CLEMSON UNIVERSITY

Credit Card

Merchant Manual

Effective Date: 10/9/2018

Table of Contents

Overview

Paying by credit or debit card is quickly becoming the preferred method of payment. Clemson University accepts Visa, MasterCard, Discover and American Express for services rendered and goods sold. The Office of Cash and Treasury Services provides a centralized credit card payment option and all departments are required to use the service provider selected by the University and/or the State of South Carolina. The Office of Cash and Treasury Services is responsible for setting up merchant accounts, ordering equipment, and is the point of contact between the credit card processing company and Clemson University. PayPal Accounts and devices like Square cannot be used to accept credit card payments on behalf Clemson University.

The Office of Cash and Treasury Services can provide departments with a range of ways to take payments including:

- Point of Sale Devices
- E-Commerce
- Mobile Payments

Merchant Requirements

A merchant is a type of business bank account that allows a business to accept and process credit card transactions. To establish a merchant account the first step is to contact the Payment Card Coordinator in the Office of Cash and Treasury Services.

Requirements for merchants include the following:

- Complete the Merchant Registration Form (point of sale merchants only) http://media.clemson.edu/cfo/cash-treasury/Merchant-Registration-Form.pdf
- Complete the Marketplace Application Form (e-commerce merchants only) http://www.clemson.edu/marketplace/application
- Complete Annual Payment Card Industry (PCI) Data Security Standard (DSS) training http://www.clemson.edu/finance/cash-treasury/merchant-card/pci-compliance.html
- Complete Annual University Self-Assessment Questionnaire (SAQ) Note: Online merchants will complete Credit Card Security SAQ: E-Commerce and Point of Sale merchants will complete Credit Card Security SAQ: POS. http://www.clemson.edu/finance/cash-treasury/merchant-card/

Security Requirements

Potential merchants that will accept credit and debit cards must comply with the PCI Data Security Standard and requirements set by Clemson University.

Payment Card Industry Data Security Standards (PCI DSS)

Background

PCI DSS originally began as five different programs: Visa's Cardholder Information Security Program, MasterCard's Site Data Protection, American Express' Data Security Operating Policy, Discover's Information

Security and Compliance, and the JCB's Data Security Program. Each company's intentions were roughly similar to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) was formed, and on December 15, 2004, these companies aligned their individual policies and released version 1.0 of the Payment Card Industry Data Security Standard.

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Below is a high-level overview of the 12 PCI DSS requirements.

Goals	Requirements
Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

For more details, consult https://www.pcisecuritystandards.org

Clemson University Card Processing Security Requirements

Below are steps that each department must take to ensure card processing safety at Clemson University:

- It is against University Policy to store cardholder data electronically or in paper format.
- Treat payment card receipts like you would cash.
- Keep cardholder data secure and confidential.
- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Assign all users a unique ID before allowing them to access system components or cardholder data.
- Never send cardholder information via email. Credit card numbers must not be transmitted in an insecure manner, such as email, unsecured fax, or through campus mail.
- Fax transmittal of cardholder data is not permissible.
- Cardholder data must be destroyed using a crosscut shredder when it is no longer needed so that account information is unreadable and cannot be reconstructed.
- Manual swipes or imprinters are not authorized for use.
- Technology changes that affect payment card systems are required to be approved by the Office of Cash and Treasury Services **prior** to being implemented.
- Any new systems/software that process payment cards are required to be approved by the Office of Cash and Treasury Services **prior** to being purchased.
- Any computer system hosting a credit card application must be housed in CCIT's data centers due to security requirements.
- Computer systems that process cardholder data must be behind a firewall.
- Use and regularly update anti-virus software.
- Do not use vendor-supplied defaults for systems passwords and other security parameters.
- Computer systems that process payment cards must have the ability to monitor and track access to network resources and cardholder data.
- Report all suspected or known security breaches to the Office of Cash and Treasury Services and CCIT's Information Security & Privacy.

Other Security Requirements for Point of Sale Devices

The department is responsible to ensure that only authorized employees have access to the credit card device. Unauthorized or unexpected individuals should not have access to the point of sale device.

All point of sale devices will be locked up in a secure area at the end of each business day to prevent unauthorized use, removal, or tampering. If the device is anchored or contained within a secure structure you do not need to lock up the device.

