ALAMO COLLEGES DISTRICT

Credit/Debit Card Acceptance Practice

Owner: Finance and Fiscal Services
Effective Date: Aug 1, 2019
Impacts: Activities that accept credit and debit cards as payment

PURPOSE

The Alamo Colleges District has adopted the following practice and supporting procedures for all types of credit card activity transacted in person or the internet. The purpose of this practice is to protect the interests of the College District and its' customers, by establishing strong internal business controls and standard revenue collection methods.

This outline will provide guidance, so the processes of accepting credit/debit card payments comply with the Payment Card Industry Data Security Standards, (PCI DSS), and are appropriately integrated with the financial and other systems. In addition, adherence to this practice will ensure compliance with federal, state and local laws, related to the protection of credit/debit card information and other personal identifying information.

Alamo Colleges District has contracted with a third party vendor, whose core business includes the support and processing of credit card and electronic transactions. The vendor provides the Alamo Colleges District with a secure gateway and hosted solution, in which all electronic personal payment information is securely transmitted to and stored on off-site computers, which the company owns and maintains. The vendor maintains PCI DSS Compliance Certification. This relationship enables the Alamo Colleges District to provide secure infrastructure for acceptance of electronic payments.

APPLICABILITY

Any Alamo Colleges District employee, contractor or agent, who in the course of doing business on behalf of the District Office, is involved in the acceptance of credit/debit card and electronic payments, is subject to this practice. Failure to comply with the terms of this practice may expose the department and/or the District to financial losses and/or legal liabilities.

ALAMO COLLEGES DISTRICT

STATEMENT

Any department desiring to collect revenue, (through credit cards or checks), on behalf of the District for goods or services, must utilize the secure web based store front. "Marketplace" is the District's preferred web based application and Point of Sales devices for electronic collection of revenue. This application can accommodate receipt of checks and credit and debit cards, (Master Card, Visa, American Express, and Discover), in a secure environment, which is maintained by the third party provider, as referenced in the purpose section.

CREDIT AND DEBIT CARD REFUNDING

When a credit card payment is processed at Alamo Colleges District and a refund is due, the following occurs:

- When a refund is due to overpayment and/or dropping of a course(s), the preferred refund method will be to refund the original card through our third party payment processor.

- If the overpayment occurs and the original transaction occurred within 180 days, Alamo Colleges District will refund the card through our third party vendor payment system. Otherwise, if the transaction exceeds 180 days, the acceptable process will be Alamo Colleges District creates an electronic refunding profile that is sent to third party processor, ECSI. This will apply to student refunds. If it is a Marketplace Mall transaction, a direct pay will be processed through our Accounts Payable department and a check issued to the purchaser of the Marketplace Mall transaction.

RESPONSIBILITIES OF A MERCHANT DEPARTMENT

MERCHANT DEPARTMENT

A Merchant Department is the department designated as the primary representative for revenue collections.

VBO

The Virtual Business Office (VBO) offers safe, convenient and secure online services for students, staff and faculty, as well as, the surrounding community. Student

ALAMO COLLEGES DISTRICT

tuition/fee charges can be paid with credit and debit cards and are accepted by route of their ACES student account.

The VBO offers the Market Place Mall, which is an online or Point-of-Sales system that allows products, services, or fees to be purchased with a credit or debit card or personal check at any Alamo Colleges or home. Merchant departments are designated as the District's College Business Offices. The following responsibilities are an important aspect of the District's compliance with the PCI Data Standards. All credit/debit card payment transactions will be taken using Point-of-Sales devices or the "Marketplace Mall or single store setups" only.

- Follow the Card Acceptance guide, (or similar rules), of the Merchant Processor/Acquirer (e.g., Global Payments) and the operating regulations and rules of any Card Associations/Networks that will be accepted by the Merchant Department (e.g., MasterCard, Visa, etc.).

- Alamo Colleges District does not collect or store credit card data at of it's locations as being physically or electronically.

- Ensure that all employees, including the MDR, contractors and agents with access to payment card data, complete compliance training on an annual basis.

- Revenue collection arrangements that require payees to enter credit or debit card numbers on preprinted order forms which are faxed, mailed or phoned in to a District department are strictly prohibited.

- An added security measure was implemented in July 2018. The payee is required to enter the CVV security code from back the credit or debit card. This requires the physical presence of the credit card or knowledge of the CVV code.

- Email is not used to transmit credit or debit card payment information, if the use of email is necessary.

- No photocopies of credit or debit cards are accepted.

- Credit or debit card card or electronic payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.

- The processing and storage of personally identifiable credit or debit card or electronic payment information on district computers and servers is prohibited.

- Only secure communication protocols and/or encrypted connections are used during the processing of electronic transactions. (NOTE: The Alamo Colleges District Information Security Department maintains a security professional who is available, as required, to provide consultative services on appropriate security practices. The Information Security Technology Office can be contacted for more information regarding these services.)

- The three-digit card-validation code printed on the signature panel of a credit or debit card is never stored in any form.

- All but the last four digits of any credit card account number are masked, if credit or debit card data is displayed.

- All discovered instances of the full credit or debit card number, bank account number or a Social Security number, must be reported to the Chief Bursar and the Information Security Office and remedied immediately.

- No credit or debit card receipt, or other document referencing the transaction, shall include more than the last four digits of the account number or the month and year of the expiration date.

No district employee, contractor or agent who obtains access to credit or debit card or other personal payment information may sell, purchase, provide, or exchange said information in any form to any third party other than to the district's acquiring bank, depository bank, Visa, MasterCard or other credit Card company, or pursuant to a government request. All requests to provide information to any outside party must be reviewed and approved in advance by the Associate Vice Chancellor of Finance and Fiscal Services, or their designee.

