The University of Memphis

BFGuide

Cash Handling Guide Part 7: Processing Credit Card Transactions

Issued: May-18-2009
Responsible Official: Assistant Vice President, Finance
Responsible Office: University & Student Business Services

Purpose

This guideline provides policy and procedures for approved credit card merchants and requirements for credit-card data security. A credit card merchant is defined as a department or other entity which processes credit transactions.

Contents

- **Links**
  - **BF Guide 10914-Cash Handling Guide Part 3: Processing Cash Collections**
- **Contacts**
  - **USBS Office**

	Definitions
Acquirer	The acquirer, also referred to as "acquiring bank" or "acquiring financial institution, processes credit card transactions on behalf of a merchant, and initiates and maintains relationships with merchants for the acceptance of payment cards. The University of Memphis merchants use the card processor selected by the University.
Credit Card	The University of Memphis merchants are approved to accept Visa, MasterCard, Discover and American Express.
Credit Card Fees	The fees paid by The University of Memphis accepting a credit/debit card for payment. For Visa and Mastercard, the largest component of the discount fee is interchange, which is charged by the Visa or Mastercard Associations. Interchange rates are non-negotiable, as they are determined by the Associations and are based on qualification requirements of each transaction. The bank that issues a credit card to an individual receives the interchange fees.
Merchant	A merchant is defined as any entity that accepts payment cards as payments of goods and services.
Payment Card Industry Data Security Standard (PCI DSS)	The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security programs with MasterCard's Site Data Protection program, the standard provides an actionable framework for developing a robust account data security process including preventing, detecting and reacting to security incidents.

Payment Application Data Security Standard (PA-DSS)	A set of requirements derived from and closely related to the PCI DSS, but intended to illustrate for payment software vendors what is required for their payment applications to facilitate and not prevent their customers' PCI DSS compliance.
Point of Sale (POS) Device/Terminal	Hardware and /or software used to process payment card transactions at merchant locations.
Primary Account Number (PAN)	Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular card holder account.

Procedures

General Information

To accommodate customers wanting to pay by credit card, authorized receipting sites may accept Visa, MasterCard, Discover, and American Express payments. These guides are consistent with other cash handling guides, though some additional steps and compliance requirements are required. The following guidelines highlight the most critical issue in providing this service, to ensure that the trusted relationship between The University of Memphis and its customers is conducted in the most secure, confidential and reliable method possible. The University requires each unit be certified as a credit card processing site and the USBS Office must approve each method and internal procedures for processing credit card transactions. This certification will include, but is not limited to, the storage of charge card numbers, data collection, system security, physical security, disaster recovery, reporting, reconciliation and privacy.

The University is required to submit certification of Payment Card Industry (PCI) compliance annually to the University's acquirer. If the University was subject to a breach of primary account numbers (PAN) data, the University would be subject to minimum of $100,000 and up to $500,000 per incident imposed by each credit card company (VISA, MasterCard, Discover and American Express) and any other remediation expenses. Departments/activities may be responsible for a portion of these expenses if the breach was due to their negligence. Departments may share in the financial responsibility of any penalties or cost associated with said breach.

General Requirements for Credit Card Merchants

Approved credit card units must meet and adhere to the following general requirements.

- Show that by accepting credit cards as a means of payment, the operation materially benefits the campus.
- Acquire approval of the Bursar and University's Payment Card Industry (PCI) Committee before entering into any contracts or purchases of software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g. e-commerce, POS device) and system must be hosted by a vendor that is Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS) compliant.

NOTE: Units must first meet with the USBS Office to review if the current University's cashiering and online-hosted payment systems will meet their needs.

- Establish departmental procedures for safeguarding PAN data and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, mail order, Internet, etc. Internal procedures must be submitted to the USBS Office for approval prior to implementing the acceptance of credit cards. Units should have a crosscut shredder available to shred PAN data when needed.
- Purchase additional workstations, equipment etc., if required, in order for current operation to meet PCI compliance.
- Employ appropriate financial controls in processing and reconciling credit card transactions and include the controls in the internal procedures.
- Comply fully with pertinent University policies and with all the terms and conditions outlined in the agreement with the University's credit card processor, bank and PCI DSS. Failure to comply with any policy or contractual term may result in the revocation of the authorization of a University department or activity to operate as a credit card merchant.
- Perform an annual security self-assessment and report results to the USBS Office to ensure compliance with University policy, guidelines and with PCI DSS.
- Ensure that staff attends credit card training annually as required by PCI compliance.

General Responsibilities of Units Processing Credit Card Transactions

All units authorized to accept credit card payments must exercise reasonable care in screening charge transactions to reduce credit card misuse and loss of funds.

- It is the unit's responsibility to ensure that the credit card receipt does not display the entire PAN data. Only the last four digits of the number should be printed.
- Staff should not have access to the full PAN data within the system software. Some hosted systems may have the option to view full card data or mask card data with only the last four digits.
- Units must process credit sales transactions using **approved** electronic data capture devices and/or web software as noted above.
- Units **cannot** accept credit card payments by email. If an email is received with the PAN data, the payment cannot be processed, and the customer should be notified that the University cannot accept credit card payments via email.
- Units **cannot** accept credit card payments by fax. If a fax is received with the PAN data, the payment cannot be processed, and the customer should be notified that the University cannot accept credit card payment via fax.

