**SECTION**: Treasury

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

**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: Changes for FY2022/FY2023/FY2024 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 – Online Credit Card Processing**

| **Activity** | **Responsibility** | **Reference/Comments** |
| --- | --- | --- |
| **KEY ROLES / TRAINING** |  |  |
| 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. |  |
| Ensure record of current individuals authorized to approve refunds is up to date per the procedures on the Treasurer’s Office website: <http://finance.umich.edu/treasury/merchant-services>. | [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.  ~~Update list of authorized users in M-Pathways of any staff changes such as a new staff member who will be processing credit card transactions and/or processing refunds or a staff member who is no longer processing transactions or processing refunds.~~ | [insert appropriate person(s)/position(s)]  Merchant Contact | 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.  ***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) |
| 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> |
| Obtain proper training and certification on an annual basis as part of 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, terminate an existing account; etc.  ***NOTE:*** *Any changes to how or where credit cards are being taken, changes to vendors or service providers, and/or changes to responsibilities should be reported to 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** |  |  |
| This merchant account is processing online and using [insert name of payment gateway provider (e.g. Nelnet, PayPal, Authroize.Net, CyberSource, etc.)] as the payment gateway provider. | Merchant Contact | The merchant must provide the Treasurer’s Office with the name of the payment gateway provider to set up the merchant account.  A screen print of the Visa web page displaying the payment gateway provider should be kept by the merchant. |
| Complete the PCI self-assessment questionnaire annually for each merchant account prior to the expiration date using the Vendor Compliance online tool. | Merchant Contact | See PCI Resources on Treasurer’s Office website: <https://finance.umich.edu/treasury/merchant-services> |
| Annually, obtain a copy of the Attestation of Compliance (AOC) for all third-party vendors/service providers. This AOC must: cover the relevant solution being used by the merchant, be current, and be signed by a Qualified Security Assessor (QSA). If an appropriate AOC cannot be provided, the vendor's PCI compliance must be reviewed and approved by the Treasurer's Office.  ***NOTE:*** *If using Bluefin, Authorize.net, and Nelnet as part of their solution provider, verify AOC with Merchant Services (as these third-party vendor contracts are held by Treasury).* | Merchant Contact |  |
| The school/college/unit/department may receive funds via online credit card payment 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 |  |
| Only the following positions/individuals have access to information (e.g. reports) containing cardholder data. | [insert appropriate person(s)/position(s)] | Credit card and personal information should be safeguarded in a manner consistent with PCI standards 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.*  Refer to the PCI Security Standard’s Council website for Merchant Resources: https://www.pcisecuritystandards.org/merchants/ or contact the Treasurer’s office at [merchantservices@umich.edu](mailto:merchantservices@umich.edu) for further information on the security requirements. |
| Obtain approval by a higher level of authority for all refunds. | [insert appropriate person(s)/position(s)] A/R Clerk, Cashier, etc. | All refunds need to be reviewed and approved by a higher level of authority.  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. |
| Compare the amount refunded to the original sales transaction to ensure the amount refunded equals the amount of the original transaction.  ***NOTE:*** *If the original credit card is no longer available (e.g., gift card, account closed), the best practice is to work with the Shared Service Center Accounts Payable department to have a check issued. If that is not an option, contact 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. |
| **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. | [insert appropriate person(s)/position(s)]A/R Clerk, Cashier, etc. | 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 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 refunds. |
| **RECONCILIATION** |  |  |
| To change chartfields, see [Merchant Services website](https://finance.umich.edu/resource/merchant-account-change-forms) for process. | ~~Department Manager~~  [insert appropriate person(s)/position(s)] Merchant Contact | 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 the Treasurer’s Office 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 or perform batch process. |
| For discrepancies, contact the [SSC Reconciliations](http://ssc.umich.edu/accounting-services/reconciliations/) for assistance. | [insert appropriate person(s)/position(s)]Unit-level SOA Reconciler |  |
| **MONITORING** |  |  |
| Monitor payment gateway reports to ensure that 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 authorized users are appropriate and have completed the 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)] 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

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 | 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 MPathways | 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 | 1-4 |  |

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

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