

Card Merchant Guide ^[1]

The Treasurer's Office of the University of Colorado is responsible, by contract and by regulation, to both its sponsoring merchant bank and to the credit card system for all card transactions accepted in payment for the sale of goods and services by all entities within the University. (Card transactions include payments by credit card, debit card, Travel & Entertainment (T & E) card, proprietary debit card, and other forms of plastic money. The cards currently recognized for acceptance are Visa, MasterCard, American Express, Discover, Diners Club / Carte Blanche and the Buff One Gold card.) When departments/units do not live up to their responsibilities as card-accepting merchants, not only is the department / unit itself liable for any potential losses, but also the University as a whole could be at significant financial risk. These risks include higher interchange rates for card transactions, legal liability for unauthorized or fraudulent items, and possible sanctions, fines, and penalties for excessive chargebacks and/or fraudulent transactions, as well as inadequate Internet site security.

It is essential that each department or business unit that wishes to accept card payments understand their responsibilities and liabilities when accepting these types of payments. This guide is meant to be an introduction to these responsibilities and the acceptable business practices that form the foundation of meeting them.

There are five main issues of which potential merchants must be aware. They are:

1. **Merchants must be qualified to accept cards for purchases.** That is, not just any department or business unit can accept cards they must demonstrate that they have sufficient resources and prudent business practices to meet the requirements imposed by the card association rules, the Treasurer's Office, any campus-specific requirements, and fraud-control measures.
2. **Merchants must adhere to the card association rules.** Visa and MasterCard, in particular, and our merchant bank on their behalf, have established specific minimum processing and operational procedures that must be followed to ensure that cards are properly accepted, correct credit is given for card purchases, and copy requests and/or chargebacks are processed timely.
3. **Merchants must fund all card costs (setup, processing, discounts, and other fees) from their own budgets.** Accepting cards for purchases is costly, as there are multiple fees involved. The department or business unit must either be able to build the cost of card acceptance into their product and service prices, or support these costs directly from their own budgeted resources.
4. **Merchants must adhere to minimum acceptable business practices.** In addition to the rules imposed by the card associations and our merchant bank, there are other prudent business practices that must be set up and followed by each card-accepting department / unit. These practices are outlined later in this document.
5. **Internet card acceptance has its own additional requirements.** There are additional requirements mandated whenever a merchant wishes to accept card payments through

its Web site. This is because of the different nature of the online medium – the speed, volume, and electronic character of these transaction require much stricter attention to security and fraud than is customary for in-person payments.

Each of the following sections of this guide will briefly discuss these issues and outline some of the necessary business practices.

Merchants Must Be Qualified

There are several criteria that must be satisfied before a department or business unit will be approved to become a card-accepting merchant.

- **First**, if it is a campus requirement, the department / unit must be approved to accept cards for payment by the designated campus official. Each campus will have its own criteria and requirements, many of which will mirror requirements specified elsewhere in this outline.
- **Second**, the unit must be approved by the Treasurer's Office. This document outlines the criteria and minimum business practices that must be established for approval. Once the department/unit is approved to become a card-accepting merchant, it may be subject to requalification if its business practices later cease to be acceptable.
- **Third**, the department or business unit must have the appropriate infrastructure in place to process card transactions. This includes, at a minimum:
 - A card authorization terminal (swipe terminal) or PC with modem and appropriate processing software as well as access to an outside (non-digital) phone line; Alternatively, access to a voice line so a telephone authorization may be obtained (this is offered as an alternative to assist in managing costs);
 - Formal business processes in place to ensure that minimum processing standards are followed;
 - Regular employees and/or paid student employees doing the card processing as a formal part of their job duties;

Other reasonable requirements as may be specified by the Treasurer's Office.

- **Fourth**, if a merchant wishes to accept other cards such as American Express, Discover, and Diners Club, they must be separately approved for each type of card. The base merchant account allows the merchant to accept Visa and MasterCard, under the University's sponsorship to the card system through our merchant bank (currently Wells Fargo Merchant Services, or WFMS). Other card issuers have their own criteria for qualifying merchants, and each merchant must satisfy those criteria in addition to the initial requirements to accept Visa/MasterCard. A department may wish to accept other cards if, for instance, many of their customers use American Express or Discover purchase cards for payment rather than Visa or MasterCard.

