21.01.02.C0.01 Credit Card Collections

Revised: September 21, 2026
Next Scheduled Review: September 21, 2031
Revision History

Procedure Summary

Texas A&M University-Corpus Christi (TAMU-CC) offers university departments the convenience of accepting credit cards as payment for goods and services provided. Departments may accept credit card payments over the counter, over the telephone, or over the internet. This procedure documents proper processing procedures, necessary training, appropriate physical storage, and authorized access to credit card data. Additional information for processing online payments is outlined in university procedure *21.01.02.C0.02, Online Payments*.

Definitions

Merchant Accounts: These are special bank accounts issued by a merchant processing bank (also called a credit card processor) that allow a business to accept credit, debit, gift, and other payment cards. University departments or offices with such accounts are hereafter referred to as "Merchants".

Merchant Level: This classification is based on transaction volume. Merchants are given ranks of Levels 1 through 4, with Level 1 being the highest-volume merchants subject to higher security risk. Any merchant that suffers a credit card data security breach, regardless of transaction volume, is automatically elevated to Level 1. Most merchants at TAMU-CC are Level 4.

Payment Card Industry Data Security Standards: Payment Card Industry Data Security Standards (PCI DSS) are the set of industry protocols by which cardholder processes and systems need to comply. These standards were created by the Payment Card Industry Security Standards Council for the purpose of safeguarding sensitive cardholder data. The precise security measures required by a department will vary depending on how credit cards are accepted (in person, over the phone, or on the internet) but all are covered in the PCI DSS.

Program Fees: These are monthly fees assessed based on the merchant's total monthly net credit card sales.

Point of Sale (POS) Software: A computerized network operated by a main computer and

linked to several checkout terminals used to analyze inventory levels on an item-by-item basis and to record sales and transactions including credit card transactions.

Marketplace U Store: This is a self-contained online store that allows university departments to create a store front, establish store- or department-specific settings, and perform all online store activity such as order fulfillment and reporting. It is a Payment Card Industry (PCI) compliant way to take online payments.

Marketplace U Pay: This is a payment application that utilizes an existing business application or website but provides a PCI compliant way for a user to take online payments. U-Pay focuses on payment collection and reporting.

Procedure

1. PROCESSES

1.1. ESTABLISHING NEW MERCHANT ACCOUNTS

1.1.1. Merchant Accounts must be in place before credit cards may be accepted. Accounts can be revoked for failure to comply with credit card processor guidelines. Departments that accept credit cards must fill out the New Credit Card Merchant Service Request Form (see Appendix section below) and submit it via email to Financial Services. Each department is required to provide Financial Services an account number to which charge backs and monthly service charges or program fees will be recorded.

1.1.2. A PCI Compliance questionnaire must be completed and submitted to Financial Services for each credit card merchant setup. See section 3 of this procedure for more information.

1.2. REFUNDS

Credit card refunds cannot be issued for more than the original transaction amount and can only be refunded on the card used for the original purchase. In most cases refunds cannot be processed back to the originating card more than 180 days after the initial transaction. In rare instances of refunds beyond 180 days, the merchant should first verify that the refund has not already been processed. If the refund request has not already been processed, the merchant should submit a payment request to Accounts Payable so that a check can be issued.

2. CREDIT CARD SECURITY

TAMU-CC and the payment card industry take the safeguarding of cardholder data very seriously. Failure to comply with university and industry security regulations may result in the revocation of the department's merchant account or, in the case of lost or stolen cardholder data, assessment of severe fines on the department by the bank. Departments are financially responsible for fines resulting from security breaches that originate from their systems.

2.1. Before a merchant department may receive credit card payments, it must develop and implement adequate security and internal controls that meet the requirements of the PCI DSS. To provide adequate security, the combined efforts of the business and information technology functions within the department or academic unit (e.g., college, school, library) are necessary.

2.2. The design and architecture of computer systems and networks associated with credit card processing, as well as the protocols used to transmit such data, must be approved by the Office of Information Security (OIS) prior to implementation. Subsequent changes must be approved prior to implementation.

2.3. All equipment and software, including POS units, must comply with current PCI security standards. No equipment will be allowed to be used unless approved by Financial Services. No software, including POS software, will be allowed to be used unless approved by OIS and Financial Services. Non-compliant equipment or software must either be reconfigured or replaced.

2.4. Business process security and internal controls features should include, but are not limited to:

2.4.1. Obtaining background checks for individuals authorized to have access to cardholder data or the ability to process credit cards, including all persons with Information Technology responsibilities related to the use of Marketplace or other approved software used for processing credit card transactions in accordance with PCI DSS and ensuring such personnel have completed system-required training for PCI and Basic Cash Handling.

2.4.2. Ensuring position descriptions include cash handling for all employees performing cash/credit card handling duties for at least 5% of their time.

2.4.3. Requiring that employees conducting in-person credit card transactions always keep the credit card within the customer's sight.