Credit Card Batch Settlement

Units will need to ensure that all credit card batches are settled daily.

- Depending on the credit card payment system/device, some units will perform a required credit card transaction settlement procedure at the end of the business day. A batch settlement report is produced at this time.
- The batch settlement report is attached to the individual sales receipts and filed with the daily cash receipts. Most units will be required to submit a copy of the batch settlement report to the USBS Office.
- Credit card payment systems/devices must electronically transmit the daily activity directly to the bank the same day or night that the transactions are settled.

Refunds/Credits

Refunds/credits must go through the normal required approval process. Units utilizing the University's official cash receipting system or POS terminals will submit the approved refund request to the USBS Office. Units that have an approved payment system (other than the official cash receipting system) and that have been approved by the USBS Office to process refunds/credits within their system will also go through the normal required approval process, but the payment system administrator or approved designee is authorized to process credits and refunds within the system. In either situation, units must have an approved internal procedure for the credit/refund process.

Reconciliations

Units must reconcile sales transactions captured through their web sales, cash receipting systems and POS devices.

- Units that utilize the University's cash receipting system that updates the University's ERP system will balance according to *BF Guide 10914-Cash Handling Guide Part 3.*
- Units that utilize the University's online payment system (Marketplace) that updates the University's ERP system will reconcile their marketplace transaction report to the unit's sale activity account within the University's account system for each active marketplace site. Reconciliations should be performed at a minimum weekly and also at the end of each month.
- Units that utilize an approved cash receipting system, online payment system or POS device that does not update the ERP system will balance according to BF Guide 10914- Cash Handling Guide Part 3 and submit a transmittal to the USBS Office or approved designee unit to record sales to the ERP system via the University's cash receipting system.
- If a unit discovers that sales transactions are missing, duplicated, or incorrectly posted, the individual responsible for reconciling the account(s) must contact the USBS Office for assistance in resolving the errors.
- The Accounting Office performs monthly reconciliations of all University credit card merchant sales transactions recorded at the bank with the payment transactions received for posting to the University account

system. The USBS Office will review the monthly reconciliation for deposits that have been recorded at the bank but have not been recorded in the account system, deposit discrepancies and deposits that have been recorded in the University's account system but have not posted to the bank. The USBS Office will contact the unit for assistance in resolving the reconciling items immediately.

- Units that continue to have discrepancies of any kind on the monthly reconciliation will be required to go through individual cash receipting training and may be subject to having their cash receipting privileges revoked.

Disputed Sales Transactions

- If a cardholder disputes a sale transaction processed through a University merchant, the USBS Office will notify the unit of the dispute.
- The unit must then review original records and submit supporting documentation to the USBS Office within three days of the request for dispute and/or the unit may have to contact the customer directly to address the dispute. If the dispute is not resolved within a specified time or if the credit card company approves the customer's dispute, the credit card company will charge back the payment to the University of Memphis bank account. Upon receiving notice of the charge back from the credit card company and verifying the bank account has been debited for the charge back, the USBS Office will charge the unit's account for the amount of the charge back.
- The department/activity will be responsible for contacting the customer and resolving the issue.

Processing Credit Card Sales Through Unit Web Sites

Capture of Minimum Required Sales Information

Each unit that receives approval to accept credit card payments through a web site must, at a minimum, capture the following information from each customer transaction:

- **Credit Card Information:**
  - Credit Card Number-must accept Mastercard, Visa, Discover, American Express
  - Expiration Date
  - Security Code

    - Credit Card Billing address
- **Other required information for web site application:**
    - Description of item or items purchased
    - Amount of purchase
    - Customer name
    - Mailing address
    - Sales tax, if applicable
    - Total amount charged
    - A unique identifier for each transaction
    - Email confirmation of payment

For security purposes and as required for PCI compliance, PAN data and security codes cannot be stored/retained on University web sites or administrative systems at any time or for any length of time (including seconds).

Batch Closing and Transmission

- Units that have an approved online payment system should have their credit card batch set to auto close right before midnight or at an approved designated time. If the online payment system does not have an auto close feature, then the unit will need to work with the USBS Office to determine the best time for the manual settlement process.

Credits/Refunds

- Refunds/Credits must go through the normal approval process, but only the web payment system administrator or approved designee is authorized to process credits and refunds. Such adjustments to customers' accounts will only be processed with the written request of a merchant unit. Units must be approved by the USBS Office to process credit card refunds/credits within the unit's system and each unit must have an approved internal procedure for the credit/refund process.

Additional Information

Fees

Each unit's transactions are subject to assessment, discount and a per-item fee charge by Visa, MasterCard, Discover and American Express and the credit card processor. Each month, the USBS Office will charge each unit's department account the appropriate credit card fees for their monthly sales.

Security Standard Requirements	The Payment Card Industry Data Security Standards (PCI DSS) include requirements for security management, policies, procedures and network architecture, software design, and other critical protective measures. The USBS Office and all units processing credit card transactions will comply with the **Payment Card Industry (PCI) Data Security Standard (DSS).**

Links	
BF Guide 10914-Cash Handling Guide Part 3: Processing Cash Collections	http://bf.memphis.edu/bfguide/10914.htm

Contacts	
USBS Office	https://www.memphis.edu/usbs/staff.php

Revision Dates
May 2021