Table of Contents

Steps to Becoming a Credit Card Merchant

Credit Card Solutions
  Department Based
  Vendors

Policies Governing Credit Card Acceptance and Merchants
  UC Policy
  PCI Compliance

Costs for Credit Card Acceptance
  Fees
  Equipment
  Compliance

Credit Card Reconciliation Process

Credit Card Terminology
Steps to Becoming a Credit Card Merchant

If a department or unit would like to accept credit cards, and become a merchant, the first step is a discussion with the Campus Credit Coordinator (“Coordinator”). At that time, the department/unit will discuss their plans, potential revenue, etc. In addition, the Coordinator will review aspects of credit card acceptance, including approval from the Chancellor, the type of setup the unit/department is requesting, potential vendors, associated fees, and UC and campus policies.

Credit Card Coordinator Review
The Coordinator will want to gain an understanding of the department/unit’s need to accept credit cards. Things to consider are the amount of potential revenue to be generated and level of staff support to manage the acceptance and reconciliation of all of the credit card income and fees. In addition, a review of the activities will be done to consider potential issues such as the need for a revenue account, unrelated business income tax (UBIT) reporting, and the approval of the activities by the campus Rate and Recharge Committee.

Chancellor Approval
The Chancellor approves all requests from departments/units to accept credit cards. This is done via a letter from the department/unit head, that is routed to the Coordinator, the campus Controller and on to the Chancellor.

Determine Type of Setup
A majority of our campus merchants wish to accept credit cards for registration fees associated with conferences the department/unit is hosting. The remaining merchants are selling other types of goods or services, such as tickets to events, or parking for example.

There are two options for accepting credit cards:

I. Department/Unit Hosted Website
For this option, the department/unit typically has technical support staff, who can create an event website and a database behind the scenes to capture all of the registration information. This setup also requires integration with a payment gateway and does not allow for any storage of credit card data. Also known as the “click to pay” model, because users are redirected to a payment gateway for secure collection of credit card data.
II. Vendor Solution

A. UC Approved Vendor
   Another option for accepting credit cards is to use an approved UC vendor, who can facilitate the development of a web page/form, which can collect the registration information, provide reports, and process the credit card transactions with the payment gateway.

B. Outside Vendor
   If a department/unit has a need to sell goods/services and wishes to use a vendor who does not currently have an approved agreement with the UC system, the vendor must meet certain guidelines prior to signing any agreement.

1. Payment Card Industry Standards (PCI)
   Any vendor who offers credit card acceptance capability, and wishes to do business with the University must agree to standard UC contract language about PCI compliance and provide evidence of their PCI validation.

2. Payment Application Best Practices
   Depending on the type of product offered by the vendor, the vendor may also have to certify their product was developed according Payment Application Best Practices (PABP).

3. Certificates of Insurance
   Any vendor who offers credit card acceptance capability, and wishes to do business with the University must agree to standard UC levels of insurance that must be carried by the vendor.

NOTE: Departments need to be very aware of the requirements outlined above. Many times smaller businesses/vendors will not be able to meet the insurance requirements, or be willing to accept or negotiate our contract language. Should this occur, we will not be able to move forward and use the vendor.
Credit Card Merchant Training

Terminology
(courtesy of Authorize.net website: www.authorize.net, Bill Collins, Former Vice President – Relationship Management, Chase Paymentech Solutions, and Visa)

Acquiring Bank
The bank or financial institution that holds the merchant’s bank account that is used for collecting the proceeds for credit card processing.

Card Associations
Credit card issuing entities such as Visa and MasterCard that govern and oversee the use of credit cards for payment transactions.

Interchange
The process by which all parties involved in a credit card transaction (i.e., processors, acquirers, issuers, etc.) manage the processing, clearing and settlement of credit card transactions, including the assessment, and collection and/or distribution of fees between parties. Also known as Credit Card Interchange.

