NOTE: Any changes to process due to remote work should be documented in procedures.

FINANCE
UNIVERSITY OF MICHIGAN

SECTION: Treasury

SUBJECT: Cash Handling Process – Credit Card Documented Procedures for Online Processing

APPLIES TO: Receiving, batching, and reconciling online credit card transactions (where the department does not have access to the full credit card number and **the customer is the individual processing transactions**).

NOTE: This document has been revised as part of the Annual Internal Controls Update

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 – Online Credit Card Processing

Activity	Responsible Party	Reference/Comments
KEY ROLES / TRAINING		
The following positions are authorized to approve refunds for the for departments supported by Executive Business Services (EBS) as determined by the Dept. Administrator.	Department (See Appendix A)	All refunds should be approved by a Higher Administrative Authority. Person approving refunds should not be the person processing refunds.
Ensure record of current individuals authorized to approve refunds is up to date and kept on file in unit. See Treasurer's Office - Merchant Services Return / Refund Policies for more information.	Department (See Appendix A)	***NOTE:*** *Merchants who process online* ***should not*** *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.*
Update list of authorized users in M-Pathways > Merchant Information > Authorized Users section. This list should identify all users authorized to process credit card transactions on the merchant account(s), including the general location where user processes sales or refunds or encounters 16-digit cardholder data. It should be kept current and updated with staffing changes.	Department (See Appendix A)	*Authorized Users* are staff who are allowed to process refunds and include the Merchant Contact. Merchant contact will be listed as an authorized user by default, and this should not be changed. Merchant Contact is responsible for updating M-Pathways with current authorized users. See Update Deposit Location and Merchant Information in My LINC for step-by-step process.

Activity	Responsible Party	Reference/Comments
Internal Controls monthly push notification reports can be monitored to: • identify any employee who is an authorized user on a credit card merchant account, who has either not completed the Merchant Certification Course (TME102) in My LINC, or whose merchant certification has expired. • identify any employee who is an authorized user on a credit card merchant account but has separated from the university. • identify a credit card merchant that does not have any authorized users. • identify credit card merchants with non-compliant, expired, or incomplete PCI Status. • identify credit card merchants with a PCI status that expires soon.	EBS Director, Department (See Appendix A)	To opt in to receive monthly push notifications for credit cards send an email request to OfficeofInternalControls@umich.edu. For more information see: Push Notifications on the Internal Controls website. ***NOTE per Audit Services:*** *It is recommended that the primary contact for each merchant receive the Internal Controls Push Notifications.*
Obtain proper training and certification on an annual basis as part of Payment Card Industry (PCI) requirements.	Department (See Appendix A)	Merchant Contact is responsible to ensure all authorized users have been properly trained prior to processing transactions. Web based training is available on My LINC, search TME102.
Use appropriate Resources for updating Merchant Account information to modify the merchant contact, address, chartfields, terminate an existing account; etc. ***NOTE:*** *To ensure PCI compliance is maintained and other internal controls are in place, contact the Treasurer's Office - Merchant Services (merchantservices@umich.edu) for approval before making any changes to:* • *how or where credit cards are being accepted (including staff processing credit cards from home),* • *vendors or service providers,* • *phone systems and/or use of call center systems* *In addition, alert merchant services if changing the merchant contact or terminating merchant account.*	Department (See Appendix A)	

Activity	Responsible Party	Reference/Comments
RECEIVING FUNDS		
The school/college/unit/department may receive funds via online credit card payment for a variety of purposes including (but not limited to): • Goods/services provided • Conference fees • Donor gifts • Tickets	Department (See Appendix A)	
This merchant account is processing online and using Authorize.Net* and/or Huntington Bank as the payment gateway provider.	Department (See Appendix A) *MI Photo & VP Secretary may use Authorize.Net*	The merchant must update Treasurer's Office – Merchant Services if there is a change in the payment gateway provider.
Only the following positions/individuals have access to information (e.g. reports) containing cardholder data.	Department (See Appendix A)	Credit card and personal information should be safeguarded in a manner consistent with PCI and U-M standards. All reports provided by the payment gateway provider should have the credit card number properly truncated (i.e. last four digits). ***NOTE:*** *It is against university policy to store more than the last four digits of any credit card number.*
Obtain approval by a Higher Administrative Authority for all refunds.	EBS Analyst	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.
Verify all refunds issued are valid and have been approved and proper evidence is maintained.	EBS Director, EBS Analyst	Person approving refunds should not be the person processing refunds.
Compare the amount refunded to the original sales transaction to ensure the amount refunded equals the amount of the original transaction.	Department (See Appendix A)	***NOTE ON REFUNDS:*** *If the original credit card is no longer available (e.g., gift card, account closed), work with SSC's AP to have a check issued.*

