21.01.02.C0.01 Credit Card Collections

Approved: March 15, 2010
Revised: September 19, 2016
Next Scheduled Review: September 19, 2021

Procedure Statement

Texas A&M University-Corpus Christi 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, through the mail or over the internet. Supplemental information regarding the program can be found in the Accounting Handbook at http://comptroller.tamucc.edu/accounting/accounting_handbook.html.

Reason for Procedure

This procedure documents proper processing procedures, necessary training, appropriate physical storage, and authorized access to credit card data.

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 ranked as level 1 through 4, 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 Texas A&M University-Corpus Christi are Level 4.

PCI (or PCI DSS) Standards: Payment Card Industry Data Security Standards are 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 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 cards.

Marketplace U Store: This is a self-contained online store allowing the university department 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 Payment Card Industry (PCI) compliant way for a user to take online payments. U-Pay focuses on payment collection and reporting.

Procedures and Responsibilities

1. PROCEDURES

1.1 ESTABLISHING NEW MERCHANT ACCOUNTS

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 to Financial Services (FS) at campus mail unit 5737. Each department is required to provide FS an account number to which charge backs and monthly service charges or program fees will be recorded.

1.1.1 A PCI Compliance Questionnaire must be completed and submitted to FS 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

Texas A&M University-Corpus Christi 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 Payment Card Industry Data Security Standards (PCI DSS) requirements and University Rule 29.01.99.C1 Security of Electronic Information Resources. To provide adequate security, the combined efforts of the business and information technology functions within the department or college are necessary.

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

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

2.4 Business process security and internal control 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 IT 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 Updating Position Descriptions to 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 agrees with the purchase amount.

2.4.6 Assuring 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 ensure that machines meet this requirement.

2.4.8 Any questions related to a third party vendor requesting access to cardholder data should be referred to ISO. 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 ISO.

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 legitimate business need. Record retention rules dictate that records be kept 2 years.

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

2.4.11 No storage of cardholder data on electronic media, including USB drives, discs, hard drives of computers or laptops, etc., is allowed.

2.4.12 If accepting credit cards by phone, any written credit card numbers must be destroyed by cross cut shredding after the transaction has been processed.

2.4.13 If accepting credit card numbers on forms, any written numbers must be destroyed 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 initial PCI Compliance Questionnaire completed during setup, each merchant is required to complete an annual PCI self-assessment questionnaire. These should be sent out by Financial Services in May and will be completed by June 30 each year.

2.6 ISO will perform periodic reviews of computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data. FS will periodically perform reviews of business procedures to help merchants identify ways to better protect cardholder information. Reviews are also available upon request.

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 a Volunteer Waiver and Criminal Background Authorization forms available on the Human Resources website. Contact FS to provide the training materials and nondisclosure agreement to be used.

3. MERCHANT RESPONSIBILITIES

Merchant departments participating in the credit card program are responsible for complying with all rules and procedures issued by FS and with all PCI Data Security Standards, including periodic business review and completion of the annual PCI questionnaire. Merchants will provide any reasonable assistance necessary to ISO 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 ISO and FS in the event of security breach. Departments must have standard operating procedures (SOP) in writing that cover use of terminals, forms, reconciling transactions, record retention, training and any other information to conduct business and provide a copy to financial services. Financial services can provide a template to assist in developing these written SOP.

4. FINANCIAL SERVICES RESPONSIBILITIES

FS is responsible for administering the Texas A&M University-Corpus Christi credit card program and for ensuring that participating departments are provided updates on all rules, procedures and security standards. In addition, FS will review standard operating procedures and may conduct periodic audits of procedures and record retention practices; coordinate with the merchant bank on the merchant's behalf- including cases of suspected security breach; distribute and coordinate the preparation of the annual PCI questionnaire by each merchant; work closely with both the merchant and ISO to ensure that all necessary security procedures are in place to ensure protection of 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. FS must approve any contract for vendors to host our merchant numbers. In the event a department contracts with a vendor to collect funds via the internet and will not use our merchant number, FS must approve the contract. Monthly services charges or program fees differ for each card type. The Contracts and Property Office will also be involved in

contract review for these services. For more information on monthly service charges, please contact FS.

5. INFORMATION SECURITY OFFICE RESPONSIBILITIES

The Information Security Office 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, the ISO standards may be stricter than the PCI requirements. The ISO 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 IT staff who support systems that process credit card data, are required to complete an on-line 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 sufficient training to volunteers based on the types of transactions volunteers may process. See Section 2.7 for Volunteer requirements. For more information on available training please see the Texas A&M University-Corpus Christi HRConnect Website.

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

TAMUS Regulation 21.01.02 Receipt, Custody and Deposit of Revenues
TAMU-CC Rule 29.01.99.C1 Security of Electronic Information Resources
TAMU-CC Procedure 21.01.02.C0.02 Online Payments

Appendix

New Credit Card Merchant Service Request Form

Contact Office

Contact for interpretation and clarification:	Associate Vice President & Comptroller 361-825-5620