Security Breach

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. In the event of a breach or suspected breach of security, including the suspicion that credit card information has been exposed, stolen or misused, the merchant

must immediately review the Clemson University Credit Card Security Incident Response Plan which can be found at the link below. It will cover the steps to take in the event of a breach or a suspected breach.

http://media.clemson.edu/cfo/cash-treasury/Credit-Card-Security-Incident-Response-Plan.pdf

Electronic Commerce

Clemson University provides a centralized e-commerce software solution to the University community. Departments wishing to accept payments electronically should visit http://www.clemson.edu/marketplace/ for more information.

Merchant Responsibilities

To become a merchant the department must complete the Credit Card Merchant Registration Form for Point of Sale Merchants or the Marketplace Application for E-Commerce Merchants. The forms contain all of the information needed to create the merchant account, and all sections must be completed. Departments should allow ample time when opening a new merchant account. The process can take up to 4 weeks. The forms can be found at:

E-commerce

http://www.clemson.edu/marketplace/application

Point of Sale

http://media.clemson.edu/cfo/cash-treasury/Merchant-Registration-Form.pdf

Equipment and Supplies

New merchants accepting credit and debit card payments throughout the year will be required to purchase their equipment. The Payment Card Coordinator can assist you with equipment options and pricing. Please note an analog phone line or network connection will be required for the point of sale (POS) credit card device. Wireless and Mobile devices do not need require hookup to a phone line or network connection, but instead, work wirelessly to accept credit card payments.

Seasonal merchants who only accept credit and debit card payments a few times a year or less can rent equipment. Please note that the Office of Cash and Treasury Services does not have equipment on hand. Please allow up to 2 weeks for equipment to be ordered and arrive. The merchant will be responsible for the monthly rental, shipping, and handling fees.

Due to changes in technology as well as new banking and PCI requirements, merchants should expect to replace equipment every 3 to 5 years. If you experience problems with your equipment please contact the Payment Card Coordinator with the Office of Cash and Treasury Services.

Departments that decide to discontinue accepting credit card payments or that decide to change the processing method, must return the credit card device to the Payment Card Coordinator in the Office of Cash and Treasury Services.

Supplies for the terminals (paper-thermal rolls) are included in the State contract with the Merchant Processor. To order paper and for pricing please contact the Payment Card Coordinator with the Office of Cash and Treasury Services. Allow 3 to 5 business days for supplies to arrive.

Payment Card Coordinator contact information – cdorfne@clemson.edu or 864-656-0530

Merchant Training

All merchants are required to annually complete PCI DSS Compliance Training. The training is designed for all merchants that accept credit or debit cards online or through a point of sale device. Merchants learn about Payment Card Industry Data Security Standards (PCI-DSS), credit card best practices, and accepting credit cards on campus. The training lasts approximately 30 to 45 minutes.

http://www.clemson.edu/finance/cash-treasury/merchant-card/pci-compliance.html

New point of sale (POS) merchants must also complete POS device training before accepting credit card payments. The training helps users become familiar with the device they will be using and includes:

- Functions – Learning the screens and functionality; closing out the device, printing reports.
- Processing Payments – how to process payments from a credit, debit, or chip card.
- Troubleshooting – How to correct errors, what to do if the device is frozen, etc.

The training takes approximately 15 to 30 minutes.

The Payment Card Coordinator will contact merchants to set-up training.

Other Merchant Requirements

Annually, merchants are required to do the following:

- Complete the Clemson University Credit Card Security Questionnaire. The questionnaire is a validation tool to assist merchants in demonstrating their compliance with the Payment Card Industry Data Security Standards and Clemson University requirements. Note: Online merchants will complete Credit Card Security SAQ: E-Commerce and Point of Sale merchants will complete Credit Card Security SAQ: POS. http://www.clemson.edu/finance/cash-treasury/merchant-card/

In addition to the annual requirements above, **point of sale** merchants must complete the following.

Annually - Point of sale merchants must complete the POS Device Control Form.
http://media.clemson.edu/cfo/cash-treasury/POS-Device-Control-Form.pdf

Weekly - Point of sale merchants must do an inspection of the POS Device and the surrounding area. The guidelines and checklist can be found at:

http://media.clemson.edu/cfo/cash-treasury/Protecting-Your-Swipe%20Devices-from-Illegal-Tampering.pdf

Accounting for Transactions and Reconciliations

Reconciliations are necessary to ensure transactions are accounted for properly and posted to the correct university department. The following reconciliations should be performed by each university merchant.

