UCSB Credit Card Merchant Handbook

Business & Financial Services
Office of the Controller

Credit Card Merchant Support
merchant.support@bfs.ucsb.edu
Table of Contents

Introduction to Credit Card Processing at UCSB
Steps to Becoming a Credit Card Merchant
Credit Card Acceptance Considerations
Credit Card Merchant Responsibilities
Credit Card Processing Methods
  e-commerce: Website Sales of Goods and Services
    Department/Unit Hosted Website
    Supplier Solutions
  e-commerce: Conferences/Events
    Use Regonline for Event/Conference Registration (Preferred Solution)
    Department Developed Web Site
    Third-Party Supplier Solution
Retail & MO/TO
  P2PE Terminal Requirement for Retail & MO/TO Merchants
Credit Card Fees
  PCI Compliance Fees
  Credit Card Acceptance Fees
  Gateway Fee
Credit Card Terminal Pricing (updated 09/01/2016)
Credit Card Reconciliation
Working with Third-Party Suppliers
  General Requirements of Third-Party Suppliers
    Payment Card Industry Standards (PCI)
    Payment Application Data Security Standard (PA-DSS)
    Certificates of Insurance
  Using Suppliers not Integrated with UCSB’s Acquirer (Merchant Processor)
PCI Compliance Requirements
  Non-Compliance with PCI DSS Requirements
  Security Awareness Education (SAE) Training Requirements
  SAQ Types
Incident Response: Suspected Cardholder Data Compromise
  Notification Procedures
  Preserve Evidence
  Information Security
  Department Operations After a Report of Compromise
Credit Card Merchant Responsibilities Acknowledgement
PCI Security Awareness Education Training Acknowledgment
Appendix A: Credit Card Merchant Terminology
Appendix B: Resources
Appendix C: Merchant Card Processing Basics
  Suggested Reading: Visa’s Card Acceptance Guidelines for Visa Merchants
  Merchant Best Practices
  Transaction Life Cycle
  Authorization Responses
  Chargebacks and Retrieval Requests
Introduction to Credit Card Processing at UCSB

UCSB's Campus Credit Card Coordinator (“Coordinator”) works with departments to enable them to accept credit card payments for products and services. These “merchants” are required to accept credit cards in a safe, secure manner that is in compliance with the Payment Card Industry (PCI) requirements for safeguarding cardholder account numbers and other sensitive data, as well as applicable University/UCOP policies.

In this handbook you will find a wide range of information, guidelines, and resources related to credit card processing. All prospective and current merchants are responsible for reading, understanding, and complying with this information. Please contact merchant.support@bfs.ucsb.edu with any questions, or to arrange a conversation about your payment acceptance needs.

Steps to Becoming a Credit Card Merchant

The first step for a department or unit that would like to accept credit cards is to have a discussion with the Coordinator. At that time, the department/unit will discuss their plans, potential revenue, etc. In addition, the Coordinator will review with them all aspects of credit card acceptance, including approval from the Chancellor, the type of setup the unit/department is requesting, potential suppliers and solutions, associated fees, and UC, campus, and regulatory policies and requirements.

Campus 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 responsibilities and costs of meeting compliance requirements, 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, which is routed to the Coordinator, the campus Controller and on to the Chancellor. The Coordinator will supply a template that can be used as the basis for the letter.
Credit Card Acceptance Considerations

A department wishing to apply for a credit card merchant account has many things to consider:

1. **Potential revenue.** If the event/conference/sales will be less than $10,000, it may be in the department's best interest to use RegOnline or accept only cash and checks, due to the workload involved with administering and reconciling a merchant account. If the event/conference/sales will be over $10,000, then establishing a merchant account for credit card acceptance may be the best option. If the expected revenue will be greater than $10,000, then the department needs to work with General Accounting to establish a new revenue account and evaluate the revenue for potential trigger of Unrelated Business Income Taxes (UBIT).

2. **Frequency of Sales.** If the event/conference will be held only one time, or sales of items will be for a limited time, it may be in the department's best interest to accept only cash and checks due to the costs and workload involved with administering and reconciling a merchant account. The department should consult with the Campus Credit Card Coordinator to discuss best options, especially if it will be a one-time only event.

3. **Technical Support.** Depending on the method of credit card acceptance, departments will need varying degrees of technical support from their IT staff. Merchants may also need technical support to complete the required annual PCI validation.

4. **Department Staffing Levels.** Acceptance of credit cards requires administration of the account, monitoring, and reconciliation. Departments should consider availability of staff for these functions.

Credit Card Merchant Responsibilities

All UCSB merchants/departments must abide by the following guidelines:

- Departments must not store cardholder data on computers (spreadsheets, etc.), and credit card information (credit card number, expiration date, card verification codes, etc.) must not be transmitted via email. If payments are accepted in-person at a remote location, terminals must be monitored and tracked at all times.
- Each department must designate an individual who holds the primary authority and responsibility for payment card processing.
- Pay the costs associated with payment card processing (bank and interchange fees, equipment fees, if applicable, and other fees as deemed appropriate).
- Comply with all PCI DSS guidelines, UCOP’s Business & Finance Bulletin 49 (BUS-49), Policy for Cash and Cash Equivalents Received, and UCSB’s policies and procedures for payment card acceptance and security.
● Validate PCI compliance annually, which includes the completion of the appropriate Self-Assessment Questionnaire (SAQ) and associated processes, if applicable, as required by the University’s acquiring bank and credit card associations.

● Require all those involved with merchant processes, either directly or as a supervisor, to participate in Security Awareness Education (SAE) training annually and upon hire.

