**University of Michigan**

**Merchant Requirements for the Acceptance of Credit Cards**

# Purpose

The University of Michigan’s Merchant Requirements support the safe and secure acceptance of credit cards by university units. These requirements are intended to prevent fraud and ensure the university’s compliance obligations to secure sensitive customer credit card information. Failure to protect customer credit card information may result in financial loss for the university unit, suspension of credit card processing privileges, fines, and damage to the reputation of the unit and potentially to U-M more generally.

# Scope/Audience

The Merchant Requirements apply to all units that accept credit cards as a form of payment, including those in Michigan Medicine, U-M Dearborn, and U-M Flint.

# Authority

As delegated by the Executive Vice President and Chief Financial Officer (EVPCFO) under Regental Bylaw 3.01 and detailed in [Delegation of Authority (SPG 601.24](https://spg.umich.edu/policy/601.24)) and [Treasury Services (SPG 519.01](https://spg.umich.edu/policy/519.01)) policies, the Treasurer has overall responsibility for the administration and oversight of all banking services, including credit card services.

The university uses a centralized approach for its Treasury Services. In order to maintain compliance with existing contracts and consistency in practice, no individual or unit has the authority to accept credit cards as a form of payment without the approval of the Treasurer’s Office.

# Overview

The Treasurer’s Office provides a number of different options for units (merchants) to use when accepting credit card payments. Contact merchantservices@umich.edu for current options.

A *Merchant* is defined as a unit or other university entity that accepts credit card payments. The Treasurer’s Office is responsible for setting up and managing merchant accounts and acts as the single point of contact between the university’s credit card processor (merchant acquirer or bank) and U-M. The Shared Services Center (SSC) is responsible for the proper recording of credit card activity in the university’s general ledger.

Units must first receive approval from the Treasurer’s Office if they wish to become a merchant. The approval process also requires the unit’s [higher administrative authority](https://teamdynamix.umich.edu/TDClient/68/Portal/KB/ArticleDet?ID=8560) to review and understand the requirements outlined in this document and approve a separate U-M merchant application asserting that their department will abide by this policy.

Additionally, a departmental management person for the unit will need to be appointed by the higher administrative authority as the merchant contact. The merchant contact is responsible for ensuring all requirements presented in this document and associated documents are followed and acts as the primary contact for the merchant account.

Net sales and fees are automatically posted to the unit’s Chartfields. The merchant is responsible for all fees related to processing credit card transactions, such as interchange and transaction fees assigned by the card brands (e.g., Visa, MasterCard, American Express, and Discover) and merchant bank. Additionally, the Treasurer’s Office assesses an additional 20 basis points administrative fee on sales to offset the administrative costs of the Merchant Program.

# Requirements

This section outlines the university requirements that units must follow when they become a merchant. It is broken down into four elements:

1) Payment Card Industry Data Security Standard (PCI DSS) Compliance

2) Internal Controls

3) Bank Card Rules

4) Other Responsibilities

The authority to interpret these requirements rests with the Treasurer’s Office and may be updated as deemed necessary.

## Payment Card Industry Data Security Standard (PCI DSS) Compliance

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies (card brands): VISA, MasterCard, Discover, American Express, and JCB to be a baseline of compliance/security. The objective of the PCI DSS is to reduce breaches involving credit card data. These security requirements evolve over time and apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment.

The PCI DSS is enforced through contract law. Part of the merchant agreement that authorizes credit card acceptance includes the responsibility to protect the card data received. A data security breach that stems from a gap in PCI compliance by the merchant or their service provider(s) is a breach of the contract between the merchant and the card brands. The resulting reputational and financial impacts can be severe. From a financial perspective, consequences for non-compliance and/or having a breach of cardholder data can include merchant fines of up to $500,000 per cardbrand and additional monthly fines thereafter until compliance is achieved. These fines are in addition to any legal and investigative costs incurred by the merchant following a breach.

Consequently, university departments that accept credit card payments must maintain compliance at all times with the entire PCI DSS and must follow the [university data security standards](https://it.umich.edu/information-technology-policies/general-policies/#standards). Merchants who fail to maintain compliance with the PCI DSS will have their merchant account inactivated and will not be able to accept credit card payments. A detailed list of PCI DSS requirements is located on the [PCI Security Standards Council website](https://www.pcisecuritystandards.org).

Key University PCI Requirements

The following is a summary of the most significant PCI requirements that are particularly relevant to a department’s decision to accept credit card payments:

* Merchantsmust timely validate compliance with the PCI DSS at least annually. The validation process may consist of the unit completing a self-assessment and/or having an audit performed of its credit card processing environment, which could include passing vulnerability scanning, pen tests and/or other requirements.
* Prior approval from the Treasurer’s Office must be obtained to use any services related to credit card processing (e.g., vendors, point of sale systems, etc.) that are independent of those services authorized by the Treasurer’s Office.
* Agreements with third party vendors must be approved by Procurement Services and include language that addresses the vendor’s and merchant’s responsibilities regarding PCI DSS compliance. Merchants using third parties that are considered in scope for PCI must at least annually obtain satisfactory evidence of these vendors' PCI DSS compliance. Evidence includes producing a valid Attestation of Compliance for Self-Assessment D-Service Provider (AOC for SAQ D-SP), which has been signed by a qualified security assessor (QSA) within the last 12 months. In addition, evidence includes producing a responsibility matrix along and credit card data flow diagram(s).
* The merchant contact and departmental staff who are involved in the acceptance of credit card payments must complete a U-M annual certification course (My LINC TME102). Those who accept credit cards with a device must review anti-tampering training at least annually.
* Storage of sensitive cardholder data[[1]](#footnote-1) in any media format is prohibited.
* Cardholder data cannot be sent or transmitted in an insecure manner:
	+ Cardholder data received via end-user messaging technologies (e.g., email, instant messaging, SMS, chat, etc.) should never be used to process payments.
	+ Fax machines used to accept cardholder data must be single purpose (i.e., dedicated) and connected to an analog phone line. Using multi-function devices that fax/print/copy to accept, send, or replicate cardholder data is not acceptable.
	+ Credit card data can only be taken by phone if using approved Treasury devices (currently approved devices are: [Zoom desksets with restrictions, business-use only “dumb” cell phones, etc.](https://www.google.com/url?q=https://finance.umich.edu/sites/default/files/2024-01/letter%2520from%2520Treasurer%2520to%2520Campus%2520regarding%2520PCI%2520and%2520Zoom%2520Phone_0.pdf&sa=D&source=docs&ust=1720535281123120&usg=AOvVaw3-Pfafn0rUOv1DlRnokOH_)).

For more specifics about accepting credit cards and the responsibilities of merchant contacts, see [How to Start Accepting Credit Cards](http://finance.umich.edu/treasury/merchant-services/credit-cards/how-to-start-accepting-credit-cards) and [Merchant Contact Responsibilities](http://finance.umich.edu/treasury/merchant-services/merchant-contact-responsibilities).

Contact the Treasurer's Office at merchantservices@umich.edu before processing credit card transactions ***outside*** of a U-M facility (e.g., working remotely). In addition, see [Off Campus Use of U-M Property](https://teamdynamix.umich.edu/TDClient/68/Portal/KB/ArticleDet?ID=8890).

### Incident Response

An incident is defined as a suspected or confirmed data compromise and falls under [Information Security Incident Reporting (SPG 601.25)](https://spg.umich.edu/policy/601.25). A data compromise is any situation where there has been unauthorized access to cardholder data. A data compromise can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data. If merchants experience or suspect a breach involving their merchant account, they must immediately send an email to the Treasurer’s Office at merchantservices@umich.edu with full details of the situation.

## 2) Internal Controls

Internal controls, per [SPG 500.01](https://spg.umich.edu/policy/500.01), provide important benefits to your unit and to the university by improving the quality of accounting information and reducing the possibility of mismanagement, error, and fraud.

Safeguarding

Units are responsible for protecting the credit card environment (CDE). This includes protecting customer credit card information and the equipment used to process credit card payments, as well as monitoring user access to any third party online portals and systems which may be used for processing and/or reporting. Access to these systems must be based on a business need, revoked immediately when the need ends, and audited annually. Maintain a current list of all system users, including what role/access level they have within the system and especially denoting those users who have the ability to process refunds through these systems. See [SPG 601.27](https://spg.umich.edu/policy/601.27) and [ITS Info Security Requirements](https://safecomputing.umich.edu/information-security-requirements).

### Separation of Duties

Separation of duties is a coordinated system of checks and balances in which tasks necessary to complete a transaction either are performed by different individuals (two or more individuals working in concert) or an independent review of the tasks. Units should ensure proper separation of duties of all credit card activity, such as processing, approving and reviewing credit card transactions and refunds.

### Reconciliation

It is the responsibility of the unit to perform the proper monitoring and reconciliation steps to validate the merchant activity is appropriate.

Refer to the [Office of Internal Controls](https://finance.umich.edu/finops/controls) website for additional resources such as: gap analysis tools, written procedure templates, and management oversight reports. A monthly report can be issued to help highlight certain aspects of a merchant's PCI DSS compliance status. See [Push Notifications](https://finance.umich.edu/finops/controls/Reports) for more information.

## 3) Bank Card Merchant Rules and Regulations

All merchants must abide by the “Bank Card Merchant Rules and Regulations.” A copy of these requirements is located on the [Treasurer’s Office Merchant Services website](http://www.finance.umich.edu/treasury/merchant-services).

## 4) Other Responsibilities

Tax Liability

Refer to the U-M Tax Department to ascertain if the intended credit card sales will be taxable.

### Change/Termination

The Treasurer’s Office must be notified prior to making any changes to the merchant account, such as the merchant name, contact information, or processing method. Additionally, the Treasurer’s Office must be notified in the event the unit decides to terminate the merchant account.

### PCards

Merchants are allowed to accept Purchasing Cards (PCards) from organizations not affiliated with the university. However, they should not process University of Michigan issued PCards. For additional information regarding PCard policies, please contact Procurement Services.

# Revisions/Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor / Author | Notes |
| 06/30/2020 | 1.0 | M. Deseck | Released Version |
| 5/25/24 | 1.1 | D. Doyle | Multiple updates |
|  |  |  |  |

Date Issued: 06/30/2020

Last Updated: 07/31/2024

Next Review Date: 07/31/2028

Applies To:

All university units or affiliates that accept credit card payments.

Owner:

Treasurer’s Office

1. At a minimum, cardholder data consists of the 16-digit credit card number. Cardholder data may also appear in the form of the credit card number plus any of the following: cardholder name, card security code, PIN, and information on the magnetic stripe (track 1 & 2 data). [↑](#footnote-ref-1)