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 Terminals & Payment Applications

APPLIES TO: Receiving, batching, and reconciling credit card transactions where the merchant is using a credit card terminal or payment application (**A U-M employee 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 – Credit Card Terminals & Payment Applications

Activity	Responsible Party	Reference/Comments
KEY ROLES / TRAINING		
The following positions are authorized to process credit card transactions for the departments supported by Executive Business Services (EBS) as determined by the Dept. Administrator.	Department (See Appendix A)	Positions responsible for processing credit card transactions should not perform reconciliation.
The following positions are authorized to approve refunds for EBS and its supported departments as determined by the Dept. Administrator.	Department (See Appendix A)	All refunds should be approved by 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)	
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 credit card transactions or refunds and include 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 and is responsible for knowing the exact street address where any terminal is being housed.

Activity	Responsible Party	Reference/Comments
		See Update Deposit Location and Merchant Information in My LINC for step-by-step process
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 consistent with 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, purchase another terminal, 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:*	Department (See Appendix A)	

Activity	Responsible Party	Reference/Comments
• *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 the merchant account.*		
RECEIVING FUNDS		
The school/college/unit/department may receive funds via credit card for a variety of purposes including (but not limited to): • Goods/services provided • Conference fees • Donor gifts • Tickets	Department (See Appendix A)	***NOTE:*** *Direct submission of gifts to the lockbox by the donor is the preferred method.* ***NOTE:*** *If credit card information for a donor gift is received via mail, it should be delivered to a development drop box, located in the Michigan League and Pierpont Commons.*
Credit card terminals (or computers) are located within the EBS Supported Departments. This location is not accessible to unauthorized individuals because it is housed in a locked office/suite. When **not** in use (e.g., after business hours), terminals are securely stored in a locked office/suite. ***NOTE: If there are any changes to how or where credit cards are being taken due to remote or flexible work locations, merchants should contact Treasurer's Office - Merchant Services (merchantservices@umich.edu) to ensure PCI compliance is maintained and other internal controls are in place.*** ***NOTE: If terminals are taken off-site, they are tracked by merchant via the unit's process to track all university-owned office equipment being used off-site.***	Department (See Appendix A)	Merchant Contact maintains a list of terminal make/model and serial number of credit card equipment with address location including room number. Merchants should control access to terminals as they would a cash box. Merchant Contact instructs staff to inspect the credit card terminal at the beginning of each business cycle for tampering or the addition of non-standard parts (AKA 'skimmer') that could be used to illegally obtain credit card info. Staff should review the vendor's P2PE Instruction Manual (PIM) for more information on protecting credit card terminals. Additional tips can be found under Security Resources for Credit Card Terminals. Contact the Treasurer's Office (see Key Contact section) immediately if there's a concern or issue. Ensure credit card terminals are maintained and serviced per the vendor's P2PE

Activity	Responsible Party	Reference/Comments
		Instruction Manual (PIM), including any additional clarifications to the PIM if provided by the Treasurer's Office.
(Only applicable if the merchant is using a software payment application.) This merchant account is using the following payment application to process transactions: N/A Ensure payment application and version number is PCI Software Security Framework (SSF) compliant on an ongoing basis by verifying their compliance status on the PCI Security Standards Council's Website.	Department (See Appendix A)	Treasurer's Office – Merchant Services should be notified immediately if payment application loses their PCI compliance status.
Only the following positions/individuals have access to information (e.g. reports, merchant copy receipts) 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 (e.g. merchant receipts, batch reports) should have the credit card number properly truncated (i.e. no more than the last four digits visible). ***NOTE:*** *It is against university policy to store more than the last four digits of any credit card number.*
Accept payment via in person	Department (See Appendix A)	Individuals processing credit card transactions should not have any responsibilities related to reconciliation. ***NOTE:*** Before implementing the process to take credit card information over the phone, contact Treasurer's Office – Merchant Services merchantservices@umich.edu to ensure PCI compliance.