● Notify the Campus Credit Card Coordinator promptly when a merchant credit card account is no longer needed.

● Respond to chargeback notifications and credit card company inquiries in a timely manner (within the timeframe specified on the notification).

● Ensure that cardholder data is not transmitted or obtained via email or stored electronically in any database, application or system.

● Maintain the physical protection of departmental credit card receipts and the secure destruction of payment card receipts and cardholder data once a program has ended and all payments have been reconciled.

● Provide full cooperation with the University’s Campus Credit Card Coordinator and/or authorized third-party assessors whenever necessary.

● Authorize and complete deposit settlement daily (strongly recommend setting up auto-settle, where possible).

Physical Access Control

● Credit card terminals must be kept in a secure location with limited physical access.

● Terminals need to be inspected for tampering at the start of every shift/daily, if applicable, or when putting a terminal into service for those that are stored when not in use. Note: For most campus merchants, the Campus Credit Card Coordinator’s office is responsible for periodic inspections required for PCI compliance validation. For more information, request a copy of “UCSB Device Inspection Guidelines” from the Coordinator.

● Cardholder information (receipts, reports, supporting documentation, etc.) must be secured and limited to only those individuals whose job requires such access.

● “Media” refers to all paper and electronic media containing cardholder data.
  ○ Strict control must be maintained over the internal or external distribution of any kind of media.
  ○ Media must be classified so that the sensitivity can be determined, and it can be adequately safeguarded if it contains sensitive data.
  ○ Physically secure paper media containing sensitive cardholder data at all times (e.g. locked down). A secure location would minimally be defined as one that is
not accessible to the public, particularly if authorized personnel are not always available to monitor security.

- Management’s approval must be obtained prior to moving media, especially when media is distributed to individuals. Logs must be maintained to track all media that is moved from a secured area, and media must be safeguarded during transport.
- Destroy media containing cardholder data when no longer needed in accordance with PCI DSS guidelines.

- Secure locations must have physical access controls (key cards, door locks, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security.
- Develop procedures to help all personnel easily distinguish between employees and visitors.

**Personnel Access Control**

- Passwords should be added for refunds/voids, where possible (used by someone other than who is processing charges).
- Restrict access to cardholder data by business need-to-know basis.
- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Restrict access rights to privileged user IDs to the least privileges necessary to perform job responsibilities.
- Assign privileges based on individual personnel’s job classification and function.
- Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to deny all unless specifically allowed.
- Strong security must be used for all applications, devices, and systems (including shared or dedicated web servers hosting e-commerce sites) in the Cardholder Data Environment (“CDE”), including at a minimum:
  - All default passwords must be changed prior to deploying a system or device.
  - Any unnecessary generic or default user accounts must be removed or disabled prior to deploying a system or device.
  - User IDs and/or passwords must never be shared for any reason.
  - All system access requires at a minimum a User ID and strong password.
  - Passwords must at a minimum have seven or more characters, and contain at least one letter and one number.
All access must be immediately terminated when an employee or contractor leaves the company.

**Storage of Cardholder Data**

Merchants that do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves. However, if a legitimate business need exists:

- Keep cardholder information storage to a minimum. Storage of sensitive cardholder data on any local device or system is prohibited.
- Do not store the Card Verification Value (three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data).
- Ensure secure storage and distribution of university keys.
- Periodically change keys and destroy old keys.
- An inventory must be maintained of all systems, electronic, and paper media containing sensitive cardholder data.

**Transmission and Distribution of Cardholder Data**

- Where authorized, all transmission and distribution of sensitive cardholder data must use a secure method to avoid unauthorized access.
- Never send or accept cardholder or other sensitive information via unencrypted e-mail, Instant Messaging or any other insecure method (e.g. File Transfer Protocol (FTP), Hypertext Transport Protocol etc.).
- Mask the credit card’s Primary Account Number (PAN) when displayed.

**Protecting Cardholder Data**

- When sensitive authentication data is received and deleted, there must be a process in place to securely delete the data and to assure the data is unrecoverable.
- All systems must adhere to the PCI DSS requirements regarding non-storage of sensitive authentication data after authorization.
- Under no circumstance should the full contents of any track from the magnetic stripe be stored. In the normal course of business, the following data elements from the magnetic stripe may need to be retained. To minimize risk, store only these data elements as needed for business.
  - The cardholder’s name
  - Primary account number (PAN)
  - Expiration Date
• Under no circumstance should the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) be stored.
• Under no circumstance should the personal identification number (PIN) or the encrypted PIN block be stored.

Maintain an Information Security Policy
All merchants should maintain a policy that addresses information security for all personnel. “Personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants have access to the cardholder data environment.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. The security policy should be reviewed at least once a year and updated as needed to reflect any changes to business objectives or the risk environment.

Disposal and Reuse of Hardware, Electronic and Paper Media

• Hardcopy media must be destroyed when it is no longer needed for business or legal reasons.
• Destruction of hardcopy media must be cross-cut shredded, incinerated or pulped so that cardholder data cannot be reconstructed. If this is not possible, credit card numbers and personal information must be “blacked-out” before destroying.
• Containers that store cardholder data to be destroyed must be secured to prevent access to the contents. Example: a “to-be-shredded” container must have a lock preventing access to its contents.
• Shred, incinerate, pulp or “black-out” paper media containing cardholder data so that it cannot be reconstructed.