Merchant
The person or business entity that sells goods or services to a customer.

Merchant Account
A financial institution or bank account that is used by a merchant specifically for the purpose of collecting proceeds consumer bank account or credit card payment transactions. A Card Present (CP) merchant account is used by merchants that receive payments in a physical location where payment is physically presented to the merchant by the customer at the time of the transaction. A Card Not Present (CNP) merchant account is used by merchants that receive payments electronically or in situations where payment is not physically presented to the merchant by the consumer at the time of the transaction.

Payment Application Best Practices (PABP)
Visa has developed "Payment Application Best Practices" to assist software vendors create secure payment applications that help ensure merchant compliance with the PCI Data Security Standard. (From the Visa website, http://www.usa.visa.com/merchants/)

Payment Card Industry Data Security Standard (PCI DSS)
The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. (From the PCICO website, https://www.pcisecuritystandards.org/tech/index.htm)
Payment Gateway
*(UCSB = Authorize.net or Cybersource)*
A system of technologies and processes that allow merchants to electronically submit payment transactions to the payment processing networks (i.e., the Credit Card Interchange and the ACH Network). Payment gateways also provide merchants with transaction management, reporting, and billing services.

Platform
*(UC = North Platform)*
The processing system "engine" the merchant account uses.

Point of Sale (POS)
A term used in the payments industry that refers to the physical location where a payment transaction takes place. POS is also used to describe credit card payment acceptance systems that are designed for the place of sale, such as card swipe terminals.

Processor
An entity in the credit card processing network that handles the posting of transactions for authorization, clearing and settlement to consumer credit card accounts at the card associations; and the settlement of funds to merchant bank accounts. Processors may also provide merchants with billing and reporting services.

Retail
The business of selling merchandise or services to consumers. Merchants that operate in a storefront or physical location and accept Card Present payments—meaning that payment is physically presented to the merchant, and credit cards are “swiped” into a card reading device. Also called “Brick and Mortar.”

Settlement
For credit card transactions, settlement occurs at the completion of transaction processing between the involved financial institutions and processing entities, and funds for the credit card transaction have been successfully deposited into the merchant’s bank account.

Terminal
A piece of electronic hardware, or a device, that is used by a merchant to submit credit card payment information to the processing network. Terminals are connected to the credit card processing network via dial-up telephone connection or Broadband. Also see “POS Device.”

Virtual Point-of-Sale (VPOS) Terminal
A secure, easy-to-use solution that allows retail, or “brick and mortar” merchants, to manually submit transactions using a computer with Windows Internet Explorer, and a MagTek USB HID card reader.
Visa Cardholder Information Security Program (CISP)
A program created by Visa stating its technology and sensitive data security requirements for merchants and merchant service providers. Compliance is required of its member institutions.
Self Assessment Questionnaires
Courtesy of Sabrina Hagberg, First Data

SAQ A
SAQ Validation Type 1 / SAQ A:
Card-not-present, All Cardholder Data Functions Outsourced

- SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises.
- Merchants in Validation Type 1 do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises, and must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:
  - Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
  - Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on a third party to handle these functions;
  - Your company has confirmed that the third party handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
  - Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; and
  - Your company does not store any cardholder data in electronic format.
- This option would not apply to merchants with a 100% face to face POS environment.
SAQ B

SAQ Validation Type 2 / SAQ B
Imprint Merchant Only, No Electronic Cardholder Data Storage

- SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or stand-alone dial-up terminals.
- Merchants in Validation Type 2 only process cardholder data via imprint machines, and must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:
  - Your company uses only an imprint machine to take your customers’ payment card information;
  - Your company **does not transmit cardholder data over either a phone line or the Internet**;
  - Your company retains only paper copies of receipts; and
  - Your company does not store cardholder data in electronic format.

