Cash Handling: Credit Cards

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

Since SMTD credit card transactions are primarily handled through our various web-based systems, only designated Office Coordinator(s) in the SMTD are authorized to receive and process credit card transactions as determined by the CAO, Christian Rafidi cerafidi@umich.edu. **For the concession stand and mobile credit card processors, the position responsible for processing credit card transactions is not performing reconciliation**. Our authorized Credit Card Handlers, staff who have been designated to receive and process credit card transactions from faculty, staff, students, and vendors, are:

Credit Card Handlers by Department

- UProd: Diane Widzinski diannwid@umich.edu
- Dance: Mary Cole mcole@umich.edu
- Michigan Marching Band: Patricia Dawson pdawson@umich.edu
- Men's Glee Club: Kyle Butler ksbutler@umich.edu

Credit Card Handlers: Key Roles and Training

SMTD may receive credit card payments for a variety of purposes including, but not limited to event fees, program fees, conference fees, donor gifts, and tickets, etc. Credit card handlers are responsible for processing credit card transactions and **should not** perform reconciliation.

- All authorized credit card handlers must obtain training and certification on an **annual basis** by successfully completing the MyLinc TME102 training course.
    - Positions responsible for processing credit card transactions **are not** performing reconciliation.
    - The Financial Manager will periodically review the CMB Treasurer's Office Certification Courses Report to monitor individuals who have taken the TME102 course.
- Access to credit card terminals and credit card data is limited to individuals with a business purpose for accessing them.
    - Handlers must ensure that all terminals are safeguarded and accounted for. All credit card terminals are located in an area that is not accessible by unauthorized individuals and when not in use are stored in a secure place such as a safe or a locked drawer, and are not left out overnight.

- Monitor handling of confidential credit card information. **It is against University policy to store the full sixteen digit credit card number via email, text message or campus mail or any format.** These are NOT secure forms of delivery/storage.
    - Credit card data must **NEVER** be stored electronically in **ANY** form.
    - If received via email, you must send a new email to sender indicating that you cannot accept the credit card number by email and to provide it in an acceptable method. (SMTD credit card transactions are primarily through web-based systems).
    - You must permanently delete all instances of emails containing the card number.
    - You must also inform your supervisor of the instance.
    - For hard-copy records destroy by cross-cut shredding, incinerating, or pulp the records.
    - Refer to the Payment Card Industry Data Security Standard or contact the Treasurer's office at merchantservices@umich.edu for further information on the security requirements.
- When a unit receives gifts via credit card, the unit must forward (via drop box) the credit card information or check to the **Gifts and Records Administration** Team along with the proper form and supporting documentation to process gifts.
    - Direct submission of gifts to the lockbox by the donor is the preferred method.
- Handlers should process credit card transactions through the approved methods, which are online forms filled out by the cardholder or credit card terminals.
    - For example: Credit Card handlers **should not** process online credit card transactions when the customer calls and says they do not have access to a PC and asks the handler to enter their credit card info through a webpage on their behalf.
- Handlers should monitor the credit card terminal for tampering or the addition of non-standard parts (AKA 'skimmer') that could pass credit card information to others. Inspect the credit card terminal / PC daily for anything out of the ordinary and contact the Treasurer's Office immediately if an issue is identified.

Authorized Users: Roles and Responsibilities

SMTD may receive credit card payments for a variety of purposes including, but not limited to event fees, program fees, conference fees, donor gifts, and tickets, etc. Authorized Users are responsible for ensuring individual transactions are valid and at the expected amounts.

Authorized Users by Department:

- YAP: Sarah Rau

- YAP: Robin Myrick
- YAP: Emily Lamoreaux
- Music: Jeanette Bierkamp
- Music: Megan McClure
- Admissions: Emily Smokovich
- Ensembles: Paul Feeny
- Music Education: Kelley Archer
- PPLP: Aya Hagelthorn
- PPLP: Mary Ann Stock
- MGC: Patrick Kiessling
- MMB: Maggie St. Clair
- UProd: Fatima Abdullah
- Dance: Katie Gunning

Authorized Users: Key roles and training:

