

SECTION: Treasury
SUBJECT: Cash Handling Process – Credit Card Documented Procedures for Terminals, Payment Applications, and Online
APPLIES TO: Receiving, batching and reconciling credit card transactions (via terminal or payment application)

Cash Handling (Credit Card) Overview

The objective of the Cash Handling process for credit cards is to ensure that all transactions are received, validated, batched and reconciled in a timely, accurate and well controlled manner.

Cash Handling Process – Credit Card Terminals

Activity	Responsibility	Reference/Comments
KEY ROLES / TRAINING		
<p>The following positions are authorized to <i>process</i> credit card transactions for departments supported by Fleming Business Services (FBS) as determined by the Department Administrator.</p>	<p>Photo Services: Clerk, Data Entry, Work study students</p> <p>Gov Rel: GR Specialist</p> <p>MPM (Michigan Radio): Business Assistant</p>	<p>Positions responsible for processing credit card transactions should not perform reconciliation</p> <p>This/These individual(s) are also listed in Section 7 of the Merchant Services Policy Document. In some cases the Merchant Contact will be the Department Administrator. When this individual changes, send an updated Section 7 to the Treasurer’s Office.</p>
<p>The following positions are authorized to <i>approve refunds</i> for the departments supported by Fleming Business Services (FBS) as determined by the Dept. Administrator.</p>	<p>Photo Services: Manager</p> <p>Gov Rel: Executive Assistant</p> <p>MPM: Business Manager</p>	<p>This/These individual(s) are also listed in Section 7 of the Merchant Services Policy Document. When this individual changes, send an updated Section 7 to the Treasurer’s Office.</p>
<p>Update list of authorized users in MPathways of any staff changes such as: a new staff member who will be processing credit card transactions and/or approving refunds, or a staff member who is no longer processing transactions or approving refunds.</p>	<p>Photo Services: Manager and/or Business Manager</p> <p>Gov Rel: Executive Assistant</p> <p>MPM: Business Manager and/or Media Financial Officer</p>	<p>Authorized users are staff who are allowed to process credit card transactions or refunds and includes the Merchant Contact. Merchant Contact is responsible for updating MPathways with current authorized users.</p> <p>Merchants who process online <i>should not</i> process transactions on behalf of their customers. Doing so will greatly increase the scope of PCI and impact their compliance status. Merchants who intend to process transactions for their customers must contact the Treasurer’s Office.</p> <p>NOTE: For step-by-step instructions see https://maislinc.umich.edu/mais/html/GL_CR_Deposit_Merchant.html.</p>

<p>Obtain proper training and certification on an annual basis consistent with PCI requirements.</p>	<p>Photo Services: Clerk, Data Entry, Work study students, Manager</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Asst, Business Manager</p>	<p>Merchant Contact is responsible to ensure all authorized users have been properly trained (MyLinc course TME102) prior to processing transactions.</p> <p>Web based training is available on My LINC, search TME102.</p>
<p>Use a Merchant Change/Termination Form to change the merchant contact, address, chartfields, buy another terminal, terminate the existing merchant account, etc.</p>	<p>Merchant Contacts Photo Services: Manager</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Manager</p>	<p>If merchants intend to change their processing method they must establish a new merchant account number. Completed New Merchant Registration Form or Internet Merchant Registration Form, and the Merchant Services Policy Document are both sent to the Treasurer's Office.</p>
<p>RECEIVING PAYMENTS</p>		
<p>The departments supported by Fleming Business Services (FBS) may receive funds via credit card for a variety of purposes, including but not limited to:</p> <ul style="list-style-type: none"> • goods/Services provided (passport photos, advertising, diploma frames). • pledge drive donations (non-gift portion). • athletic tickets. 		<p>The gift portion of pledge drive donations are sent to and handled by the Development Office.</p> <p>NOTE: Direct submission of gifts to the lockbox by the donor is the preferred method.</p>
<p>For payments received online, merchant account is using PayPal (MPM & PS), Authorize.Net (PS) as the payment gateway provider.</p> <p>Ensure PayPal and Authorize.Net is PCI DSS compliant on an ongoing basis by verifying their compliance status on the Visa website at:</p> <p>http://www.visa.com/splisting/searchGrsp.do</p>	<p>Photo Services: Manager</p> <p>MPM: Business Manager</p>	<p>The merchant must provide the Treasurer's Office (via the New Merchant Registration Form) with the name of the payment gateway provider when setting up the merchant account. If payment gateway provider loses their compliance status, immediately notify the Treasurer's office.</p>