SAQ Validation Type 3 / SAQ B
Standalone, Dial-out Terminal Merchant, no Electronic Cardholder Data Storage

- SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or stand-alone dial-up terminals.
- Merchants in Validation Type 3 process cardholder data via stand-alone, dial-out terminals, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchants.
- Merchants in Validation Type 3 must validate compliance by completing SAQ B and the associated Attestation of Compliance, confirming that:
  - Your company uses only standalone, dial-out terminals (**connected via a phone line to your processor**);
  - The standalone, dial-out terminals are not connected to any other systems within your environment;
  - The standalone, dial-out terminals are not connected to the Internet;
  - Your company retains only paper reports or paper copies of receipts; and
  - Your company does not store cardholder data in electronic format.
SAQ C

SAQ Validation Type 4 / SAQ C
Merchants with Payment Application Systems Connected to the Internet

• SAQ C has been developed to address requirements applicable to merchants whose payment application systems (e.g., point-of-sale or shopping cart systems) are connected to the Internet either because:
  1. The payment application system is on a pc that is connected to the Internet (e.g., for email or browsing), or
  2. The payment application system is connected to the Internet to transmit cardholder data.

• Merchants in Validation Type 4 process cardholder data via payment application systems connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone-order (card-not-present) merchants.

• Merchants in Validation Type 4 must validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:
  1. Your company has a payment application system and an Internet connection on the same device;
  2. The payment application system/Internet device is not connected to any other systems within your environment;
  3. Your company retains only paper reports or paper copies of receipts;
  4. Your company does not store cardholder data in electronic format; and
  5. Your company’s payment application software vendor uses secure techniques to provide remote support to your payment application system.
SAQ D

SAQ Validation Type 5 / SAQ D
All Other Merchants and All Service Providers Defined by a Payment Brand as Eligible to Complete an SAQ

- SAQ D has been developed to address requirements applicable to all merchants who do not fall under Validation Types 1-4.
- Merchants in Validation Type 5 must validate compliance by completing SAQ D and the associated Attestation of Compliance.
- While many of the organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to wireless technology.
Credit Card Reconciliation Process

- All credit card receipts from all campus departments are deposited via Bank of America Merchant Services, to the UCSB Bank Account at Bank of America.

- Based on the Bank of America statement, Accounting clears the UCSB bank account by crediting campus merchants for the deposits, and debiting departments for the fees associated with acceptance of credit cards on the campus.

- On the first day of the month (i.e., March), Accounting emails to the department a spreadsheet, showing the total receipts collected for the prior month (i.e, February), as indicated on our Bank of America statement.

- Based on the Bank of America statement, Accounting prepares a journal that debits the department/merchant’s clearing account for the deposits and credits the department/merchant’s clearing account for the fees.

- The department then needs to prepare a journal that debits their clearing account, and credits the appropriate department account for the income.

- The department also prepares a journal that credits their clearing account, and debits the appropriate department account for the fees. Object Code 7226 should be used for this entry. The fees are one month in arrears.

- The department should reconcile the transactions between the Bank of America statement, the Bank of America Merchant Services statement and any internal records kept for deposits.
Internet Gateways with UC Agreements

Authorize.net
http://www.authorize.net

Card Not Present
Gateway Fee: $10.00/mo
Transaction Fee: $.03/transaction
Reactivation Fee $25

Retail
Set up Fee: $49
Gateway Fee: $8.00/mo (includes 100 transactions)
Transaction Fee: $.04/transaction
Reactivation Fee $25

Cybersource
http://www.cybersource.com

$19.95/mo, plus $.10/transaction

RegOnline
http://www.regonline.com/

4.95% processing fee for Visa / MC using them as a Gateway (card processor) or; .95% processing fee if using another Gateway like Auth.net PLUS, $3.75 per registration
# Credit Card Terminals