Each department or business unit must be set up within the centralized University banking and accounting environment. That is, merchants may NOT set up their own banking relationships for card processing and card receipts MUST be deposited into designated University of Colorado bank accounts. The Treasurer's Office negotiate all banking and card processing relationships on behalf of the entire University, thereby taking advantage of the volume discounts and internal controls not available to individual department or business units. In addition, the Treasurer's Office is responsible for automatically posting certain transactions directly into the PeopleSoft system on behalf of each merchant department or

business unit.

Adhere to Card Association Rules

Once a department or business unit is approved to become a card merchant, there are business process requirements imposed by the card associations and our merchant bank. In general, they include:

- **Follow proper card authorization and acceptance procedures.** To protect the University, all card transactions must be authorized before a purchase transaction may be completed. The card associations have specified uniform procedures that must be followed when requesting an authorization for a purchase; these procedures are given in the bank's reference guide as well as other materials sent to the new merchant. Procedures will vary depending on the type of transaction, whether the card is present or not, the authorization terminal, and the authorization code returned back to the merchant.
- **Merchants cannot discriminate against cards as a form of payment.** All card associations require that merchants accept card payments at par value, without giving preference to other methods of payment such as checks. That is, a merchant may not impose a surcharge on the purchaser when they pay by card. The only discount that may be given is for payment by cash, which should be carefully considered before being implemented in light of fairness, operational, security, and internal control issues.
- **Timely response to copy requests.** Consumers have the right to dispute card transactions that they claim were not authorized or in error, and their card-issuing financial institution will then request a copy of the transaction from the merchant. If the merchant does not respond within 12 calendar days to the request for copy, the transaction is ?charged back? to the merchant account. There is no grace period, and no appeal if the merchant misses the deadline. Therefore, all merchants must have adequate business processes in place to support the timely turn-around of copy requests and other transaction inquiries.
- **Fraud avoidance procedures.** Card fraud is rampant in our society, and the card associations have mandated that all card merchants put in place minimum fraud detection and avoidance procedures. These procedures include steps such as comparing the signature on the charge slip to that on the back of the card obtaining certain information from the cardholder when a card is not present, reading the magnetic stripe on the back of the card if a swipe terminal is used for authorization, etc. Merchants are subject to additional fees, fines and penalties if excessive fraud and/or chargebacks are encountered and may be subject to revocation of their merchant privileges.
- **Chargeback prevention procedures.** Chargebacks are costly and time consuming, so merchants are encouraged to implement business practices that minimize them.
- **Truncate card number to last 4 digits on receipt given to customer.** Compliance with this mandate depends on the type of authorization / receipt-printing equipment used by the merchant, and is a security measure to protect the privacy of the card number. Both the card associations and the State of Colorado independently require this action; the effective dates for both requirements are in the future. However, the Treasurer's Office will require all new merchants to comply with this directive immediately (that is, purchase compliant equipment from the start), and will work with all existing merchants to bring them into compliance as soon as practicable.

- **Additional requirements for Internet card transactions.** A subsequent section will outline the additional requirements for Internet card purchase transactions, from additional infrastructure mandates to internal controls.

Fees and Charges

As noted above, each department is responsible for paying the costs of card acceptance themselves. These costs include the following (prices noted are current as of October 2003):

- **Setup fees.** Our merchant bank is currently waiving their new merchant setup fees, but it is possible that they could be implemented at some future date. There is, however, a setup fee for Internet card authorization services through Verisign, the University's designated Internet card authorization service provider. These fees are discussed in the section on Internet card acceptance.
- **Authorization terminal lease / purchase.** Each merchant must have a means of obtaining an authorization, as well as sending the approved transaction to the card system for processing. The preferred means of doing so is electronically, either with a special-purpose authorization/processing terminal or through a PC / software / modem connection. Most in-person card transactions are processed on a special-purpose terminal. Prices for these terminals vary, but range from approximately \$35 per month for a leased terminal, to \$750 to purchase a terminal. There are advantages and disadvantages to both leasing and purchasing, and the Treasurer's Office can assist you in evaluating your options. If transactions are not made with a card present, another option would be to use a PC with special software and a modem to obtain the authorization and transmit the approved transaction. The Treasurer's Office can assist in evaluating and recommending appropriate software. A third alternative is to obtain authorizations via an Audio Response Unit (ARU) over a regular telephone. All of these options except the last entail what may be an additional expense — a phone line that does not go through the campus switchboard. Please check with your campus to determine the cost of any necessary infrastructure to obtain outside lines for transmitting card transactions.
- **Transaction processing fees.** Each authorization and card transaction is subject to processing fees. These fees total between \$0.15 and \$0.50 per transaction, depending on the authorization and processing method (electronic authorization and processing is most cost effective; manual processing is most costly and should be avoided whenever possible).
- **Merchant discount.** The card associations charge a discount fee on most card transactions. This fee is a percentage of the total purchase transaction, and varies according to the type of card presented (regular credit card, purchase card, American Express, etc.) and the merchant's terminal capabilities (ability to pass purchase card information to the authorization network, etc.). The discount fee ranges from approximately 1.5% up to 3.25%. The Treasurer's Office can assist you in obtaining a more accurate estimate of your discount fees.

