**SECTION**: Treasury

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

**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: Changes for FY2025 are identified in red text**

**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 [insert name of school/college/unit/ department] as determined by the Dept. Administrator. | [insert appropriate person(s)/position(s)] Admin. Accountant, A/R Clerk, Cashier, etc. | Positions responsible for processing credit card transactions should not perform reconciliation. |
| The following positions are authorized to approve refunds for the [insert name of school/college/unit/department] as determined by the Dept. Administrator. | [insert appropriate person(s)/position(s)] Supervisor, Manager, etc. |  |
| Update list of authorized users in M-Pathways > Merchant Information > Authorized Users section. This list should be kept current, in line with staffing changes, and identify all users authorized to process credit card transactions on account. | [insert appropriate person(s)/position(s)]  Merchant Contact | 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 M-Pathways with current authorized users.  ***NOTE:*** *For information on who should be an authorized user and step-by-step instructions see:* [*https://finance.umich.edu/authorized-users*](https://finance.umich.edu/authorized-users) |
| Ensure records of current individuals authorized to approve refunds are up to date and kept on file in unit. See [Treasurer's Office - Merchant Services Return / Refund Policies](https://finance.umich.edu/resource/merchant-tip-month-april-2024) for more information. | [insert appropriate person(s)/position(s)] Supervisor, Manager, etc. |  |
| 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. | [insert appropriate person(s)/position(s)] Department Manager, Accounting Supervisor, Lead Budget Administrator, etc. | 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: <https://finance.umich.edu/finops/controls/Reports>  ***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. | Merchant Contact, Authorized Users | 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](https://its.umich.edu/enterprise/administrative-systems/training/my-linc-overview), search TME102. |
| Use appropriate process/form to modify the merchant contact, address, chartfields, purchase another terminal, terminate an existing account; etc.  ***NOTE:***  *Before any changes to how or where credit cards are being accepted (including remote locations), any changes to vendors or service providers, any changes to phone systems and/or use of call center**systems, and/or any changes to responsibilities, contact Treasurer's Office - Merchant Services (merchantservices@umich.edu) to ensure PCI compliance is maintained and other internal controls are in place.* | Merchant Contact | See the Treasurer’s Office website for appropriate process/form to use: <http://finance.umich.edu/treasury/merchant-services> |
| **RECEIVING FUNDS** |  |  |
| The school/college/unit/department may receive funds via credit card for a variety of purposes including (but not limited to):   * [insert examples that may apply to your school/college/unit/dept.] * Goods/services provided * Conference fees * Donor gifts * Tickets | Merchant Contact | ***NOTE:*** *Direct submission of gifts to the lockbox by the donor is the preferred method.*  ***NOTE:*** *If credit card information is received, it should be delivered to a development drop box, located in the Michigan League and Pierpont Commons.* |
| Credit card terminals (or computers) are located [insert location of credit card terminals when in use]. This location is not accessible to unauthorized individuals because it is [insert description of how terminal is maintained in a secure environment (i.e. in a restricted area, behind a desk, etc.)]  When **not** in use (e.g., after business hours), terminals are securely stored in [insert location of credit card terminals when **not** in use (i.e. safe, locked drawer)]  ***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***](mailto: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 reported to the Treasurer’s Office - Merchant Services at merchantservices@umich.edu and must be tracked by merchant via unit process to track all university-owned equipment being used off-site.*** | Merchant Contact | 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 terminal tampering training located on the Treasurer’s Office website [<http://finance.umich.edu/treasury/merchant-services>](http://www.finance.umich.edu/treasury/merchant-services/merchant-contact-responsibilities). 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 Instruction Manual (PIM), including any additional clarifications to the PIM if provided by the Treasurer's Office. ~~Credit card terminals are only serviced or replaced by Treasurer’s Office staff.~~ ~~Exceptions must be approved by 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: [insert name of payment application and version number].  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](https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html). | Merchant Contact | 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. | [insert appropriate person(s)/position(s)] | 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.*  Refer to the [PCI Security Standard’s Council website](https://www.pcisecuritystandards.org/) or contact the Treasurer’s office at [merchantservices@umich.edu](mailto:merchantservices@umich.edu) for further information on the security requirements. |