- All authorized users must obtain training and certification on an **annual basis** by successfully completing the MyLinc TME102 training course.
- Authorized users have access to information (e.g. reports) containing cardholder data.
    - Credit card and personal information should be safeguarded in a manner consistent with Payment Card Industry, PCI, standards.
    - All reports provided by the payment gateway provider (Nelnet or Authorize.net), should have the credit card number properly truncated (i.e. delete the first eight digits, only the last four or less visible).
    - Reports will either be pushed (via email or through the online system) to the Authorized users or the Authorized user may export reporting as needed.
    - For hard-copy records destroy by cross-cut shredding, incinerating, or pulp the records.
    - Refer to the Payment Card Industry Data Security Standard or contact the Treasurer's office at merchantservices@umich.edu for further information on the security requirements.
- The Authorized user will ensure individual transactions that batched are valid and that the amounts were processed correctly.
    - This should be performed on a daily, but no less than weekly, basis by comparing the point of sale / inventory records / expected amounts to the credit card transaction.
    - Discrepancies must be resolved on a timely basis.
    - Contact the Merchant Contact/Financial Manager for assistance.

- Authorized users when contacted for a refund must confirm accuracy of the refund and ensure that final approval is given by a higher level of authority (this is the Merchant Contact/Financial Manger).
    - All payment gateway providers, like online systems Nelnet and Authorize.net, should have controls in place to trace a refund to an individual.
    - The refund should be no more than the amount of the original transaction.
- Authorized users will compare the amount refunded to the original sales transaction to ensure the amount refunded equals the amount of the original transaction.
    - 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 or if the cardholder no longer has the original credit card used to make the purchase. Amount is **NOT** refunded to a different card.
- Authorized user will send transaction information to the Merchant Contact/Financial Manager for approval and for the Merchant Contact to issue the refund reimbursement.
    - A credit card receipt may be issued in the amount of payment / refund and a copy of the receipt is kept for each transaction for 18 months.
- Authorized user will annually complete the Internal Controls Gap Analysis certifying that their department is compliant with all of the Cash Handling responsibilities.

Merchant Contact: Key Roles/Responsibilities

- Serve as department merchant activities coordinator and as point person for the Treasurer's Office.
- This merchant account is processing online and using (e.g. Nelnet, PayPal, Authorize.net, etc.) as the payment gateway provider.
- Serve as the person who completes the annual self-assessment questionnaire for PCI (Payment Card Industry) compliance through the 3rd party company, Trustwave and ensures PCI compliance at all times.
    - Merchant contact successfully completes the PCI self-assessment questionnaire annually for each merchant account prior to the expiration date using the Trustwave online tool.
- Successful completion of UM My LINC Merchant Certification TME102 Course annually by:
    - You
    - All applicable staff
        - New and existing staff who are authorized to process credit cards or refunds

        - Any staff who do not process credit cards but come into contact with credit card data (i.e., full 16 digits of credit cards). For example, a person who opens the mail where credit card data is present.
    - Read and follow the SPG policies and Merchant policies (e.g. Merchant Services Policy Document which govern credit card activities.
        - Review annually
    - Prepare (and update when necessary) departmental Internal Controls Written Procedures which also includes:
        - Segregation of Duties
        - Review of Daily Transaction Activity
        - Controlled Access to Resources
        - Supervision
        - Verification
        - Documentation
    - Annually complete the Internal Controls Gap Analysis.
    - Merchant Contact must maintain a list of credit card terminal(s) make/model and serial numbers and update as replaced.
- The Merchant Contact maintains a listing of all personnel who are authorized to process credit card transactions and approve refunds in MPathways and updates it with any staff changes before a new staff member processes any credit transactions.
        - **All refunds must be approved by a higher level of authority.**
        - The person verifying refunds is not processing transactions or running batches/settlement reports.
    - Train all departmental staff on processing credit card transactions and refunds if applicable.
        - Merchant Contact is responsible to ensure all authorized users have been properly trained (MyLinc course TME102) prior to processing transactions
            - Review the CMB Treasurer's Office Certification Courses Report in Business Objects.
    - Update the "Authorized Users" in the Merchant Information page of MPathways Financial & Physical Resources System (FINPROD) whenever authorized user staff changes.
        - An authorized user is anyone who handles cardholder data (i.e. the full '16 digit' credit card number) or issues credit card refunds.
            - You will receive an ITS email when you have been granted this MPathways access.
            - Updating Authorized Users instructions are listed on pages 3 and 4.