There is one situation in which a discount is not charged, but is offset by a higher processing fee. This occurs when a debit card is presented at the point of sale, and the merchant has the purchaser key in a PIN number to authorize the sale. The amount of the fee varies, but for large value purchases is more than offset by the absence of the discount. The Treasurer's Office can make recommendations about whether you should

promote this option in order to reduce some of your processing costs.

- **Other fees.** There are other fees of which merchants should be aware, but which are not part of the standard processing routine. These fees are charged to the merchant on an as-incurred basis.
- **Numerical examples.** This first numerical example assumes a total purchase (including sales taxes) of \$100.00, authorization and processing using a special purpose swipe terminal, and a regular Visa card.

Purchase Amount	\$100.00
Merchant Discount 1.43%	1.43
WFMS Service Fee 0.22%	0.22
Emerging Markets Per- Item Fee	0.05
Authorization Fee	0.10
Total	\$ 101.80

The second example assumes a total purchase (including sales taxes) of \$100.00, audio response authorization and processing, and a MasterCard purchase card.

Purchase Amount		\$ 100.00
Merchant Discount	1.90%	1.90
WFMS Service Fee	0.22%	0.22
Emerging Markets Per- Item Fee		0.05
Authorization Fee		0.05
Total		\$ 102.67

The last example assumes a total purchase (including sales taxes) of \$100.00, audio response authorization and manual processing, and a standard MasterCard card.

Purchase Amount		\$ 100.00
Merchant Discount	2.65%	2.65
WFMS Service Fee	0.22%	0.22
Emerging Markets Per- Item Fee		0.05
Authorization Fee		0.50
Total		\$ 103.42

The Treasurer's Office can assist you in obtaining an estimate of the cost of accepting cards so you can better budget for the impact of the associated costs.

Note: Keep in mind that the department or business unit must support these costs from their own budget. If the department or business unit has the option, it is recommended that you include these costs in the final price of your good or service.

Minimum Acceptable Business Practices

In addition to the above - noted business practices required by the card associations, the Treasurer's Office (and each campus, as applicable) will require certain other prudent procedures to be in place. These include, but are not limited to, the following:

- Consistent business processes in place to meet the card association requirements (chargeback processing within 12 calendar days, three-year record retention, logical and consistent filing system, adequate security of records).
- Preserving the security and confidentiality of card numbers and cardholder information.
- Timely accounting, journal posting, and reconciliation of card transactions purchase revenues, chargebacks, and fees – both in their bank account (if applicable) and in PeopleSoft.
- Awareness of fraud techniques and how to recognize and counter them.
- Training for staff accepting / processing cards.
- Specific procedures related to telephone order / mail order (MOTO) processing.
- Additional business practices necessary to meet Internet transaction requirements, if applicable.

The Treasurer's Office and the campus will work with each department to ensure that these and any other necessary requirements are met. It is our expectation that because these practices are prudent, they should already be in place within the department or business unit. We will work with each merchant and campus to ensure that there is sufficient support to bring business practices in line with these expectations, as well as with the overall business practice standards of the University of Colorado.

Internet Card Acceptance

The Internet environment presents additional challenges to the merchant accepting cards for payment. There is no card physically present to compare the cardholder's signature on the purchase slip with that on the back of the card. Stolen card numbers can be immediately duplicated by the millions, and programmatically presented within seconds to the merchant site for purchase of goods and services. Hackers can download scripts to break into systems without having any competency in programming or other technologies. Web site programming errors can leave gaping holes in a site's security.