Incident Reporting
In the event of a verified or suspected security breach in which a person’s Personal Information is reasonably believed to have been stolen by an unauthorized person, the breach must be reported immediately to a supervisor, and the department/merchant responsible party must follow the instructions in the section, Incident Response: Suspected Cardholder Data Compromise, below.
Credit Card Processing Methods

There are many options available to departments that want to accept credit cards. Departments can accept credit cards over the web/internet (e-commerce), in person (retail), or by mail/over the phone (MO/TO). Credit cards can be accepted for goods and services, such as tickets to events, parking permits, registration fees associated with conferences the department/unit is hosting, dining, lodging, and other purposes. Each of these needs may have several solutions the merchant can consider in consultation with the Coordinator. Note: All options require coordination with the Campus Credit Card Coordinator to establish accounts and gateways.

e-commerce: Website Sales of Goods and Services

I. Department/Unit Hosted Website

For this option, the department/unit typically has technical support staff that can create a website to display the goods/services available for purchase, and may capture non-sensitive customer information during the purchase process. This can be accomplished using a custom-built database, or merchants may choose to use an approved third-party shopping cart. To complete the purchase using credit cards, this setup requires redirection to an approved, completely outsourced payment gateway, and does not allow for any processing, storage, or transmission of credit card data. This is also known as the “click to pay” model, because users are redirected to a payment gateway for secure collection of credit card data.

II. Supplier Solutions

A. UC Approved Supplier

Another option for accepting credit cards online is to use an approved UC supplier that can provide, or facilitate the development of, a website. The website can manage inventory, collect non-sensitive customer information, provide reports, and more. In almost all cases, this setup requires redirection to a completely outsourced payment gateway to complete transactions, and does not allow for any processing, storage, or transmission of credit card data (exceptions will be considered on a case-by-case basis by the Coordinator).

B. Third-Party Supplier

If a department/unit has a need to sell goods/services and wishes to use a supplier that does not currently have an approved agreement with UCSB or the UC system, the supplier must meet certain guidelines prior to signing any
agreement. The agreement must be submitted to, and approved by, the campus Procurement Services group to ensure it meets all required standards. The Coordinator will participate in the review to address all credit-card related concerns. For more details, see Working with Payments Processing Suppliers, below.

**e-commerce: Conferences/Events**

I. **Use Regonline for Event/Conference Registration *(Preferred Solution)***

RegOnline is a UC system-wide supplier, and has all the functionalities that departments need to design and maintain an online event registration system ([http://www.lanyon.com/features](http://www.lanyon.com/features)). For credit card acceptance, departments use RegOnline’s payment processing, so there is no separate merchant application necessary and no PCI Compliance requirements to manage. RegOnline then sends a check for department for the revenue collected minus fees. Fees for RegOnline are currently $2.30 per registration plus 3.5% of transaction amounts processed by credit card.

II. **Department Developed Web Site**

If a department has IT support, the department will need to develop a website, with a backend database to collect demographic information about the participants who are registering for the events/conferences. This will allow the department to do reporting and have information about the participants. To complete the registration using credit cards, this setup requires redirection to a completely outsourced payment gateway, and does not allow for any processing, storage, or transmission of credit card data.

III. **Third-Party Supplier Solution**

For more details, see Working with Payments Processing Suppliers, below.

**Retail & MO/TO**

To accept credit cards in person, or through the mail or over the phone, the department/merchant must use a secure physical terminal (Virtual Terminal, the typing of credit card information into an internet browser using a computer’s keyboard or non-approved device, is not allowed).

Payment terminals are generally rented or purchased from an approved supplier, and will usually be requested by the Coordinator. In certain circumstances, a merchant may purchase
equipment from another supplier when specific terminals are required. Prices vary per month depending on the type of terminal. See Credit Card Terminal Pricing for current costs.

**P2PE Terminal Requirement for Retail & MO/TO Merchants**

PCI-validated P2PE (Point to Point Encryption) solutions are the most secure processing systems currently available, and significantly reduce annual validation costs and resource requirements, as well as offering the highest security for the cardholders who do business with the University. UCSB has contracted with Bluefin Payment Systems as the primary provider of approved P2PE solutions, including terminals for retail, mobile, and MO/TO merchants.

UCSB requires all new credit card processing solutions to use P2PE solutions wherever possible. Existing merchants are encouraged, but not required, to replace terminals with P2PE solutions. The Coordinator can discuss non-P2PE solutions with merchants, if a merchant feels there is a reason why P2PE is not a preferred or viable option.

*Note: Many suppliers claim to offer P2PE solutions, but ONLY solutions listed on the PCI SSC website are validated, approved by UCSB, and guarantee the automatically reduced scope of PCI compliance efforts. Non-validated solutions will be considered by the Coordinator on a case-by-case basis, but will subject the merchant to significant additional compliance fees. The list is continually updated here.*

**Credit Card Fees**

There are many costs to accepting credit cards. Fees include, but may not be limited to:

**PCI Compliance Fees**

There can be one or more fees related to PCI compliance for a merchant. For example:

- $67/year for each self-assessment questionnaire (“SAQ”). This is a pass-through fee assessed by the Office of the Controller to departments via a journal on an annual basis. A merchant can have more than one SAQ, depending on how many merchant accounts and processing environments are supported (e.g., e-commerce and retail);
- $500 to $2,500 for a QSA Facilitated SAQ, if required due to an unusual or complex processing environment, or at a department’s request;
- $1,000 to $10,000+ for external/internal network scans and penetration testing, depending on the complexity of the processing environment (SAQ-C and -D, primarily);
- $9,000+ for a QSA examination of a non-validated P2PE environment (i.e., not listed as a validated solution on the PCI SSC website)
Credit Card Acceptance Fees

For most UCSB merchants, these fees total approximately 2-2.5% of the transaction, and are identified in the monthly statement that comes from Bank of America Merchant Services (“BAMS”). Certain types of merchants may be subject to higher fees, depending upon how they are classified by the Acquiring Bank.

