Payment Card Processing Policy at the University of St. Thomas

Policy number: 800-BA-11
Policy owner: Business Office

Date of initial publication: June 30, 2009
Date of latest revision: December 20. 2022

SECTION I. PURPOSE

This policy is intended to create and maintain a secure environment for acceptance and processing of payment (“credit/debit”) card information at the University of St. Thomas (“University” or “St. Thomas”). The University of St. Thomas is committed to maintaining a secure environment for the acceptance and processing of payment card transactions. The following guidelines have been established in accordance with the Payment Card Industry Data Security Standards (“PCI DSS”), as well as other applicable laws, regulations, and/or contractual agreements.

SECTION II. SCOPE AND APPLICABILITY

This policy governs all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment card account processing — including merchants, processors, acquirers, issuers, and other service providers on behalf of the University. Every employee, regardless of status as student, contract, regular, FTE, volunteer, or other, is responsible for adhering to these guidelines. All departments handling payment card data must also comply with the PCI DSS.

SECTION III. DEFINITIONS

When used in this policy, the following terms have the following meanings:

a. ***Acquirer*** – Also referred to as “acquiring bank,” or “acquiring financial institution.” Entity that issues merchant accounts for St. Thomas; JP Morgan Chase is the designated acquirer for the University.

b. ***Attestation of Compliance (AOC)* –** A declaration of an organization’s compliance with PCI DSS. Assessment is completed by either a Qualified Security Assessor (QSA) or internally by the merchant, resulting in either a Report on Compliance (ROC), AOC, or both.

c. ***Campus Merchant* –** A department or operating area that has been approved to accept and process payment card transactions and has been assigned a merchant identification number. Campus merchants are fully responsible for their merchant account and related PCI DSS compliance.

d. ***Card Association* –** Organization owned by financial institutions that licenses bank credit card programs. Two of the most prominent are VISA and MasterCard.

e. ***Cardholder Data (CHD)* -** At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

f. ***Cardholder Data Environment* (*CDE)* -** The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data**.**

g. ***Information Security* -** Protection of information to ensure confidentiality, integrity, and availability.

h. ***Issuing Bank* –** The bank that provides the customer with a payment card. There are over 40,000 issuing banks in the U.S.

i. ***Merchant Identification Number (MID)* -** A merchant identification number (MID) is a unique identifier assigned to the Campus Merchant by the acquiring bank; also referred to as the merchant account.

j. ***PCI* -** Acronym for "Payment Card Industry."

k. ***SAQ* -** Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment.

l. ***Sensitive Authentication Data (SAD)* -** • Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

m. ***Third Party Processors* -** Companies that accept and receive credit and debit card payments on behalf of your business.

SECTION IV.

A. Approval Required for Payment Card Acceptance

Prior to any entering into any contracts, agreements, or purchases that include the processing of payment card data or transactions on behalf of St. Thomas, the proposed equipment, software, application, system, and/or third-party vendor solution must be reviewed and approved by the Business Office and meet the ITS Standards for Payment Card Acceptance at St. Thomas. University departments are prohibited from setting up their own banking relationships for processing payment transactions.

B. Merchant Identification Numbers

A merchant identification number ("MID") is required for processing payment card transactions. The MID is issued by St. Thomas' Acquiring Financial Institution and all individual numbers will fall under the greater University of St. Thomas umbrella.

To apply for a MID, the department must contact the Director of the Business Office. Due to the expense and liability of accepting card payments, a determination will be made as to whether the benefits of card acceptance exceed the liabilities. If it is determined that the requesting department should receive a MID, the department will work with staff from the Business Office to set-up the new account with the Acquiring Financial Institution.

Departments that are approved for a merchant account to process payment card transactions are considered campus merchants. Campus merchants are responsible for all costs associated with processing payment card transactions. Additionally, each campus merchant must designate at least one individual responsible for PCI DSS compliance oversight and other related merchant account issues. This individual is responsible for completing the appropriate Self-Assessment Questionnaire (SAQ), along with all of the supporting documentation related to their payment processing account annually, as per PCI requirements for compliance.

C. Third Party Processors

All campus merchants at the University must use the approved third-party vendor/service provider for processing payment card transactions. The University has established partnerships with an Acquiring Financial Institution and designated payment gateway providers. Should the functionality provided by these preferred vendors not meet the needs of the campus merchant, a request must be made, and approval obtained to use a different third-party vendor; requests should be submitted to the Director of the Business Office for review. If there are significant costs or effort required to bring a new payment card system into PCI compliance, or the new system would require a change in the University's PCI level or status, approval of the CFO and CIO will be required.