<p>Credit card terminals (or computers) are located:</p> <ul style="list-style-type: none"> • in locked cabinet (MPM). • in a locked office (Gov Rel). • at front counter. (Photo Services) <p>This location is not accessible to unauthorized individuals because they are either locked or behind a secure counter (in presence of an authorized user).</p> <p>When <i>not</i> in use, terminals are securely stored in a locked cabinet or safe within a locked office.</p>	<p>Photo Services: Manager, Clerk or Data Entry</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Manager</p>	<p>Merchant Contact maintains a list of terminal make/model and series number of credit card equipment and notifies Treasury to update as replaced. Can do a screenshot of this info from MPathways. Contact Treasury with any changes.</p> <p>Merchants should control access to terminals as they would a cash box.</p> <p>Merchant Contact instructs staff to inspect the credit card terminal each business day for tampering or the addition of non-standard parts (AKA ‘skimmer’) that could be used to illegally obtain credit card info. Staff should review terminal tampering training located on the Treasury website. Contact the Treasurer’s Office immediately if there’s a concern or issue.</p> <p>A list of credit card terminal serial numbers must be maintained.</p> <p>Credit card terminals are only serviced or replaced by Treasurer’s Office staff.</p>
<p>Only the following positions/individuals have access to information (e.g. reports, merchant copy receipts) containing cardholder data.</p>	<p>Photo Services: Manager, Clerk or Data Entry</p> <p>Gov Rel: GR Specialist, FBS</p> <p>MPM: Business Manager and Business Assistant</p>	<p>Credit card and personal information should be safeguarded in a manner consistent with PCI standards. All reports (e.g. merchant receipts, batch reports) should have the credit card number properly truncated (i.e. no more than the last four digits visible).</p> <p>NOTE: It is against University policy to store a full 16-digit credit card number in any format.</p> <p>MPM and Gov Rel write credit card number down and shred as soon as transaction is processed.</p> <p>Refer to the PCI Security Standard’s Council website or contact the Treasurer’s office at merchantservices@umich.edu for further information on the security requirements.</p>

<p>Accept payment via in person/swipe card, fax (Gov Rel only), or phone (Gov Rel and MPM only)</p>	<p>Photo Services: Clerk, Data Entry, Work study students</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Assistant</p>	<p>Individuals processing credit card transactions should not have any responsibilities related to reconciliation.</p>
<p>Authorize Transaction:</p> <p>If card present:</p> <ol style="list-style-type: none"> 1. Swipe card. 2. Verify signature on the back of the card. Make sure customer signs receipt when applicable. <p>If card not present (e.g. phone, fax, etc.):</p> <ol style="list-style-type: none"> 1. Key enter the card number. 2. Verify address; enter zip code when prompted by terminal. 3. Obtain the card validation code on the back of the card (Gov Rel only). Be sure to properly dispose of (i.e. shred) the card-validation code number once the transaction is authorized. 	<p>Photo Services: Clerk, Data Entry, Work study students</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Assistant</p>	<p>Refer to the quick reference guide provided with your terminal for further instructions on how to authorize a transaction.</p> <p>NOTE: If you obtain the <i>card-validation code</i> as part of the authorization process, you are not allowed to store this number under any circumstance. Storing this number would be a violation of PCI DSS and could result in penalties and fines being issued against the merchant.</p>
<p>Issue a credit card receipt in the amount of payment/refund and retain a copy of the receipt. Gov Rel sends copy to FBS.</p>	<p>Photo Services: Clerk, Data Entry, Work study students</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Assistant</p>	<p>Copies of sales receipts should be kept for up to 18 months in order to satisfy any disputes/chargebacks. These receipts should be kept in a locked file cabinet or safe. After the 18 month period has expired, sales receipts should be shredded in order to protect cardholder information. The receipts should have the credit card number properly truncated (i.e. first six and last four digits visible.)</p>
<p>Obtain approval by a higher level of authority for all refunds.</p>	<p>Photo Services: Clerk, Data Entry, Work study students</p> <p>Gov Rel: GR Specialist</p> <p>MPM: Business Assistant</p>	<p>All payment gateway providers should have controls in place to trace a refund to an individual. Additionally, it should limit a refund to no more than the amount of the original transaction.</p>
<p>Verify all refunds issued are valid and have been approved and proper evidence is maintained.</p>	<p>Photo Services: Manager</p>	<p>All refunds should be approved by a higher level authority.</p>

	Gov Rel: FBS MPM: Business Manager	Persons approving refunds should not be processing refunds.
Compare the refund receipt to the original sales receipt to ensure the amount refunded equals the amount of the original transaction.	Photo Services: Manager Gov Rel: Executive Assistant MPM: Business Manager	Cash refunds should not be given for credit card transactions. The only exception to this rule is if the purchase was made with a prepaid card (e.g. Visa or MasterCard gift card) and the cardholder is returning items, but has discarded this card.
BATCHING/SETTLEMENT		
At the end of each day (if applicable), run a batch process for each credit processing system and transmit the stored transactions to the credit processor.	Photo Services: Clerk, Data Entry, Work study students Gov Rel: GR Specialist MPM: Business Assistant	Refer to the quick reference guide provided with your terminal for further instructions on how to batch out your transactions.
Compare each settlement report to merchant receipts to ensure all transactions have batched correctly.	Photo Services: Clerk, Data Entry, Work study students Gov Rel: GR Specialist MPM: Business Assistant	
For payments received online, use the reporting tools from PayPal and/or Authorize.Net to ensure all transactions have batched correctly.	Photo Services: Clerk, Data Entry, Work study students MPM: Business Manager	Online merchants should be set up to <i>auto batch</i> daily and should not have to batch out manually. If you are not set up to auto batch contact your payment gateway provider.
Verify all refunds issued are valid and have been approved by: <ul style="list-style-type: none"> • Photo Services: Manager • Gov Rel: Executive Assistant • MPM: Business Manager 	Photo Services: MMD Business Manager Gov Rel: GR Specialist MPM: Business Assistant	Person approving refunds should not be processing transactions.
RECONCILIATION		
To change Chartfields, complete the	Photo Services:	Upon initial setup of Merchant account,