- **Processor Fee**: Charged and collected by BAMS
- **Access & Assessments**: Collected by BAMS and forwarded to VISA and Mastercard
- **Interchange**: Collected by BAMS and forwarded to the bank that issued the credit card

Gateway Fee

If applicable (e.g., for e-commerce transactions), these additional fees are charged by the Gateway used to process the transaction. They are included on the monthly bank statement from Bank of America, and are identified on the financial journal as part of the total fees.

- **Authorize.net**: e-commerce account is $10.00/month and $.03/transaction
- **Bluefin Payment Systems**: e-commerce transactions are $.05 each, with no monthly fee

Credit Card Terminal Pricing (updated 09/01/2016)

<table>
<thead>
<tr>
<th>BAMS/FIRST DATA TERMINALS:</th>
<th>Rental</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD130 / FD130 DUO TERMINAL</td>
<td>$35.90</td>
<td>$600.00/$728.00</td>
</tr>
<tr>
<td>FD35 PIN PAD</td>
<td>$12.50</td>
<td>$128.00</td>
</tr>
<tr>
<td>FD410 WIRELESS (ADDITIONAL CELLULAR FEE MAY APPLY)</td>
<td>$92.00</td>
<td>$701.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BLUEFIN P2PE TERMINALS*:</th>
<th>Purchase</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAX S500 STANDALONE (IP)</td>
<td>$349.00</td>
</tr>
<tr>
<td>NOMAD BLUETOOTH (REQUIRES IOS DEVICE)</td>
<td>$125.00</td>
</tr>
<tr>
<td>SREDKEY KEYPAD (USB)</td>
<td>$249.00</td>
</tr>
<tr>
<td>PAX D210 (WiFi)</td>
<td>$500.00</td>
</tr>
</tbody>
</table>

*Other terminals may be available for specific supplier solutions. Bluefin terminals are each subject to a one-time encryption “key injection” fee of $35.00, plus shipping costs, and $25/mo P2PE “device management” fee.

Credit Card Reconciliation

All campus credit card revenue and fees are deposited/charged to one central campus bank account. General Accounting reviews the bank statement and distributes the revenue and fees to a balance sheet account assigned to each merchant. Departments are responsible for transferring their revenue and fees to the appropriate department revenue and expense accounts in coordination with General Accounting.
Credit card reconciliation can be a complex process requiring review of multiple statements to ensure revenue and fees are accounted for appropriately. The following is a list of steps in the 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, Gateway deposit records (if applicable), and any internal records kept for deposits.

**Working with Third-Party Suppliers**

UCSB departments will, whenever possible, use suppliers previously vetted by Office of the President (UCOP) or UCSB to ensure security, PCI DSS compliance, and efficient use of University resources.

If not using an UCOP/UCSB vetted supplier, departments must ensure third-party service providers, and their payment software, gateways, equipment, and outsourced payment services, are PCI DSS compliant and the appropriate data security language must be included in all contracts with third party service providers involving payment card acceptance. Third party payment solutions must be approved by the Coordinator and Procurement Services.
General Requirements of Third-Party Suppliers

In general, if a department wants to work with an outside (third-party) supplier to sell goods and/or services on behalf of the UC Regents, the supplier must meet the following requirements:

- Will use the University merchant account
- Will use a UC Approved gateway
- Can demonstrate PCI compliance with evidence of passing PCI certification
- Is listed on the PCI approved Payment Applications (if appropriate)
- Will accept all terms and conditions of the UC Data Security and PCI Addendums
- Is willing to negotiate terms and conditions as part of the contract process

The following is additional information about some of these requirements.

Payment Card Industry Standards (PCI)

Any supplier that 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. PCI validation must be verified by the merchant or Coordinator annually, and any supplier that fails to maintain compliance with PCI standards is subject to being discontinued as an approved supplier to UCSB merchants.

Payment Application Data Security Standard (PA-DSS)

Depending on the type of product offered by the supplier, the supplier may also have to certify their product was developed according to the PA-DSS. Suppliers listed on the PCI SSC website’s List of Validated Payment Applications (https://www.pcisecuritystandards.org) or Visa’s Global Registry of Service Providers (http://www.visa.com/splisting/) are automatically accepted as being compliant with PA-DSS.

Certificates of Insurance

Any supplier that 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 supplier.

NOTE: Departments need to be very aware of the requirements outlined above. Many times smaller businesses/suppliers will not be able to meet the PCI and/or 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 supplier.

Using Suppliers not Integrated with UCSB’s Acquirer (Merchant Processor)

UCSB has contractual obligations with its merchant processor. When contracting with third-party suppliers that use their own merchant processor, an exception may need to be obtained
from UCSB’s acquiring bank, and written Variance approved by the Controller’s Office may be required before implementation.

**PCI Compliance Requirements**

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure ALL merchants that process, store or transmit credit card information maintain a secure environment.