2.4.4. Accepting credit card transactions for no more than the amount of the purchase.

2.4.5. Confirming that the amount entered into the credit card machine matches with the purchase amount.

2.4.6. Ensuring that the credit card expiration date is not included on the receipt.

2.4.7. Ensuring that only the last 4 digits of the credit card number prints on the receipt copy given to the customer. Departments must verify that machines meet this requirement.

2.4.8. Referring any questions related to a third-party vendor requesting access to cardholder data to OIS. All third-party vendors will be under contract and contractually obligated to comply with PCI security standards. These contracts cannot be signed without the approval of Financial Services and OIS.

2.4.9. Ensuring that the storage of printed cardholder data, such as merchant copies of receipts or daily batch reports, are secured in a location with access limited to those with a legitimate business need. Records will be kept in accordance with the Texas A&M University System Records Retention Schedule (see Appendix).

2.4.10. Requiring that the authorization of access to keys for file cabinets containing cardholder data be restricted to personnel who have a legitimate business need for such access.

2.4.11. Ensuring no storage of cardholder data on electronic media, including USB drives, discs, hard drives of computers or laptops, etc. occurs.

2.4.12. Destroying any written credit card numbers accepted by phone by cross-cut shredding after the transaction has been processed.

2.4.13. Destroying any forms with written credit card numbers by cross-cut shredding after the transaction has been processed. Forms should have customer information at the top of the form and credit card information at the bottom of the form so the bottom portion can be cut off and cross-cut shredded.

2.5. In addition to the PCI Compliance Questionnaire completed during merchant setup, each merchant must complete an annual PCI Self-Assessment Questionnaire (SAQ). Multiple versions of the SAQ are available and are assigned based on the department's credit card payment acceptance methods.

2.6. OIS will perform periodic reviews of computers and/or computer networks to

ensure that security features are in place and are adequate to protect credit card data. Financial Services is available to conduct reviews of business processes to help merchants identify ways to better protect cardholder information.

2.7. Volunteers are not normally allowed to process credit cards or conduct transactions involving university merchant numbers. If the department has a large event and needs to use volunteers, they must sign a Volunteer Non-Disclosure Agreement for Volunteers Handling Cash form and receive training on PCI standards. Volunteers must also complete a Volunteer Waiver and Criminal Background Authorization form available on the Human Resources website.

3. MERCHANT RESPONSIBILITIES

Merchant departments participating in the credit card program are responsible for complying with all university rules and procedures, requirements issued by Financial Services, and all PCI DSS, including periodic business review and completion of the annual PCI questionnaire. Merchants will provide any reasonable assistance necessary to OIS in the performance of periodic reviews of credit-card related computer or computer network security. This includes providing IP addresses and network configuration diagrams for use in scanning systems for vulnerabilities. Merchants are responsible for notifying OIS and Financial Services in the event of security breach. Departments must have a standard operating procedure (SOP) in writing that cover use of terminals, forms, reconciling transactions, record retention, training, and any other information to conduct business and provide copies to Financial Services. Financial Services can provide a template to assist in developing these written SOPs.

4. FINANCIAL SERVICES RESPONSIBILITIES

Financial Services is responsible for administering the TAMU-CC credit card program and ensuring that participating departments are kept current on all rules, procedures and security standards. In addition, Financial Services will coordinate with the merchant bank on the merchant's behalf, including on cases of suspected security breach. Financial Services will distribute and coordinate the preparation of the annual PCI questionnaire for each merchant; work closely with both the merchant and OIS to ensure that all necessary security practices are in place to protect sensitive credit card data; assess service charges to merchant department accounts for credit card transactions based on information supplied by Visa/MasterCard, Discover, and American Express. Monthly service charges or program fees differ for each card type. For more information on monthly service charges, please contact Financial Services.

5. INFORMATION SECURITY OFFICE RESPONSIBILITIES

OIS may perform vulnerability scans of computer systems and will require configuration changes to eliminate vulnerabilities. This is both in preparations for and in addition to vendor scans that may be required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. In order to meet university security needs, OIS requirements may be stricter than the PCI standards. OIS is responsible for approving the configuration of merchants' PCI computer systems if applicable.

6. REQUIRED TRAINING

All departmental staff who will be involved in the acceptance of credit card data, including Information Technology staff who support systems that process credit card data, are required to complete an online PCI security training course before being allowed to handle credit card information. Annual refresher courses will also be required. The department is responsible for providing volunteers with sufficient training as outlined in section 2.7 of this procedure.

7. DISPOSAL OF SURPLUS OR NONFUNCTIONAL EQUIPMENT

When a department no longer needs a particular device to swipe or read credit cards, that card-reader must be returned to the University Surplus department for disposal.

Related Statutes, Policies, or Requirements

Payment Card Industry Data Security Standards
System Regulation *21.01.02, Receipt, Custody and Deposit of Revenues*
University Rule *29.01.99.C1, Management of Information Resources*
University Procedure *21.01.02.C0.02, Online Payments*

Appendix

New Credit Card Merchant Service Request Form
Texas A&M University System Records Retention Schedule

Contact Office

Contact for interpretation and clarification: Associate Vice President & Controller
361.825.5620