Activity	Responsible Party	Reference/Comments
		See Treasurer's Office - Merchant Services Return / Refund Policies for more information.
BATCHING/SETTLEMENT		
Use the reporting tools from the payment gateway provider to ensure all transactions have correctly batched the business day following batching. This can be done by comparing batch records to the point of sale/inventory records/expected amounts. Resolve discrepancies on a timely basis.	Department (See Appendix A)	Online merchants should be set up to **auto-batch** 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 and proper evidence is maintained.	EBS Director, EBS Analyst	Person approving refunds should not be processing refunds.
Complete the PCI self-assessment questionnaire (SAQ) annually for each merchant account prior to the expiration date using the online portal linked in notification emails.	Department, Merchant Contact	See PCI Resources on Treasurer's Office – Merchant Services website.
Annually collect applicable PCI documents from supplier(s). Documents include Attestation of Compliance (AOC)/SAQ D - Service Provider, a responsibility matrix and a credit card flow diagram. Treasurer's Office - Merchant Services seeks copies of these documents each summer. Contact pcicompliance@umich.edu with document questions. ***NOTE:*** *Treasurer's Office - Merchant Services holds the U-M contracts for the following third-party suppliers: Bluefin, Authorize.net, and Nelnet. Merchants using these suppliers as part of their solution may reach out to pcicompliance@umich.edu to request a copy of the relevant documents, in lieu of contacting the supplier.*	Department, Merchant Contact	The Treasurer's Office - Merchant Services will contact for copies of documents.
Merchants who undergo monthly vulnerability scan should review scan results for PCI status monthly and immediately address any issues identified.	Department, Merchant Contact	See the Security Unit Liaison Directory for list of unit SUL.

Activity	Responsible Party	Reference/Comments
Provide scan results to IT Security Unit Liaison (SUL).		
RECONCILIATION		
To change chartfields, see Resource for updating Merchant Account information on the Treasurer's Office - Merchant Services website for process.	EBS Analyst	Upon initial setup of Merchant account and subsequent changes, chartfield allocations are reviewed by the Shared Services Center (SSC) to ensure each payment will be ~~is~~ posted to the correct G/L account. See Merchant Forms & Policies on the Treasurer's Office – Merchant Services website.
Review all refund activity to ensure all refunds are valid and authorized. Maintain proper evidence of reconciliation. ***NOTE:*** *Refund activity can be found on the Credit Card Controls report in M-Reports under the Compliance tab and within the FN03 JrnlDetail Merchant Management Report in Business Objects.*	EBS Analyst	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. Person reviewing the refunds should not process transactions or perform batch process.
For discrepancies, contact the SSC Reconciliations for assistance.	EBS Analyst	
MONITORING		
Monitor payment gateway reports to ensure that all refunds were approved by a higher level authority.	Department (See Appendix A)	
Review the various tabs within the *FN03 JrnlDetail Merchant Management Report* in Business Objects to monitor items such as: • Sales trends • Number of refunds issued • Current PCI compliance status • Merchant certification status Review Merchant Certification Status tab to ensure authorized users are appropriate and have completed the TME102 training course.	EBS Analyst, EBS Director, Department (See Appendix A)	Report can be accessed through Wolverine Access > Business Objects at: Home > Folders > Public Folders > UM-Maintained > Financials > FN03 Journal Detail

Activity	Responsible Party	Reference/Comments
Review the Credit Card Controls report in M-Reports to monitor the following: • All merchants in unit and their activity • All merchants PCI status (for the past 12 months)	EBS Analyst, Department (See Appendix A)	Report can be found in M-Reports (go to Wolverine Access > M-Reports) under the Internal Controls Other Reports/Tools menu within the Compliance tab.

Other related information:

Treasurer's Office Key Contacts:

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

Related Standard Practice Guides:

- See SPG 519.01, Treasury Services: Banking, Debt Issuance and Credit Card Acceptance for credit card payment related policies

Treasurer's Office – Merchant Services website

Record of Revisions:

Date of Issue	Description of Change	Page(s) Affected	Approved By
6/10/2009	Original template created	All	Eric Sortor
11/25/2009	Minor revisions made for FY2010 Certification	All	
12/22/2010	Minor revisions made for FY2011 Certification (including updating links for new website, adding BO reports, etc.)	2-4	
12/1/2011	Only minor changes made – added training course name, corrected link for Visa website, corrected link for additional info on BO report, updated location/title of M-Report.	1,2,4	
10/9/2012	Minor changes – My LINC link, note on storing cc numbers policy	1-2	
2/25/2013	Added the review of the new report which shows who has completed the training and the date they completed it.	4	
10/15/2013	Updates for FY14 include new Visa link, new process where units maintain list of authorized users in M-Pathways	1-2	
1/15/15	Review refund activity, Various	All	
11/2016	Updated link and added clarifying language, removed redundancies	1-3	

11/2017	Added link to Merchant Services Policy Document, Updated links, Added clarifying language regarding the storing of credit card numbers, and replaced reference to deleted SPG 519.06 with new SPG 519.01	1-5	
11/2018	Updated links	1 - 3	
11/2019	Added clarifying language and updated links to go to Treasurer's Office/Merchant Services website.	All	
11/2020	Removed M-Reports link, updated with Wolverine Access link	5	
12/2021	Added note about link	1	
12/2022	Updated language	2	
2/2024	Updated language, added notes about Internal Controls Push Reports, added PCI and AOC	1, 2, 4, 6	
12/2024	Updated language, added note per Audit Services	1-5	
11/2025	Updated links per Accessibility Quick Tips, added clarifying language, added vulnerability scanning	All	

Document Owner: Executive Business Services (EBS) and its supported departments
Administrative Owner: Executive Business Services (EBS)