PCI DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

The following is important information for each merchant to know about PCI compliance at UCSB:

- UCSB works to ensure that all merchants are 100% PCI compliant as validated on a specific date each year. Merchants must complete their validation by the given date, unless prior arrangements are made with the Coordinator, or will risk having their credit card acceptance privileges suspended or revoked. Non-compliance can also result in fines and other penalties from the card brands and/or our acquiring bank.
- PCI validation is an annual requirement to attest that at a single point-in-time (the finish date of the validation for that year), a merchant is in compliance with PCI DSS requirements. However, merchants are obligated, as part of the conditions of accepting credit cards, to be compliant at all times (24x7x365). Never make changes to your processing environment (e.g., changing POS security settings, changing terminals, etc.) without considering how the changes might affect PCI compliance, and credit card security in general.
- To comply with PCI DSS, campus merchants must validate their compliance by completing an annual self-assessment questionnaire (SAQ). An online portal called Coalfire One (formerly Navis, available at [https://idp.coalfire.com/account/signin](https://idp.coalfire.com/account/signin)) is supplied by the UC’s contracted QSA, Coalfire Systems, for easier and more efficient completion of the assessment.
- Each merchant must designate a Primary PCI Contact for each credit card processing environment, and the Coordinator will establish a Coalfire One login account for that person.
While each merchant is responsible for completing their own SAQ(s), the Coordinator will provide guidance where possible, and/or will arrange for a quote for facilitated assistance from our QSA at UC-negotiated prices.

Non-Compliance with PCI DSS Requirements

Failure to comply with the PCI DSS can result in:

- Large fines and fees assessed by each card brand
- Civil fees and audit costs
- A loss of reputation and payment card privileges for the University
- Notifications to all customers affected
- Additional costly, ongoing PCI DSS reporting requirements.

The non-compliant UCSB department is liable for all costs associated with a data breach. In addition, employees may be subject to disciplinary action or termination (in accordance with Human Resources policies and procedures) if they fail to adhere to the University’s policies and procedures for payment card acceptance or for the mishandling of cardholder data and/or payment card fraud.

Security Awareness Education (SAE) Training Requirements

Each University of California employee is responsible to safeguard the information assets entrusted to us. The UC Office of the President requires all employees to complete Cyber Security Awareness Training upon hire, and annually thereafter. In addition, every UCSB employee involved with any aspect of credit card processing, including student workers, must complete the PCI DSS Security Awareness Training upon initial hire, and on an annual basis thereafter. To access the training, access the UC Learning Center (https://www.learningcenter.ucsb.edu/) and enter “PCI” in the Search field. The training takes approximately 20 minutes.

SAQ Types

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants report the results of their PCI DSS self-assessment. Merchants should ensure they meet all the requirements for a particular SAQ before using the SAQ. The correct SAQ will be selected in consultation with the Coordinator, the supplier of the POS system in use, our QSA, and through the Coalfire One portal’s selection wizard.

There are currently eight SAQs covering various processing environment, but except in extraordinary circumstances, UCSB only allows systems that qualify for the following
(definitions directly from PCI DSS documentation; a full list of SAQ types and qualifying factors is available on the PCI SSC website (https://www.pcisecuritystandards.org/):

SAQ-A
Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises. Not applicable to face-to-face channels.

SAQ-B
Merchants using only:
• Imprint machines with no electronic cardholder data storage; and/or
• Standalone, dial-out terminals with no electronic cardholder data storage.
Not applicable to e-commerce channels.

SAQ-P2PE (preferred for Retail & MO/TO merchants)
Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.

SAQ-C (by exception only)
Merchants with payment application systems connected to the Internet. No e-commerce or electronic cardholder data storage.

SAQ-D (by exception only)
All merchants not included in descriptions for the above SAQ types.

Incident Response: Suspected Cardholder Data Compromise
An incident, for purposes of this plan, is defined as a suspected or confirmed compromise of cardholder data. At a minimum, cardholder data consists of the full card number. Cardholder data may also appear in the form of the full card number plus any of the following: cardholder name, expiration date and/or sensitive authentication data. A cardholder data compromise is any situation where intrusion into a computer system occurs and unauthorized disclosure, theft, modification, or destruction of cardholder data is suspected or the suspected or confirmed loss or theft of any material or records that contain cardholder data.
Departments that suspect or have confirmed an account data compromise must take prompt action to prevent additional exposure of payment card data. The following steps must be taken:

1. Immediately notify the appropriate University contacts. See details.
2. Immediately contain and limit the exposure and preserve evidence. See details.
3. Document any steps taken until contacted by the Coordinator. Include the date, time, person/persons involved and action taken for each step.
4. Assist the Coordinator, UCSB’s Information Security team, and any other personnel as they investigate the incident.
5. The Coordinator has additional reporting responsibilities, including notifying our compliance vendor (the UC’s QSA, Coalfire Systems), and the following:
   a. For incidents involving Visa, MasterCard or Discover network cards, contact BAMS Merchant Incident Response Team at (800) 228-5882 within 72 hours of the reported incident. For further information, see the document “Responding to a Breach: A Guide Provided by Bank of America Merchant Services” at https://merch.bankofamerica.com/assets/documents/10162/12961/responding breach.pdf
   b. For incidents involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident at (888) 732-3750 or email EIRP@aexp.com.
   c. Additional resources:
      i. MasterCard – Responding to a Breach: Follow the steps set forth in the resource Account Data Compromise User Guide
      ii. Visa – Responding to a Breach: Follow the steps set forth in the resource What To Do If Compromised Guide
      iii. American Express – Responding to a Breach: Follow the steps set forth in section two of AMEX Data Security Operating Policy – U.S.

Notification Procedures
If you suspect a compromise of credit card data, notify the following contacts immediately:

Matt Coy, Campus Credit Card Coordinator
matt.coy@ucsb.edu | (805) 893-3959

Sam Horowitz, Chief Information Security Officer
samh@ucsb.edu | (805) 893-5005
Preserve Evidence

The following guidelines are courtesy of Visa’s “What To Do If Compromised” publication (https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf).

To identify the root cause and facilitate investigations, it is important to ensure the integrity of the system components and environment by preserving all evidence.