- It is the responsibility of the point of sale merchant to "close out" the point of sale device and reconcile the merchant sales slips to the settlement report daily. Once the reconciliation is complete and balances, the department should submit a TouchNet Web Deposit.
- Third-party e-commerce merchants must reconcile their internally generated transaction report to the third-party processor's Batch Summary Report daily. Once the reconciliation is complete and balances, the department should submit a TouchNet Web Deposit.
- Departmental deposits are to be reviewed monthly to ensure deposits post to the correct account and for the correct amount. The reconciliation process must be adequately documented and completed in a timely manner.
- The TouchNet e-commerce merchant reconciliation process can be found in the Clemson University Marketplace Manual located at http://www.clemson.edu/marketplace/docs/CU_Marketplace_Manual.pdf.

Merchant Fees

Merchants that accept credit cards shall be responsible for all transactions fees. These fees are paid by the Payment Card Coordinator with the Office of Cash and Treasury Services on behalf of university merchants. Documentation is emailed to each university merchant monthly. Applicable fees include:

- **Interchange Fees** – Interchange fees are determined by the payment brands. The rate paid for a transaction varies depending on the type of card (debit, credit, rewards card), type of transaction (card is present, a phone order, an online order), and the average transaction volume. The fee charged is also tied to the level of risk for that transaction; the lower the risk, the lower the rate. So for example, a transaction conducted with a card that is present is a lower risk and fee than a card-not-present transaction.
- **Assessment Fees** - Assessment fees are paid directly to the card associations (American Express, Discover, MasterCard, and Visa)
- **Access Fees** - Merchants are charged an access fee every time their processing system makes a connection with the network. This also includes voice authorizations, attempted sales that are declined, voids, operator error, and invalid card numbers.

Contact the Payment Card Coordinator with the Office of Cash and Treasury Services for current fees and rates.

Chargebacks

A credit card chargeback is a reversal of a credit card transaction, which is usually initiated by the cardholder or card issuer. Usually the resolution process results in a favorable decision for the cardholder. Chargebacks result in additional service fees and loss of revenue to the university merchant. Chargebacks are time-sensitive, and if

the department chooses to dispute the chargeback, it is critical to provide supporting documentation within 10 days.

Appropriate Supporting Documentation:

- Copy of Signed and/or Electronically Captured Sales Slip
- Copy of Signed Cancellation Policy
- Copy of Signed Order Form
- Signed Proof of Delivery, including Proof of Positive AVS (Address Verification System)
- Signed Rental Agreement
- Copy of the Hotel/Motel Folio
- Copy of Recurring Billing Agreement
- Copy of the Credit Receipt
- Proof that the Authorized Signer was known by the Cardholder
- Documentation Showing Additional Transactions by the Cardholder
- Proof of CVV2 (Card Verification Value) in Lieu of Imprint
- Proof of Authorization
- Proof that the Cardholder has Possession of the Merchandise/Service (ie. Photographs, Emails)
- Other Documentation

Non Face-to-Face Transactions

The merchant processing bank recommends that you provide as much information as possible to establish cardholder participation in a transaction. **Non face-to-face transactions are made at the merchants own risk.**

Face-to-Face Transactions

Network rules require a signed transaction document to establish cardholder participation in a transaction.

Process

All chargebacks are mailed to the Office of Cash and Treasury Services. The Payment Card Coordinator will provide the merchant with a copy of the chargeback. Merchants are responsible for providing all supporting documentation that substantiates the charge. The department has a limited amount of time to respond, usually 10 days. All supporting documentation will be faxed to the Merchant Processor and the Payment Card Coordinator will be responsible for monitoring disputed charges.

If the merchant fails to respond by the deadline or cannot provide supporting documentation, the merchant processor will debit the State Treasurer's Account. The Payment Card Coordinator will contact the merchant and the merchant will provide a PeopleSoft general leger number. The GL number will be charged and the State Treasurer's Account reimbursed for the debit. The chargeback will appear on the Revenue Report as a debit. Upon receipt of the debit to the GL account, the department will attempt collection of the debt for the chargeback.

- **Note: Cardholder contact information will not be provided by the issuing bank.**

Collection

Begin the collection and recover process within 10 days. All necessary efforts to collect the funds must be performed. If the department has not collected within a reasonable amount of time (30 days from date of debit to GL account) contact the Office of Cash and Treasury Services for advice on what further collection efforts may be implemented.

- Repayment should not be in the form of another credit card payment; but should be cash or guaranteed check.
- These recovery procedures are subject to auditing, therefore, records of recovery efforts must be kept.