All third-party vendors must be PCI DSS compliant, meeting the requirements of the PCI Software Security Framework ("SSF") and acknowledge their security responsibility as a contractual requirement. The third-party vendor should:

- Be recognized on the PCI SSC lists of Validated Payment Software and/or Secure SLC Qualified Vendors (as of October 2022)
- Previous to October 2022, vendors should be listed on the applicable PCI PA-DSS List of Validated Payment Applications, List of PCI Approved PTS Devices, and/or List of PCI P2PE Solutions
- As applicable, be listed on:
    - MasterCard's List of Compliant Service Providers
    - Visa's Global Registry of Service Providers
- Provide St. Thomas a copy of their PCI DSS Attestation of Compliance
- Employ point-to-point encryption (P2PE) and tokenization to protect payment card data

D. Payment Card Data

Under no circumstances should email ever be used to relay payment card information! If payment card information is provided via email, even though unsolicited, do not retain or process the payment card transaction.

It is highly recommended that, whenever possible, payment card transactions be handled completely electronically through an approved secure payment application processor. For security purposes it is always best when the cardholder is able to enter their own information directly into the payment application. However, it is recognized that an online option is not always available. Therefore, the following guidelines must be adhered to when handling physical payment card data:

- Physical payment card data must be locked in a secure area when it is not of immediate use for processing
- Access to physical payment card data should be restricted on a 'need to know' basis
- Only essential information should be stored
- Never store the three-digit card validation code printed on the signature panel of a payment card (referred to as CAV2, CID, CVC2, or CVV2)
- Sensitive payment card data should never be kept electronically in a spreadsheet, text document, or other similar electronic file

- Sensitive payment card data should never be downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers, or mobile phones
- Payment card data should be retained only for the time necessary to process.
- When payment card data is no longer needed, it should immediately be destroyed using a cross-cut shredder
- All payment card receipts must display truncated payment card numbers only
- Appropriate segregation of duties shall be maintained between payment card processing, the processing of refunds, and the reconciliation function. Secondary approval for all refunds must be obtained.
- Wireless networks will not be used for any payment card administration unless it has been approved by the ITS security team.
- Fax machines should not be used to transmit payment card information.

E. Employees Responsible for Payment Card Processing

For employees who will participate in any part of the payment card acceptance process, the following shall apply:

- Potential employees will be screened during the hiring process by completing a background check
- Employees must successfully complete the online PCI training module annually to review policies, procedures, updates, and best practices.

F. Requirements

All transactions that involve the transfer of payment card information must be processed on systems approved by the University's PCI Council, adhere to ITS's Standards for Payment Card Acceptance, and signed-off by the University's CFO.

Any University department that collects credit card information must have security controls in place that comply with the Payment Card Industry Data Security Standard ("PCI DSS"). These security controls for campus merchants include, but are not limited to the following:

- Must use P2PE encryption if transmitting payment card information in person or over the phone.
- Encrypt and protect cardholder data when either stored or transmitted.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Do not store sensitive authentication data and limit cardholder data retention.
- Protect systems and networks and be prepared to respond to a system breach.
- Secure payment applications.
- Monitor and control access to your systems.
- Complete compliance efforts (policies, procedures and processes), and ensure all controls are in place.

- Maintain an information security policy that addresses security controls and procedures.

G. Administration and Enforcement

The University of St. Thomas Business Office, in conjunction with ITS and other members of the University's PCI Council, is responsible for oversight of the Payment Card Processing Program at the University. Issues, questions, concerns, or requests should be directed to the Director of the Business Office. The Director of the Business Office and Chief Information Security Officer should be contacted immediately if a breach in data security is suspected, and all parties need to follow the Credit Card Security Incident Response Plan (IRP).

The Business Office and ITS reserve the right to perform both annual audits and unannounced audits of campus merchants. Full compliance with these requests is expected.

Failure to follow the guidelines established within this document will result, at a minimum, in the suspension of privileges to accept payment cards. Major violations of this policy by campus merchants could result in (but not limited to) fines by the card providers, restitution for any resulting damages, and damage to the reputation of the University of St. Thomas.