- Do not access or alter compromised system(s) (e.g., do not log on to the compromised system(s) and change passwords; do not log in with administrative credentials). Visa strongly recommends that the compromised system(s) be taken offline immediately and not be used to process payments or interface with payment processing systems.
- Do not turn off, restart, or reboot the compromised system(s). Instead, isolate the compromised systems(s) from the rest of the network by unplugging the network cable(s) or through other means.
- Identify and document all suspected compromised components (e.g. PCs, servers, terminals, logs, security events, databases, PED overlays etc.).
- Document containment and remediation actions taken, including dates/times (preferably in UTC), individuals involved, and detailed actions performed.
- Preserve all evidence and logs (e.g. original evidence such as forensic image of systems and malware, security events, web logs, database logs, firewall logs, etc.).

Information Security

UCSB’s Information Security will follow their protocols for data security breaches, which is governed by the University of California’s “UC Privacy and Data Security Incident Response Plan” (http://www.ucop.edu/information-technology-services/_files/uc_incidentresp_plan.pdf).

Department Operations After a Report of Compromise

The Department may continue business operations, excluding credit card acceptance, until notified by the Coordinator that they may resume credit card processing activities.
● In the event the breach occurs at a department with multiple credit card processing methods (ecommerce, registers, etc.), the credit card processing activity for each method must be suspended until the notification is received from the Coordinator that a method may be resumed.

● If the breach is not isolated to a single department's processing environment, all credit card processing activity across campus is subject to suspension until Coordinator notifies each department that it is acceptable to resume operations.
Credit Card Merchant Responsibilities Acknowledgement

To be signed and returned to merchant.support@bfs.ucsb.edu by an authorized department representative.

I have thoroughly read the UCSB Credit Card Merchant Handbook, and understand the Credit Card Merchant Responsibilities outlined in the handbook; and, I understand that my department must follow PCI DSS and BUS-49 requirements in the handling of credit card data. The Campus Credit Card Coordinator reserves the right to suspend or terminate my department’s ability to process credit card payments at any time if sufficient security measures are not employed. By signing below, I acknowledge that I understand the responsibilities and requirements of being a Credit Card Merchant at UCSB.

Department Name: _____________________________________________________________

Your Name & Title: __________________________________________________________________________

Email Address: _____________________________ Ext: ________________

Signature: _____________________________ Date: ________________

Merchant Account(s) This Acknowledgement Covers:
(please list below either the account name/DBA (e.g., “UCSB Concessions”) or Merchant ID (12 digits) of all merchant accounts your acknowledgement covers)

__________________________________________________________________________________________

__________________________________________________________________________________________

__________________________________________________________________________________________

__________________________________________________________________________________________

__________________________________________________________________________________________

__________________________________________________________________________________________
PCI Security Awareness Education Training Acknowledgment

Each University of California employee is responsible to safeguard the information assets entrusted to us. The UC Office of the President requires all employees to complete Cyber Security Awareness Training upon hire, and annually thereafter. In addition, every UCSB employee involved with any aspect of credit card processing, including student workers, must complete the PCI DSS Security Awareness Training upon initial hire, and on an annual basis thereafter. To access the training, access the UC Learning Center (https://www.learningcenter.ucsb.edu/) and enter “PCI” in the Search field. The training takes approximately 20 minutes.

Credit Card Merchant PCI Training Acknowledgement

To be signed and returned to merchant.support@bfs.ucsb.edu by an authorized department representative.

I certify that all personnel involved in the handling of Cardholder Data for any of the Merchant Accounts listed below have completed the required class, “PCI DSS Security Awareness Training,” either upon hire (if less than one year ago), or within twelve months of the employee’s last successful completion of the training.

Department Name: _____________________________________________________________

Your Name & Title: __________________________________________________________________

Email Address: _____________________________________________ Ext: ______________

Signature: _______________________________________________ Date: ______________

Merchant Account(s) This Acknowledgement Covers:
(please list below either the account name/DBA (e.g., “UCSB Concessions”) or Merchant ID (12 digits) of all merchant accounts your acknowledgement covers)

________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
________________________________________
Appendix A: Credit Card Merchant Terminology

(courtesy of Authorize.net www.authorize.net, and PCI Security Standards

Acquiring Bank
(UCSB = Bank of America Merchant Services (aka “BAMS”))
Also referred to as “merchant bank,” “merchant processor,” “acquirer,” or “acquiring financial institution” Entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. Note: UCSB is required to report the PCI compliance status of our merchants to our acquiring bank, BAMS.

Approved Scanning Vendor (“ASV”)
Company approved by the PCI Security Standards Council to conduct scanning services to identify common weaknesses in system configuration. The UC’s QSA, Coalfire Services, is our ASV.

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

Card Data / Customer Card Data
At a minimum, card data includes the primary account number (PAN), and may also include cardholder name and expiration date. The PAN is visible on the front of the card and encoded into the card’s magnetic stripe and/or the embedded chip. Also referred to as cardholder data. See also Sensitive Authentication Data for additional data elements which may be part of a payment transaction but which must not be stored after the transaction is authorized.

Chip / Chip Card / EMV (“Europay MasterCard Visa”)
Also known as “EMV Chip.” The microprocessor (or “chip”) on a payment card used when processing transactions in accordance with the international specifications for EMV 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. For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

**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.

**Mobile Payment Acceptance**
Using a mobile device to accept and process payment transactions. The mobile device is usually paired with a commercially available card-reader accessory. Only approved, secure mobile card readers may be used by UCSB merchants; consult the Coordinator for processing options.

**MO/TO (“Mail Order / Telephone Order”)**
The business of selling merchandise or services to consumers, where card payments are received through the mail or by telephone. Credit cards are typed into an internet-based payment portal using a secure, approved card reading device.

