the job.
- Under no circumstances should payment 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. The level of access should be restricted to the minimum access needed to complete their job duties effectively.
- 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 when no longer needed; usually once authorization has been received 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 or software that process payment cards are required to be approved by the Office of the Treasurer, your campus information security team and hte Procurement Service Center prior to being purchased.
- Do not use vendor-supplied defaults for system passwords or other security parameters

Equipment Security Measures

- 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 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 them.

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 creates streamlined requirements, compliance criteria, and validation processes.

University of Colorado departments who accept payment cards are responsible for ensuring all card information is received and maintained in a secure manner in accordance with PCI DSS. 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 payment 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 (TPSP)

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 environment (CDE). 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 payment 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 payment 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, payment 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. 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 plenty of time for IT Security Reviews and contract negotiations. For questions regarding contracting, please refer to the Procurement Service Center's website (cu.edu/psc [15]).

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

Each campus has a unique IT review and approval process. These approvals must be completed before a merchant account will be opened. Please reference websites below for your specific campus' process.

University of Colorado Boulder: http://www.colorado.edu/ictintegrity/ [16].

University of Colorado Denver/Anschutz: https://www.cuanschutz.edu/offices/information-security-and-it-compliance [17]

University of Colorado Colorado Springs: https://oit.uccs.edu/security [18]

For additional questions, please contact your campus' IT Security Contacts:

University of Colorado Boulder: pci-compliance@colorado.edu [19]

University of Colorado Denver/Anschutz: UCD-OIT-RAC@ucdenver.edu [10]

University of Colorado Colorado Springs: Charlie Wertz cwertz@uccs.edu [20]

Accessing Commerce Control Center

Commerce Control Instructions [21]

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 the merchant services program.

Source URL:https://www.cu.edu/treasurer/services/merchant-services

Links
[1] https://www.cu.edu/treasurer/services/merchant-services [2] mailto:MerchantServices@cu.edu
[3] https://secure.touchnet.net/C20369_ustores/web/index.jsp?clearPreview=true
[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://cu.edu/psc
[16] http://www.colorado.edu/ictintegrity/ [17] http://https://www.cuanschutz.edu/offices/information-security-and-it-compliance [18] https://oit.uccs.edu/security [19] mailto:pci-compliance@colorado.edu
[20] mailto:cwertz@uccs.edu [21] https://www.cu.edu/system/files/pages/151455-merchant-services/docs/signing-up-commerce-control-center-reporting.pdf