    - Merchant updates 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.
        - A staff member who is no longer processing transactions or approving refunds.
- Update the merchant contact and Merchant Policy document signers with personnel changes.
- Always contact merchantservices@umich.edu if you suspect or identify a credit card data loss/breach.
- The merchant contact must provide the Treasurer's Office (via the New Registration Form) with the name of the payment gateway provider when setting up the merchant account.
- It is critical to monitor the compliance status of the payment gateway provider's expiration date listed on Visa's website.
    - If the payment gateway provider is no longer listed, immediately notify the Treasurer's office.
- If accepting payments online, payment gateway is monitored (via the Visa website at http://www.visa.com/splisting/) on an ongoing basis to ensure they are PCI DSS compliant.
    - Notify Treasurer's Office immediately if payment gateway loses their PCI compliance status. (Online)
- Merchants who use PC software or a cash register to process credit cards, verify that it is PA DSS compliant (via the PCI Security Standard Council's website at https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html) on an ongoing basis. Notify Treasurer's Office immediately if company loses its compliance status.
- Merchants who use a website (ecommerce) to process credit cards, verify PCI Level One compliance (on Visa's vendor listing at http://www.visa.com/splisting/searchGrsp.do) on an ongoing basis.
- Use a Merchant Change/Termination Form to change the merchant contact, address, chartfields, buy another terminal, terminate the existing merchant account, etc.
    - If merchants intend to change their processing method they must establish a new merchant account number. Completed new Merchant Registration Form (Internet Merchant version) and Merchant Services Policy document are both sent to the Treasurer's Office.

- Review 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

For Merchants Who Utilize Credit Card Terminals

- Maintain a list of your terminal make(s), model(s), serial number(s), and location(s).
    - List must be updated when terminal is replaced or relocated. The serial number is located on the underside of the terminal.
    - Terminal data is maintained in MPathways - FINPROD. Required list can be verified here and printed instead of manually creating a list. FINPROD discrepancies are reported to merchantservices@umich.edu.
- Ensure that all staff processing credit cards be trained on terminal tampering.
    - Merchant contact instructs staff to monitor credit card terminal tampering or the addition of non-standard parts (AKA 'skimmer') that could pass credit card information to others. Staff inspects the credit card terminal / PC daily for anything out of the ordinary and contacts the Treasurer's Office immediately if an issue is identified.
- Inform staff that only Treasury Office staff can repair or replace terminals.

Merchants Batching/Settlement

- At the end of each business cycle / shift, a credit card terminal batch process is run and the stored transactions are transmitted to the bank, the receipts are attached to the batch settlement report and forwarded to the reconciler.
- Using the reporting tools from your gateway provider (**Nelnet or Authorize.net**) to ensure all transactions have batched correctly.
    - 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 the Merchant Contact and proper evidence is maintained.
    - Person approving refunds **should not** be processing refunds.
    - If the 3 digit (4 digits for Amex) Card-Validation Code is obtained as part of the authorization process, immediately destroy it after valid transaction.

- Storing this number would be a violation of PCI DSS and could result in penalties and fines being issued against the merchant.

Reconciliation:

Reconciliation **should not** be performed by the individual responsible for processing credit card transactions, Credit Card Handlers.

- The Merchant Contact will ensure individual transactions that batched are valid and amounts were processed correctly on a daily basis, weekly at a minimum, by comparing to the point of sale / inventory records / expected amounts. Discrepancies will be resolved on a timely basis.
  - Person reviewing the refunds should not process transactions or perform batch process.
  - For discrepancies, contact Financial Operations for assistance.
- The Merchant Contact will review all refund activity to ensure all refunds are valid and authorized.
  - Proper evidence of reconciliation will be maintained.
  - Refund activity can be found on the Credit Card Controls report in MReports under the Compliance tab.

Monitoring & Oversight:

- The CAO and/ or Financial Manager will review merchant account and subsequent changes, and chartfield allocations to ensure each payment is posted to the correct G/L account.
- To change chartfields, complete the Change/Termination Form (which is provided by Treasury) with the appropriate updates.
  - Forward the completed form to the Treasurer's Office.
- The CAO and/ or Financial Manager will monitor payment gateway reports to ensure that all refunds were approved by a higher level authority.
- Daily batch receipts/Settlement reports are monitored by the Financial Manager to ensure that all credit transactions were performed by authorized personnel, and all refunds were approved by a higher level of authority.
- The CAO and/ or Financial Manager will review the standard Cash Handling report provided in M-Reports or the FN03 Jrnl Detail Merchant Management report to monitor the following:
  - All merchants in unit and their activity
  - All merchants PCI compliance status (for the past 12 months)

- Sales and refund activity