**P2PE / PCI-Listed Point-to-Point Encryption Solution**
Encryption solution that has been validated per the PCI Point-to-Point-Encryption (P2PE) standard and is listed on the PCI Council website.

**Payment Gateway**
(UCSB = Authorize.net or Bluefin Payment Systems)
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.

**Payment Processor / Processor**
Entity engaged by merchants to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers (merchant banks) unless defined as such by a payment card brand. Also called a “payment gateway” or “payment service provider” (PSP). See also Merchant Bank.

**Payment System**
Encompasses the entire process for accepting card payments in a merchant retail location (including stores/shops and e-commerce storefronts) and may include a payment terminal, an electronic cash register, other devices or systems connected to the payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to a merchant bank.

**PCI**
Acronym for “Payment Card Industry.”

**PCI DSS**
Acronym for the PCI Council's “Payment Card Industry Data Security Standard.” 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. Everyone storing, processing or transmitting cardholder information is required to follow the Payment Card Industry Data Security Standard (PCI DSS).

**PCI DSS Compliant (“PCI Compliant”)**
Meeting all applicable requirements of the current PCI DSS, on a continuous basis via a business-as-usual approach. Compliance is assessed and validated at a single point in time; however, it is up to each merchant to continuously follow the requirements in order to ensure robust security. Merchant banks and/or the payment brands may have requirements for formal annual validation of PCI DSS compliance.
PCI DSS Validated
Providing proof that all applicable PCI DSS requirements are met at a single point in time. Depending on specific merchant bank and/or payment brand requirements, validation can be achieved through the applicable PCI DSS Self-Assessment Questionnaire or by a Report on Compliance resulting from an onsite assessment.

Processing Platform / Platform
(UC = FDMS North, Nashville Platforms)
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.

Qualified Security Assessor (“QSA”)
A company approved by the PCI Security Standards Council to validate an entity’s adherence to PCI DSS requirements. Note: Coalfire Services is the QSA for the entire UC system.

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.”

Self Assessment Questionnaire (“SAQ”)
PCI DSS validation tool used to document self-assessment results from an entity’s PCI DSS assessment. Every credit card merchant is required to complete the SAQ appropriate for their processing environment annually. Note: UCSB merchants complete the SAQ on Coalfire System’s online portal, Coalfire One.
Sensitive Authentication Data
Security-related information including, but not limited to, card validation codes/values (e.g., three-digit or four-digit value printed on the front or back of a payment card, such as CVV2 and CVC2 data), full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. **Sensitive authentication data must not be stored after authorization.**

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.

Payment Terminal
Hardware device used to accept customer card payments via swipe, dip, insert, or tap. Also called “point-of-sale (POS) terminal,” “credit card machine,” or “PDQ terminal.”

Virtual Payment Terminal / Virtual Terminal
Web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. The merchant manually enters payment card data via the securely connected web browser. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes. **For security reasons, UCSB does not allow use of Virtual Terminal credit card processing except via an approved, secure payment terminal.**
Appendix B: Resources

Contacts

General Merchant Credit Card Support
805-893-3919
merchant.support@bfs.ucsb.edu

Matt Coy
Campus Credit Card Coordinator
805-893-3959 | matt.coy@ucsb.edu

Kimberly Ray
Associate Director of Controls
805-893-7667 | kimberly.ray@ucsb.edu

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

Procurement Services (Contract negotiations & signature)
www.bfs.ucsb.edu/procurement/news | purchasing@bfs.ucsb.edu

Policies

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

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

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

UC Privacy and Data Security Incident Response Plan
http://www.ucop.edu/information-technology-services/_files/uc_incidentresp_plan.pdf

SB 1386 and AB 1298 Guideline
Appendix C: Merchant Card Processing Basics

Suggested Reading: Visa’s Card Acceptance Guidelines for Visa Merchants

“The Card Acceptance Guidelines for Visa Merchants is a comprehensive manual for all businesses that accept Visa® transactions in the card-present and/or card-absent environment. The purpose of this guide is to provide merchants and their back-office sales staff with accurate, up-to-date information and best practices to help merchants process Visa transactions, understand Visa products and rules, and protect cardholder data while minimizing the risk of loss from fraud.” Download the guide: https://usa.visa.com/dam/VCOM/global/support-legal/documents/card-acceptance-guidelines-visa-merchants.pdf

Merchant Best Practices

The following are tips courtesy of Bank of America Merchant Services.

Obtain Authorization

- Swipe/Dip the card. If the card does not read, follow fallback/manual key entry procedures
- Follow all PCI DSS best practices for imprints and storage of any sensitive cardholder data
- There are common reasons you may have issues obtaining a successful swipe, such as: De-magnetized card; dirty swipe reader; not following through on the swipe
- Follow all terminal prompts. If you receive a decline, DO NOT process the transaction (ask for another form of payment)
- Card-not-present merchants: Obtain AVS & CVV2/CVC2 match

Review Card Security Features

- Compare account numbers, ensuring the account number on the card matches the account number printed on the sales draft (last four digits of the masked account number)
- Ensure that there is a hologram on the front (and possibly back) of the card

Compare Signatures
● If the card is not signed, request ID and have the cardholder sign the card in front of you. *Note: Merchants may ask to see ID as long as it is not a condition of the sale*
● The name on the front of the card must match the name on the back
● Unsigned cards or “See ID” provide a false sense of security and are not valid (this is actually printed on the back of the card!)
● If signatures do not match, check ID