Activity	Responsible Party	Reference/Comments
Authorize Transaction: If Card Present: 1. Process card. 2. Make sure customer signs receipt when applicable. Verify signature on the back of the card. If Card Not Present (e.g., mail, phone etc.): 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 for transactions -N/A. Be sure to properly dispose (i.e. shred) of the card-validation code number once the transaction is authorized.	Department (See Appendix A)	Please refer to the user guide provided with your terminal for further instructions on how to authorize a transaction. ***NOTE:*** *It is against university policy and a violation of PCI DSS to store the 3 or 4-digit* ***card-validation code*** *as part of the authorization process. Storing these numbers could result in penalties and fines being issued against the merchant.*
Issue a credit card receipt in the amount of payment/refund to the original card and retain a copy of the receipt. ***NOTE ON REFUNDS:*** *If unable to refund the original credit card (e.g., gift card, account closed), work with SSC's AP to have a check issued.*	Department (See Appendix A)	Copies of sales receipts should be kept for 18 months to satisfy any disputes/chargebacks. After the 18-month period has expired, the sales receipts should be shredded to protect cardholder information. The receipts need to have the credit card number properly truncated (i.e. last four digits).
Obtain approval by a Higher Administrative Authority for all refunds.	EBS Analyst	
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.

Activity	Responsible Party	Reference/Comments
Compare the refund receipt to the original sales receipt to ensure the amount refunded equals the amount of the original transaction and the card refunded is the same as the original card.	Department (See Appendix A)	Cash refunds should not be given for credit card transactions. 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. See Treasurer's Office - Merchant Services Return / Refund Policies for more information.
BATCHING/SETTLEMENT		
At the end of each day, run a batch process/settlement report for each credit processing system. Attach receipts to the batch settlement report and forward to the reconciler.	Department (See Appendix A)	Refer to the user guide provided with the terminal for further instructions on how to batch out transactions.
Compare each settlement report to merchant receipts to ensure all transactions have batched correctly.	Department (See Appendix A)	***NOTE:*** *If using Bluefin terminals, reconcile receipts with data from Payconex.*
Verify all refunds issued are valid and have been approved by EBS Supported Department and proper evidence is maintained.	Department (See Appendix A)	Person approving refunds should not be processing transactions.
Complete the PCI self-assessment questionnaire (SAQ) annually for each merchant account prior to the expiration date using the portal linked in notification emails.	Merchant Contact (See Appendix A)	See PCI Resources on Treasurer's Office – Merchant Services website.
Annually collect applicable PCI documents from supplier(s). Documents include Attestation of Compliance/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	Merchant Contact (See Appendix A)	Treasurer's Office - Merchant Services will contact for copies of documents.

Activity	Responsible Party	Reference/Comments
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.*		
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 SSC to ensure each payment 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.
For discrepancies, contact SSC Reconciliations for assistance.	EBS Analyst	
MONITORING		
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.	Department (See Appendix A)	

Activity	Responsible Party	Reference/Comments
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 appropriate staff are authorized users and have completed TME102 training course.	EBS Director, EBS Analyst, Department (See Appendix A)	Report can be accessed through Wolverine Access > Business Objects at: Home > Folders > Public Folders > UM-Maintained > Financials > FN03 Journal Detail
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	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	

12/1/2011	Minor revisions made – added training course name, corrected link for additional info on BO report, updated location/title of M-Report.	1 & 5	
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.	5	
10/15/2013	Update for FY14 – new process where units maintain list of authorized users in M-Pathways	1	
1/15/15	Review refund activity, Various		
11/2016	Updated link and added clarifying language, removed redundancies, and added info regarding maintaining terminal serial numbers	1-4	
11/2017	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	2, 3, 5, 6	
11/2018	Added clarifying language and updated links	All	
11/2019	Added clarifying language and updated links to go to Treasurer's Office/Merchant Services website.	All	
11/2020	Added Note about changes due to COVID-19, removed M-Reports link, updated with Wolverine Access link	3, 7	
12/2021	Added note to link	1	
12/2022	Updated language	2, 3	
2/2024	Updated language, added notes about Internal Controls Push Reports, added PCI and AOC	1-3, 5, 6, 8	
12/2024	Updated language, added notes per Audit Services, added annual collection of PCI documents	1-8	
11/2025	Updated links per Accessibility Quick Tips, added clarifying language	All	

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