The Fair Debt Collection Practices Act (FDCPA) prohibits debt collectors from using abusive, unfair, or deceptive practices to collect a debt. The Act covers personal, family and household debts. The following is a brief list of best practices concerning collection of debt.

DO

- Only discuss the debt with the debtor or attorney of the debtor.
- Contact the consumer via registered letter at a minimum. You can also contact the consumer via phone and/or email.
    - Send a registered letter to the debtor as soon as you become aware of the debt. The Office of Cash and Treasury Services has created a returned item letter template that all departments must use to collect on the returned item. The letter can be found at: http://media.clemson.edu/cfo/cash-treasury/CC-Return-Item-Letter.docx.
    - Keep a copy of the letter and proof it was sent registered or certified.
    - Document call times and conversations with the debtor.
    - Keep all emails between the department and the debtor.
- Identify yourself and state the reason for your call (if you are speaking to debtor directly).
- Call only between the hours of 8:00am and 9:00pm at the debtor's location.
- Do notify debtor of the consequences of non-payment (no longer conduct business with said debtor, etc.)

DON'T

- Do not discuss the debt of someone other than the debtor.
- Do not communicate by post card.
- Do not use any language or symbol on any envelope or in the contents of any communication that indicates you are collecting a debt.
- Do not communicate with any person other than the debtor's attorney once you have been provided with that attorney's name and address.
- Do not call at times you know to be inconvenient.
- Do not call, fax, or email debtor at work.
- Do not use or threaten to use violence.
- Do not use obscene or profane language.
- Do not cause a telephone to ring or engage in telephone conversations repeatedly or continuously with the intent to annoy, abuse, or harass.
- Do not leave voice messages stating you are calling for collection of debt.
- Do not contact the debtor once they have filed for bankruptcy.

Below are some tips for avoiding e-commerce chargebacks:

- Use AVS (Address Verification Service)
  - Using AVS helps card-not-present merchants reduce risk.
- Ship to the billing address
  - If the shipping address doesn't match you should carefully review the transaction. Reach out to the cardholder or call the issuing bank.
- Obtain delivery confirmation
  - Obtain documentation that the shipment was delivered and received.
- Get the card security code
  - Security codes are part of the authentication system that helps merchants ensure the card is actually in the cardholder's possession. Always require customers to enter the card security code during the checkout process.
- Process refunds quickly
  - Refunds can take 5 to 7 business days to be returned to a cardholder's account. Process the refund as quickly as possible.
- Provide refund details in writing
  - Email the cardholder that the refund was issued, providing the amount and date the refund was processed. Notify the cardholder that the refund will take 5 to 7 business days to post back to the credit card account.
- Share contact information
  - Make sure contact information is easy to find. Include at least the phone number and email address on each page of the website. Create a more detailed "Contact Us" page.
- Make cancellations easy
  - Consider a no-strings-attached cancellation policy. The more restrictive a cancellation is, the more resistance you will receive. A "no-questions-asked" policy is recommended.
- Obtain Acceptance of Terms and Conditions of the Sale
  - Customer must agree to the terms of sale before the transaction is completed.
- Settle Transactions Daily
  - If a transaction is more than 7 days old, request a new one before settling the transaction.

Merchant Rules and Regulations

Card companies have set standards that provide merchants with clear direction as to their responsibilities when accepting credit cards for payment. The Bank Card Merchant Rules and Regulations can be found at:

American Express - https://www209.americanexpress.com/merchant/services/en_US/merchant-regulations

Discover - http://www.osc.nc.gov/secp/discover/2011_Discover_Operating_Regulations.pdf

MasterCard - https://www.mastercard.com/ca/merchant/en/getstarted/rules.html

Visa - https://usa.visa.com/dam/VCOM/download/merchants/card-acceptance-guidelines-for-merchants.pdf

Ongoing Policy Management

The Office of Cash and Treasury Services may modify this policy from time to time as required. This document is a working draft and is expected to be modified as PCI Compliance grows and changes.

The Banking and Payment Card Coordinator with the Office of Cash and Treasury Services is responsible for overseeing an annual review of this policy, making appropriate revisions and updates and issuing the revised policy to the appropriate merchant departments.

Related Links

Cash and Treasury Services Website

http://www.clemson.edu/finance/cash-treasury/index.html

Office of Information Security Website

http://www.clemson.edu/ccit/help_support/safe_computing/

PCI Security Standards Council

https://www.pcisecuritystandards.org/pci_security/