Process to become a Marketplace Merchant Department

The MDR or his/her designee must follow the steps below in order to request approval to obtain a Marketplace site:

ALAMO COLLEGES DISTRICT

1. Notify the College's Assistant Bursars or the District Bursar of a need to accept credit or debit cards and/or electronic payments by presenting a formal request to become a Marketplace Merchant department.

2. It is the responsibility of the department head to approve the business request and all other information provided.

3. The official request should be submitted to the College's Assistant Bursars or the District Bursar for review and approval.

4. If the request is approved, the College's Assistant Bursars or the District Bursar will create a Marketplace design for the storefront for the department.

5. The College's Assistant Bursars or the District Bursar will arrange the necessary training for the department (i.e.: reports, PCI regulations), as well as any additional information pertinent to the approved payment method for any online or Point-of-Sales devices.

Third Party Vendors Scope of the Third Party Vendor

There is limited service not offered by Alamo Colleges District, (i.e.: food service, bookstore, vending machines and ATMs). Therefore, occasionally, Alamo Colleges District releases a "RFP", where outside vendors will provide a service for Alamo Colleges District within the premises Alamo Colleges District.

Responsibilities of the Third Party Vendor

- Third party vendors are not Alamo Colleges District employees.

- These vendors may offer services where credit and debit card payments are accepted.

- The services offered are offered on their behalf and not Alamo Colleges District.

- These vendors service our customers, due to an agreed upon contract.

- Any transactions, (including electronic based), that involve the transfer of credit and debit card data, must not be on Alamo Colleges District systems.

- The contract will require the contracting vendor to supply Alamo Colleges District with an annual document/certificate, indicating PCI compliance.

- Failure to submit said document could cause a rejection of its contract.

- If a third party vendor should experience or even suspect a breach of security, the vendor should contact the Associate Vice Chancellor of Finance and Fiscal Services and the Information Technology Security Officer.

Process for Responding to a Security Breach

Security breaches can result in serious consequences for the District, including release of confidential information, damage to our reputation, added compliance costs, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept credit and debit cards and electronic payments.

In the event of a breach or suspected breach of security, the Chief Bursar or Merchant Department must immediately perform the following steps:

1. Contact the Associate Vice Chancellor of Finance and Fiscal Services and the Information Technology Security Officer. The Information Technology Security Officer will provide further instructions which will include measures that will preserve electronic evidence.

2. The Information Technology Security Officer will implement a Crisis Response plan to isolate, investigate, document and remediate the situation in partnership with the Associate Vice Chancellor of Finance and Fiscal Services, or designee.

3. All investigations and collection of evidence will be done by the Information Technology Security Officer. To prevent alteration of the compromised system or systems, Information Security asks the MDR to follow the requests below:

a. Do not switch off the compromised machine.

b. Do not attempt to isolate the compromised system(s) from the network by unplugging the network connection cable.

c. Do not log on to the machine and/or change passwords.

4. Be on HIGH alert and monitor all electronic applications and report suspicious activity to Information Security.

5. The Associate Vice Chancellor of Finance and Fiscal Services, or designee, shall alert the Merchant Bank, the Payment Card Associations and the Alamo Colleges District Police Department. The Associate Vice Chancellor of Finance and Fiscal Services shall report the suspected breach to the Vice Chancellor of Finance and Fiscal Services, who will in turn take the appropriate actions to alert the Chancellor.

6. Where an actual breach of Credit Card Data is confirmed, the Associate Vice Chancellor of Finance and Fiscal Services, with the assistance of the Information Technology Security Officer, will ensure that compromised credit card account information is securely sent to the appropriate credit and debit card associations and credit reporting agencies.

7. Within 48 hours of the breach, the Associate Vice Chancellor of Finance and Fiscal Services, with assistance from the relevant MDR, shall provide the affected credit and debit card associations with proof of PCI Compliance.

8. Within 4 business days of the breach, the Associate Vice Chancellor of Finance and Fiscal Services, with assistance from the relevant MDR, shall provide the affected credit and debit card associations with an Incident Report.

9. At the relevant credit and debit card association's request and depending on the level of risk and data elements compromised, the District may, within 4 business days of the event:

a. Arrange for a Network and System Vulnerability Scan.
b. Complete a Compliance Questionnaire and submit it to relevant card association(s).

ALAMO COLLEGES DISTRICT

10. In the event that personal data is exposed, per Alamo Colleges District Information Use and Security Policy #UTS165, the District will provide notification to any resident of Texas and the data to the owner whose personal identifying information was or is reasonably believed to have been acquired without authorization.

Ongoing Management

Alamo Colleges District may make modifications from time to time as required, provided that all modifications are consistent with Payment Card Industry Data Security Standards then in effect. The Associate Vice Chancellor of Finance and Fiscal Services, along with Treasury Services and the District Business Office, is responsible for initiating and overseeing an annual review of this practice, making revisions and updates and ensuring that the updated practice has received the appropriate approvals and is distributed to the Merchant Departments.

References

Links to Global Payments, MasterCard and Visa are provided for reference:

Global Payments Card Acceptance
https://www.globalpaymentsinc.com/-/media/global-payments/files/shared/latest-card-acceptance-guide-us.pdf

MasterCard Worldwide Rules and Chargeback
http://www.mastercard.com/us/merchant/support/rules.html

Visa Merchant Responsibility and Card Acceptance Guide
http://usa.visa.com/merchants/new_acceptance/merchant_responsibility.html

Relevant Statues
Sections 35.60, 72.004 and 502.002 of the Texas Business & Commercial Code