*University of California Updated pricing 12/22/2008*

<table>
<thead>
<tr>
<th>TERMINALS</th>
<th>Rental</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD 50 TERM</td>
<td>$16.50</td>
<td>$349.00</td>
</tr>
<tr>
<td>FD100 TERM</td>
<td>$22.00</td>
<td>$439.00</td>
</tr>
<tr>
<td>FD200 TERM AND CHECK</td>
<td>$28.00</td>
<td>$669.02</td>
</tr>
<tr>
<td>FD300 MULTI MERCH</td>
<td>$28.00</td>
<td>$648.18</td>
</tr>
<tr>
<td>FD400 WIRELESS</td>
<td>$28.00</td>
<td>$799.25</td>
</tr>
<tr>
<td>FD20 CONTACTLESS READER</td>
<td>$28.00</td>
<td>$218.43</td>
</tr>
<tr>
<td>T7PLUS *</td>
<td>$35.00</td>
<td>$550.00</td>
</tr>
<tr>
<td>VX570</td>
<td>$35.00</td>
<td>$675.00</td>
</tr>
<tr>
<td>NURIT 8000</td>
<td>$60.00</td>
<td>$1,095.00</td>
</tr>
</tbody>
</table>

### OLD TERMINALS:

<table>
<thead>
<tr>
<th>TERMINALS</th>
<th>Rental</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>T330</td>
<td>$30.00</td>
<td>$400.00</td>
</tr>
<tr>
<td>T380</td>
<td>$35.00</td>
<td>$450.00</td>
</tr>
<tr>
<td>T380X2-256K</td>
<td>$35.00</td>
<td>$490.00</td>
</tr>
<tr>
<td>ECLIPSE</td>
<td>$45.00</td>
<td>$725.00</td>
</tr>
<tr>
<td>OMNI 3200 *</td>
<td>$39.00</td>
<td>$595.00</td>
</tr>
<tr>
<td>OMNI 3750DM *</td>
<td>$39.00</td>
<td>$675.00</td>
</tr>
</tbody>
</table>

### PINPADS:

<table>
<thead>
<tr>
<th>PINPADS</th>
<th>Rental</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD10</td>
<td>$12.50</td>
<td>$127.27</td>
</tr>
<tr>
<td>FD10C</td>
<td>$13.00</td>
<td>$127.27</td>
</tr>
<tr>
<td>PP1000SE (3 DES) *</td>
<td>$15.00</td>
<td>$175.00</td>
</tr>
<tr>
<td>S9 (3 DES) *</td>
<td>$15.00</td>
<td>$225.00</td>
</tr>
</tbody>
</table>

### PRINTERS:

<table>
<thead>
<tr>
<th>PRINTERS</th>
<th>Rental</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>P900</td>
<td>$26.00</td>
<td>$296.00</td>
</tr>
</tbody>
</table>

* Denotes a 5 year warranty. Swaps = $50.
-- All other terminals only have a 1 year warranty.

**MAINTENANCE PROGRAM**

<table>
<thead>
<tr>
<th></th>
<th>PER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Program</td>
<td>$8.00</td>
</tr>
</tbody>
</table>
Resources

Contacts

Jonelle Miller
Credit Card Coordinator
805-893-3959
Jonelle.Miller@bfs.ucsb.edu

Neil Clark
Associate Director of Controls
805-893-7667
Neil.Clark@bfs.ucsb.edu

Russell Remington
General Accounting Supervisor
Credit Card Reconciliation
805-893-2372
Russell.Remington@bfs.ucsb.edu

Kimberly Tapia
Contracts Manager
805-893-5836
kimberly.tapia@bfs.ucsb.edu

Meta Clow
Campus Policy and Records Management Coordinator
805-893-4212
meta.clow@vcadmin.ucsb.edu

Policies

BUS-49, Policy for Cash and Cash Equivalents Received
http://policy.ucop.edu/doc/3420337/BFB-BUS-49

Use of University Logo
http://www.policy.ucsb.edu/policies/logo/

Terms of Use
http://www.policy.ucsb.edu/terms_of_use/