ALAMO COLLEGES

Credit/Debit Card Acceptance Practice

Owner: Finance and Fiscal Services
Effective Date: June 30, 2011
Impacts: Activities that accept credit 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, over the phone, via fax, mail 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 that the processes of accepting credit/debit card payments complies 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 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 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 to provide secure infrastructure for acceptance of electronic payments.

Applicability

Any Alamo Colleges' employee, contractor or agent who, in the course of doing business on behalf of the District, is involved in the acceptance of credit 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.

Statement

ALAMO COLLEGES

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 storefront. "Marketplace" is the District's preferred web based application for electronic collection of revenue. This application can accommodate receipt of checks and credit 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.

REFUNDING

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

1. All students are requested to create an electronic refunding profile on line through their ACES account.
2. When a refund is due to overpayment and or dropping of a course (s), the preferred refund method is to be sent to your checking or saving account electronically or the alternate method is to print a check.
3. If funds need to be returned to the credit card, the card holder will need to advise the District Business office at 210-485-0359, otherwise the acceptable process will be as described in step 2 above.

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. The VBO offers the Market Place Mall, which is an online system that allows products, services, or fees to be purchased online with a credit card or personal check at any Alamo College or in the comfort of your 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 card payment transactions** will be taken using the "VBO" or a walk up to one of the colleges Business offices.

1. 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.).
2. Ensure that all employees, including the MDR, contractors and agents with access to payment card data complete compliance training on an annual basis.

3. Revenue collection arrangements that require payees to enter credit card numbers on preprinted order forms which are then mailed to a District department are not allowed.

4. Ensure that all credit card data collected, regardless of how it is stored (physically or electronically, including but not limited to account numbers, card imprints, and Terminal Identification Numbers) is secured. Data is considered to be secured only if the following criteria are met:

O Only those with a need-to-know are granted access to credit card and electronic payment data.

o Email is not used to transmit credit card payment information. If the use of email is necessary, only the last four digits of the credit card number are displayed.

O No photocopies of credit cards are accepted.

o Credit 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.

o Fax transmissions (both sending and receiving) of credit card and electronic payment information are limited to those fax machines whose access is restricted to authorized individuals. The transactions must be processed immediately and the documents must be shredded.

o The processing and storage of personally identifiable credit card or electronic payment information on District computers and servers is prohibited. Exceptions can only be made if the processing and storage methods are compliant.

o Only secure communication protocols and/or encrypted connections are used during the processing of electronic transactions.

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

o all but the last four digits of any credit card account number are masked if credit card data is displayed.

o all credit card and electronic payment data that is no longer deemed necessary or appropriate to store is destroyed or rendered unreadable.

o All discovered instances of the full credit card number, bank Account number, or social security number must be reported to the, Chief Bursar, and the Information Security Technology Office and remedied immediately.

5. No credit 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 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 or their designee.

Process to become a Merchant Department

The MDR or his/her designee must follow the steps below in order to request approval to obtain a merchant number and or to become a Merchant Department.

1. Notify the Chief Bursar in Finance and Fiscal Services of a need to accept credit cards and/or electronic payments by presenting a formal request to become a Merchant Department.
2. Final approval request should come from the division Department Head. It is the responsibility of the Department Head to approve the business case and all other information provided in the request.
3. The official request should be submitted to the Chief Bursar for review and approval by the Associate Vice Chancellor.
4. If the request is approved, the Chief Bursar will coordinate the District Web Services design of a new Marketplace storefront for the Department. The requesting Department should allow sufficient time for this process to be completed.
5. The Chief Bursar will arrange the necessary training for the Department, as well as any additional information pertinent to the approved payment method.

Third Party Vendors

Scope of the Third Party Vendor

There are limited services not offered by Alamo Colleges i.e. food service, bookstore, vending machines and ATM's. Therefore, occasionally Alamo Colleges releases a "RFP" where outside vendors will provide a service for Alamo Colleges within the Alamo Colleges premises.

Responsibilities of the Third Party Vendor

Third Party vendors are not Alamo Colleges employees.
These vendors may offer services where credit card payments are accepted.
The services offered are offered on their behalf and not Alamo Colleges.
These vendors service our customers due to an agreed upon contract. All transactions (including electronic based) that involve the transfer of credit

card data must be performed on systems approved by Alamo Colleges Information Technology department.
The contract will require the contracting vendor to supply Alamo Colleges 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 breach of security, the vendor should contact: Associate Vice Chancellor and the IT Security Incident response Protocol for contacts within one business day of identified breach.

Process for Responding to a Security Breach

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

In the event of a breach or suspected breach of security,

1. Contact the Associate Vice Chancellor and the Incident Coordination Team (ICT). ICT will provide further instructions which will include measures that will preserve electronic evidence.
2. ICT will facilitate a Crisis Response Plan to isolate, investigate, document and remediate the situation in partnership with the Associate Vice Chancellor or designee.
3. All investigations and collection of evidence will be done by ICT. To prevent alteration of the compromised system or systems, Information Security asks the MDR to follow the requests below:
    - o Do not switch off the compromised machine.
    - o Do not attempt to isolate the compromised system(s) from the network by unplugging the network connection cable.
    - o Do not log on to the machine and/or change passwords
    - o Be on HIGH alert and monitor all electronic applications and report suspicious activity to Information Security.
4. The Associate Vice Chancellor or designee shall alert the merchant bank, the payment card associations and the Alamo Colleges Police Department. The Associate Vice Chancellor shall report the suspected breach to the Vice Chancellor who will in turn take the appropriate actions to alert the Chancellor.
5. Where an actual breach of credit card data is confirmed, the Associate Vice Chancellor, along with ICT, will ensure that compromised credit card account information is securely sent to the appropriate credit card associations and credit reporting agencies.

6. Within 24 hours of the breach, the Associate Vice Chancellor, with assistance from the relevant MDR, shall provide the affected credit card associations with proof of PCI compliance.

7. Within 4 business days of the breach, the Associate Vice Chancellor, with assistance from the relevant MDR, shall provide the affected credit card associations with an incident report.

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

- o Arrange for a network and system vulnerability scan.
- o Complete a compliance questionnaire and submit it to relevant card association(s).

9. In the event that personal data is exposed, per Alamo Colleges IT Security Incident Response Protocol, the District will provide notification to any resident of Texas and data an owner whose personal identifying information was or is reasonably believed to have been acquired without authorization.

Ongoing Management

Alamo Colleges 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 along with Information Technology and the District Business Office are 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. The revised practice will be distributed to the Merchant Departments.

References

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

- Global Payments Card Acceptance
  http://www.globalpaymentsinc.com/myglobal/cag.html
- 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 Statutes:

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