Merchants accepting cards over the Internet must implement these additional practices:

- **Purchase authorizations must be processed through the Verisign payment / authorization gateway service.** Verisign is an established processor using secure, state-of-the-practice processing procedures for online transactions; using their services also meets many of the requirements of the Visa Cardholder Information Security Program discussed below. In addition, under the Verisign process, the card number is not stored on the merchant's server, so it is not at risk in the event of a break - in to the merchant's (department's or business unit's) system.

Note: some departments may wish to use the online card - processing module for software they have already purchased for other uses (say, for conference registration, or a membership database). The Treasurer's Office will work with the department and their software provider to ensure that the proposed system meets our processing standards.

Adherence to the Visa Cardholder Information Security Program (CISP) requirements for online merchants. Many of these requirements should already be standard operating procedures within all departments (e.g., use of anti-virus programs, unique user IDs, changing of vendor supplied defaults, tracking of access by user ID, physical security of data). Other requirements will require more technical sophistication than a department or business unit may currently possess (e.g., use of SSL, encryption of stored data, information security policies, testing of security systems and processes). Therefore, each merchant wishing to accept cards over their department or business unit's Internet site will need to work closely with their campus IT department to ensure that these requirements are met, not only at initial setup, but on an ongoing basis. The Treasurer's Office considers the requirements of the CISP to be the minimum acceptable business practices for accepting card transactions over the Internet. Existing Internet card merchants will also be required to bring their infrastructure and business practices up to this level. These standards can be reviewed at:

http://usa.visa.com/business/merchants/cisp_how_to_comply.html [2]

- **Professional programming review or assistance in creating the merchant web site.** Many of the Visa CISP requirements are of a technical nature and require programming skills not normally possessed by departmental programmers or student work/study staff. It will be important for the department to work closely with the campus IT department or other technical professionals to ensure that the card purchase section of their web site (shopping cart, registration form, etc.) is programmed properly, and follows standard security protocols for handling authorizations and transactions.
- **Additional fraud screening and detection measures.** As the University acquires more experience with Internet card transactions, particularly with fraudulent transactions, additional fraud screening will become prudent. The Treasurer's Office will work with merchants, UMS, and campus IT departments to continually enhance our procedures and detect potentially fraudulent transactions before they result in losses to the University.
- **Continual review of site security and procedures.** The world of hackers and thieves does not stand still. As crooks become smarter and develop new types of attacks, or discover new holes in existing systems, we must respond by continually updating our site and card-processing security. In addition, we must continually assess not only our external protections, but also our internal controls to ensure that we meet and exceed the standards to which we are being held.

Additional Internet card costs:

There is a setup fee for Internet card authorization services through Verisign, the University's designated Internet card authorization service provider. This setup fee currently ranges from \$180 to \$250, depending on the expected monthly transaction volume. However, Verisign occasionally has special package deals that can lower the initial setup cost (for instance, if the merchant prepaids for 12 months of processing).

There are two different ways to pay for Verisign authorization charges: a fixed monthly fee for

a set number of transactions, or a per-item fee of \$0.25 per transaction. The fixed monthly fees are either \$19.95 (for up to 500 transactions in a month) or \$59.95 (for up to 1,000 transactions in a month). (Transactions over the limit are charged at \$0.10 per item.)

This example assumes a total purchase (including sales taxes) over the Internet of \$100.00, authorization through

Verisign on a per-transaction basis, and the use of Visa card for the purchase.

Purchase Amount		\$ 100.00
Merchant Discount	1.43%	1.43
WFMS Service Fee	0.22%	0.22
Emerging Markets Per- Item Fee		0.05
Authorization Fee		0.25
Total		\$ 101.95

For More Information

For additional information, please contact Joe Tinucci in the Treasurer's Office. Joe can be reached by telephone at (303) 837-2185, or by email to joe.tinucci@cu.edu ^[3]

The Visa home page for the Cardholder Information Security Program is at:
https://usa.visa.com/business/merchants/cisp_how_to_comply.html ^[2]

Wells Fargo Merchant Services has several publications available to assist you in setting up and maintaining the business practices necessary to manage your merchant account. Please contact Joe Tinucci for more information or for samples.

Groups audience:

Treasurer

Source URL:<https://www.cu.edu/treasurer/card-merchant-guide>

Links

[1] <https://www.cu.edu/treasurer/card-merchant-guide>

[2] https://usa.visa.com/business/merchants/cisp_how_to_comply.html [3] <mailto:joe.tinucci@cu.edu>