THE UNIVERSITY OF ALABAMA | Division of Financial Affairs

Campus Mail Service Credit Card Transaction and Security Policy

Unit: Business Activities
Effective Date: 3/20/2017
Revision Date: 12/18/2017

Contact: Christina Mullis
Title: Senior Director of Process Review and Financial Compliance

Purpose

The purpose of this policy is to address the protection of credit card data including data access limitation, data storage, data retention, and data disposal.

This policy applies to all Campus Mail Service employees who handle payments by credit card. It is intended that this policy be followed for the security and confidentiality of personally identifiable information and to comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements.

Policy

Protecting Customers' Personal Credit Card Information

All personal credit card information must be strictly controlled and protected. Failure to maintain strict controls over this information could result in unauthorized use of a credit card number and serious problems for the customer, department and the University. Personal credit card data, including the credit card number, expiration date, and security code should never be removed from campus for any reason. This information should never be stored on a personal computer or any type of transportable USB drive.

No employee should ever send or request cardholder information to be sent via e-mail, fax, instant messaging, chat, etc. Credit card information transmitted in this manner should be destroyed immediately. The customer should be reminded that there are alternative methods in place for submitting credit card information that would provide better security of personal data.

Transport of Secured Credit Card Data to Another Area

Since printed receipts for credit card transactions, generated by Campus Mail Service, do not contain the full credit card number, Campus Mail Service does not have a policy to address the Transfer of Custody of Credit Card Information. Receipts only show the last four digits of the credit card number. These receipts are sent to the Financial and Administrative Specialist for scanning.

Securing and Storing Customer's Personal Credit Card Information

No documents should be stored which contain personal credit card data.

Credit Card Transactions Processed Through a Terminal

The merchant copies of credit card receipts generated from a terminal transaction are accumulated throughout the day by the responsible staff member. The credit card receipts are safely stored in a locked cash drawer and submitted to the appropriate member of management on a daily basis. The Ferguson Mail Center and Fingerprinting and Passport Office will store all daily credit card receipts in the locked safe in the respective location(s). Only supervisor(s), manager(s), and the director will have access to the locked safe where credit card receipts will be stored. This includes credit cards that may be accidentally left at the customer service window by a customer. All credit cards returned to the customer must be verified against a valid ID prior to release.

Credit Card Information Received by Telephone

Customer credit card information should not be taken over the phone. In order for Campus Mail Service to accept a credit or debit card as a method of payment at the Ferguson Mail Center or Fingerprinting and Passport Office, the customer must be at the customer service window, in person, ready to make a purchase with the card available.

Credit Card Information Processed Online

Online credit card payments are made by the customer via a secure, hosted payment gateway. Department employees should never enter credit card data on behalf of the customer into the web site. Staff members do not have access to any Personally Identifiable Information (PII) related to payments processed online.

Securely Processing Customer Refunds to a Credit Card

When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited to the same credit card account from which the purchase was made. This is a requirement of the credit card contract. Crediting to the same account used for the charge protects the customer. Processing refunds as a credit back to the card honors the banking agreement and reduces credit card fees incurred by the University. Refunds must be submitted immediately to the supervisor or manager.

Refunds of online transactions are conducted via the secure, third party hosted gateway or other method approved by Administrative Services and may only be authorized by the Director of Campus Mail. No PII is accessible or necessary to the staff.

If a transaction is rung up incorrectly on the credit card terminal, the entire transaction must be voided. DO NOT try to process the card again in order to correct the amount or make up the difference. The original sale must be voided and a copy of the voided sale receipt should be submitted to the supervisor or manager.

Batch/Settling

All credit card funds will be deposited daily into a University designated account by settling a credit card batch every evening. All credit card transactions must be settled daily.

Credit Card Terminals

A list of credit card terminals, including make and model of the device, physical location, and serial number, will be maintained by the System Support Coordinator. The list will be reviewed monthly and updated as terminals are added, relocated, disposed, etc.

Customer Service Associates and other departmental personnel with access to the terminals will receive training so they are aware of procedures to detect and report attempted device tampering and substitution. Personnel will be trained to verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices, not to install, replace or return devices without verification, to be aware of suspicious behavior around devices, and to report suspicious behavior and indications of device tampering or substitution to appropriate personnel.

Terminal surfaces will be inspected monthly by the System Support Coordinator in order to detect possible tampering or substitution. In addition, Customer Service Associates will be trained as to signs of tampering and substitution and will informally inspect terminals as they are used during day-today operations. Any terminals with limited volume or that remain in idle status for more than two business days should be stored in the locked safe until needed again to process transactions.

Credit Card Data Retention and Disposal

Because of the nature of Campus Mail Service business needs, credit card receipts generated from a terminal are scanned and retained for a period of 3 years. Terminal receipts only contain the last four digits of the customer's credit card; therefore, scanning and retaining receipts does not affect compliance with PCI requirements. Any other information received containing the entire credit card number, expiration date, or security code should be destroyed

using a cross-cut shredder. Maintenance of the terminal receipts is performed by the Financial and Administrative Specialist.

Customer Reported Suspected Credit Card Misuse

If any mail center employee is contacted by a customer to report suspected fraudulent use of their credit card, the customer should be referred to Student Account Services. Student Account Services will assist and involve other University authorities as needed.

If the Ferguson Mail Center or Fingerprinting and Passport Office knows or suspects that their credit card receipts or other stored credit card data has been breached, they should contact the OIT Information Security Officer as quickly as possible. Do not turn device(s) off, but unplug only the network cable. UA has an incident response team which will determine the appropriate course of action needed.

Information Security Policy

Campus Mail Service and Financial Affairs Business Activities will review and update the credit card policy and associated procedures to address protection of credit card data on an annual basis. Mandatory training for all employees who have access to credit card data will be provided annually or within three days from initial date of employment for all new employees. All new users will not be granted access to the point of sale system until training has been completed. Employees will acknowledge in writing that they have read and understood the department's security policy and procedures including data access limitation, data storage, data retention, and data disposal. This written acknowledgement must be reviewed and re-signed annually. All employees must also complete the University required online training through Skillport (PCI DSS Compliance Awareness Training). A certificate of completion will be issued and a copy must be sent to the Director of System Support and Administrative Services. The signed acknowledgments and certificate of completions will be kept on file in the Office of Business Activities.

Definitions

Payment Card Industry Data Security Standard -mandated set of security standards created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding cardholder data for all credit card brands.

Personal Credit Card Information - personally identifiable information related to an individual's credit card including the full credit card number, the expiration date, and the security code.

Personally Identifiable Information - an individual's personal data that may be subject to misuse. Examples include full credit card number, credit card expiration date, credit card security code, etc.

Point of Sale System - a point of sale system refers to the computer hardware, software and checkout terminals used by staff to process in-person customer transactions, create and print receipts, and maintain and update the associated databases and reports. POS systems process and transmit card holder data but do not store card holder data on University equipment or systems.

Security Code - a three- or four-digit value printed on the card or signature strip on the back of the card, used to verify that the customer has the card in their possession or has a least physically seen the card.

Scope

This policy applies to all Campus Mail Service employees who handle payments by credit card.

Office of the Vice President of Financial Affairs

Signed: DocuSigned by: DC7FC10D23404E0... 12/18/2017

Cheryl Mowdy
Assistant Vice President for Financial Affairs