**Complete the Transaction**

● Require the customer to sign the receipt (when applicable)
● Deposit the transaction in a timely manner (close the batch at the end of each day, if applicable)
● Retain the sales draft (13 months for Visa/MC, two years for AMEX, three years for Discover)

**Transaction Life Cycle**

**Card-present Merchants**

Payment card transactions for card-present merchants have many steps, from initiation to completion:

● Cardholder presents card for payment to the Merchant
● The Merchant processes the transaction request through their POS device that goes to the Acquirer (BAMS for UCSB)
● The Acquirer will transmit that request to the Payment Card Network (Visa/MC/Discover/AMEX)
● The Payment Card Network reaches out to the cardholder’s Issuing Bank (Issuer) and requests approval
● The Issuer will approve or decline the transaction, and send the information back to the Payment Card Network, which then passes it to the Acquirer, and finally back to the Merchant

**Card-not-present (e-commerce and MO/TO Merchants)**

Transactions take a similar route, with these changes:

● The cardholder enters the payment information into an internet-based payment page on, or connected to, the merchant’s website; or, an employee enters the cardholder’s payment information into an internet-based POS or payment page *(using an approved, secure terminal at UCSB)*
● The payment information is processed through a Payment Gateway, which passes it to the Acquirer. The rest of the routing is identical to card-present transactions, above.

Authorization Responses

An authorization is a request for verification that the cardholder’s account is in good standing with funds available at the time of the request. For most merchants, the authorization is obtained during the sale transaction. It does not warrant that the person presenting the card is the rightful cardholder, nor is it a promise or guarantee the sale will not be subject to a chargeback. The following are some examples of responses received from the card issuers.

- **Approved** - Transaction is approved by issuer/company that governs the payment card
- **Referral** - Message indicating that the merchant must call their authorization center and follow instructions provided. *Note: When a referral response is received the merchant should not attempt additional authorizations on the same card. The merchant should call the authorization center to receive a voice approval code to complete the transaction. A voice authorization should only be requested when a referral response is received. If the merchant receives an unfavorable response, another form of payment should be requested.*
- **Declined** - Transaction was not approved by issuer/company that governs the payment card. The transaction should not be completed. Request another form of payment. *Note: If a sale is declined, do not pursue alternative measures with the same card to obtain approval. Instead, request another form of payment. Merchants accepting and processing transactions with multiple authorizations are subject to chargebacks, Payment Card Company fines and/or cancellation of their processing agreement*
- **Pick Up Card** - Card issuer wants to recover the card. Do not complete the transaction. Ask for another method of payment and if you feel comfortable recover the card from the cardholder. *Note: Follow your internal procedures for card recovery*

Chargebacks and Retrieval Requests

The following information is excerpted from Visa’s “Chargeback Management Guidelines for Visa Merchants” (https://usa.visa.com/dam/VCOM/download/merchants/chargeback-management-guidelines-for-visa-merchants.pdf)

What is a Chargeback?

A “chargeback” provides an issuer with a way to return a disputed transaction. When a cardholder disputes a transaction, the issuer may request a written explanation of the problem from the cardholder and can also request a copy of the related sales transaction receipt from the acquirer, if needed (“Retrieval Request”). Once the issuer receives this documentation, the
first step is to determine whether a chargeback situation exists. There are many reasons for chargebacks - those reasons that may be of assistance in an investigation include the following:

- Merchant failed to get an authorization
- Merchant failed to obtain card imprint (electronic or manual)
- Merchant accepted an expired card

When a chargeback right applies, the issuer sends the transaction back to the acquirer and charges back the dollar amount of the disputed sale. The acquirer then researches the transaction. If the chargeback is valid, the acquirer deducts the amount of the chargeback from the merchant account and informs the merchant.

Under certain circumstances, a merchant may re-present the chargeback to its acquirer. If the merchant cannot remedy the chargeback, it is the merchant’s loss. If there are no funds in the merchant’s account to cover the chargeback amount, the acquirer must cover the loss.

**Proper Disclosure is Critical in Preventing Chargebacks**

As a merchant, you are responsible for establishing your merchandise return and refund or cancellation policies. Clear disclosure of these policies can help you avoid misunderstandings and potential cardholder disputes. Visa will support your policies, provided they are clearly disclosed to cardholders. For face-to-face or eCommerce environment, the cardholder must receive the disclosure at the time of purchase. For guaranteed reservations made by telephone, the merchant may send the disclosure after by mail, email or text message.

**Disclosures for Card-Present Transactions**

For card-present transactions, Visa will accept that proper disclosure has occurred before a transaction is completed if the following (or similar) disclosure statements are legibly printed on the face of the transaction receipt near the cardholder signature area or in an area easily seen by the cardholder. If the disclosure is on the back of the transaction receipt or in a separate contract, it must be accompanied by a space for the cardholder’s signature or initials.

**Disclosures for Card-Not-Present Transactions**

- Phone Order - For proper disclosure, your refund and credit policies may be mailed, emailed, or texted to the cardholder. As a reminder, the merchant must prove the cardholder received or acknowledged the policy in order for the disclosure to be proper.
- Internet or Application - Your website must communicate its refund policy to the cardholder in either of the following locations:
  ○ In the sequence of pages before final checkout, with a “click to accept” or other acknowledgement button, checkbox, or location for an electronic signature, or
○ On the checkout screen, near the “submit” or click to accept button
○ The disclosure must not be solely on a link to a separate web page

Storage of Receipts (electronic or paper)
Storage of receipts varies by card brand, and merchants should be prepared to produce timely copies of them upon request by our acquirer. Current storage requirements are:

● Visa & MasterCard - 13 months
● American Express - Two years
● Discover - Three years