<p>Merchant Change/Termination Form with the appropriate changes. Forward the completed form to the Treasurer’s Office.</p>	<p>Manager Gov Rel: FBS MPM: Business Manager</p>	<p>chartfield allocations were reviewed to ensure each payment is posted to the correct General Ledger account. Notify the Treasurer’s Office of any chartfield changes.</p>
<p>Reconcile SOA to all settlement reports and bank statement activity to ensure all monthly activity is accurately reflected on the SOA. Maintain proper evidence of reconciliation.</p>	<p>Photo Services: Manager Gov Rel: FBS MPM: Grants Accountant and Business Manager</p>	<p>Person performing reconciliation should not process transactions. Settlement reports for an online environment should be available within the reporting tool of the payment gateway provider.</p>
<p>Review all refund activity to ensure all refunds are valid and authorized. Maintain proper evidence of reconciliation.</p> <p>Note: Refund activity can be found on the Credit Card Controls report in MReports under the Compliance tab.</p>	<p>Photo Services: Manager Gov Rel: FBS MPM: Grants Accountant and Business Manager</p>	<p>Ensure individual transactions that batched are valid and amounts were processed correctly by comparing to the point of sale / inventory records / expected amounts. Resolve discrepancies on a timely basis.</p> <p>Report can be found in M-Reporyts under the Internal Controls menu within the Compliance tab.</p> <p>Person reviewing the refunds should not process transactions or perform batch process.</p>
<p>For discrepancies, contact SSC AR for assistance.</p>	<p>Photo Services: Manager Gov Rel: FBS MPM: Grants Accountant and Business Manager</p>	
MONITORING & OVERSIGHT		
<p>Monitor batch receipts to ensure that all credit card transactions were performed by authorized personnel, and all refunds were approved by a higher level authority.</p>	<p>PS: Clerk Data Entry and/or Manager MPM: Membership Manager</p>	

<p>Review the various tabs within the FN03 JrnlDetail Merchant Management Report in Business Objects to monitor items such as:</p> <ul style="list-style-type: none"> • Sales trends • Number of refunds issued • Current PCI compliance status • Merchant certification status <p>Review Merchant Certification Status tab to ensure appropriate staff are authorized users and have completed TME102 training course.</p>	<p>Photo Services: Manager</p> <p>Gov Rel: FBS</p> <p>MPM: Grants Accountant and Business Manager</p>	<p>Report can be accessed through Business Objects at:</p> <p>UM-Maintained → Financials → FN03 Journal Detail</p> <p>Click here for additional information regarding the report.</p> <p>The CMB Treasurer’s Office Certification Course Report in Business Objects may be reviewed to monitor all individuals who have taken the TME102 course.</p>
<p>Review the standard Cash Handling report provided in M-Reports to monitor the following:</p> <ul style="list-style-type: none"> • All merchants in unit and their activity • All merchants PCI status (for the past 12 months) 	<p>Approver/Unit Administrator</p>	<p>Report can be found in M-Reports under the Internal Controls menu within the Compliance tab.</p> <p>The title of the report is: Credit Card Controls</p>

Other related information:

Treasurer’s Office Key Contacts:

- merchantservices@umich.edu or (734) 763-1299

Related Standard Practice Guides:

- See SPG [519.01](#) for credit card payment related policies

Treasurer’s Office – Merchant Services website:

<http://finance.umich.edu/treasury/merchant-services>

Record of Revisions:

Date of Issue	Description of Change	Page(s) Affected	Approved By
6/10/2009	Original template created	All	
11/25/2009	Minor revisions made for FY2010 Certification	1,2,3,5	
12/22/2010	Minor revisions made for FY2011 Certification (including updating links for new website, adding BO reports, etc.)	2-6	

8/24/11	Updated to reflect FBS supported units' processes	All	
9/14/11	Incorporated Online processes	2, 4-6	
2/25/2013	Added the review of the new report which shows who has completed the training and the date they completed it.	4	
9/9/2016	Added information on updating list of authorized users, statement on direct submission of gifts to lockbox, and statement on updating Merchant Contact with terminal make/model changes.	1, 2, 3	
8/2018	Updated to reflect recommended changes.	All	

Document Owner: Fleming Business Services (FBS) supported departments and FBS

Administrative Owner: FBS