| Accept payment via [insert Unit’s detailed processing method] (i.e., in person, mail, phone, etc.) | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | 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](mailto:merchantservices@umich.edu) to ensure PCI compliance. |
| Authorize Transaction:  If Card Present:   1. Process card. 2. Verify signature on the back of the card. Make sure customer signs receipt when applicable.   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 greater than [insert amount]. Be sure to properly dispose (i.e. shred) of the card-validation code number once the transaction is authorized. | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | 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 the original credit card is no longer available (e.g., gift card, account closed), the best practice is to work with SSC's AP to have a check issued. If that is not an option, contact Treasurer’s Office - Merchant Services at* [merchantservices@umich.edu](mailto:merchantservices@umich.edu)*.* | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | 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 level of authority for all refunds. | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. |  |
| Verify all refunds issued are valid and have been approved and proper evidence is maintained. | [insert appropriate person(s)/position(s)] Supervisor, Senior Manager, etc. | All refunds should be approved by a higher-level authority.  Person 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 and the card refunded is the same as the original card.  ***NOTE ON REFUNDS:*** *If the original credit card is no longer available (e.g., gift card, account closed), the best practice is to work with SSC's AP to have a check issued. If that is not an option, contact Treasurer’s Office - Merchant Services at* [merchantservices@umich.edu](mailto:merchantservices@umich.edu)*.* | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | Cash refunds should not be given for credit card transactions, instead work with the SSC to have a check issued. |
| **BATCHING/SETTLEMENT** |  |  |
| At the end of each [insert cycle (i.e. shift, day, etc.], run a batch process/settlement report for each credit processing system. Attach receipts to the batch settlement report and forward to the reconciler. | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | 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. | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | ***NOTE:*** *If using Bluefin terminals, reconcile receipts with data from Payconex.* |
| Verify all refunds issued are valid and have been approved by [insert appropriate person(s)/position(s)] and proper evidence is maintained. | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | Person approving refunds should not be processing transactions. |
| Complete the PCI self-assessment questionnaire annually for each merchant account prior to the expiration date using the CampusGuard portal. | Merchant Contact | See PCI Resources on Treasurer’s Office – Merchant Services website: <https://finance.umich.edu/treasury/merchant-services> |
| 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 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.* | Merchant Contact | Treasurer’s Office - Merchant Services will contact for copies of documents. |
| **RECONCILIATION** |  |  |
| To change chartfields, see Treasurer’s Office - [Merchant Services website](https://finance.umich.edu/resource/merchant-account-change-forms) for process. | [insert appropriate person(s)/position(s)] Merchant Contact | 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 the Treasurer’s Office – Merchant Services website for appropriate process/form to use: <http://finance.umich.edu/treasury/merchant-services> |
| 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.* | [insert appropriate person(s)/position(s)] Unit-level SOA Reconciler | 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](https://ssc.umich.edu/accounting-services/reconciliations/) for assistance. | [insert appropriate person(s)/position(s)] Unit-level SOA Reconciler |  |
| **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. | [insert appropriate person(s)/position(s)] Merchant Contact, Approver, Unit Administrator, etc. |  |
| 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. | [insert appropriate person(s)/position(s)] Merchant Contact, Approver, Unit Administrator, etc. | Report can be accessed through Business Objects at:  UM-Maintained 🡪 Financials 🡪 FN03 Journal Detail  Click [here](https://finance.umich.edu/system/files/CashHandlingBOReports.doc) for additional information regarding the report. |
| 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) | [insert appropriate person(s)/position(s)] Merchant Contact, Approver, Unit Administrator, etc. | Report can be found in M-Reports (go to [Wolverine Access](https://wolverineaccess.umich.edu/collection/all/faculty-staff-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](mailto:merchantservices@umich.edu)  or (734) 763-1299

* [pcicompliance@umich.edu](mailto:pcicompliance@umich.edu)

Related Standard Practice Guides:

* See [SPG 519.01](http://www.spg.umich.edu/policy/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 | [insert name] |
| 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 |  |

Document Owner: [insert name], [insert title]

Administrative Owner: [insert name], [insert title]