UCSB Credit Card Processing and PCI Compliance

Sandra Featherson
Associate Director of Controls
Campus Credit Card Coordinator
May 2011
Agenda

• Campus Credit Card Process Overview
  • Terminology
  • Approval/Acceptance Process
  • Policy and Procedures
• PCI Compliance
• Department Responsibilities
• Questions
Credit Card Terminology

- **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.
  
  *UCSB:* Bank of America Merchant Services

- **Processor:** Handles the posting of transactions for authorization, clearing and settlement
  
  *UCSB:* First Data Merchant Services (FDMS)

- **Gateway:** Allows merchants to electronically submit payment transactions
  
  *UCSB:* Authorize.net or Cybersource

- **PCI DSS:** Payment Card Industry Data Security Standard
Credit Card Approval Process

• Meeting with Campus Credit Card Coordinator
  • Discuss needs, policies, fees, security, internal controls, vendors and the reconciliation process
  • Potential issues include UBIT, or activities not approved by the Rate and Recharge Committee

• Letter to Chancellor
  • Routed through Accounting – Campus Credit Card Coordinator
Credit Card Acceptance Process

- Review of Potential Vendors
  - Evaluate PCI and/or PA DSS Compliance
- Establish Appropriate Merchant/Gateway Accounts and User Access
- Establishment of Clearing account and possible Revenue accounts with General Accounting
Campus Policy and Procedures

- UC Business and Finance Bulletin, BUS-49, Policy for Cash and Cash Equivalents Received (http://www.ucop.edu/ucophome/policies/bfb/bus49.html)
  - Outlines UC Policy for Acceptance of Cash, Cash Equivalents, and Credit/Debit Cards
  - Department needs to ensure secure storage and protection of sensitive data, and/or personal data (SB 1386)
Credit Card Models

• Storing the Credit Card information – build/buy a solution that collects credit card information, and sends to processor for payment
• Click to Pay – Build/buy a solution, collect demographic information, and then transfer to a Gateway for collection of payment information and processing
• 3rd Party Vendor
Merchant Accounts

- Merchant Accounts are requested by Campus Credit Card Coordinator
- Separate merchant accounts are required for web/ecommerce and retail/card present transactions
- University policy requires use of our own merchant accounts
Gateway Providers

- UC approved Gateways are: Authorize.net and Cybersource
- Accounts are setup by Accounting
- Department needs technical support to integrate the Gateway with their web page
Credit Card Fees

• Fees to Accept Credit Cards
  • *Processor Fee*: Charged and collected by FDMS
  • *Access & Assessments*: Collected by FDMS and forwarded to VISA & Mastercard
  • *Interchange*: Collected by FDMS and forwarded to the bank that issued the credit card

• Gateway Fees
  • Usually charged by month and per transaction
Gateway Example

- Authorize.net

http://www.authorize.net/resources/howitworksdiagram/
3rd Party Vendors

- Vendors that provide a service, such as selling tickets or advertising, and will be accepting credit cards on behalf of the University (UC Regents)
Using 3\textsuperscript{rd} Party Vendors

- Must be PCI Compliant and/or PA DSS Compliant depending on situation
- Must allow use of the University merchant account
- Must be certified to the FDMS “North” platform
- All contracts for 3\textsuperscript{rd} Party Vendors must be reviewed at the campus level, and then approved by UC Office of the President
Vendor Contracts

- May require additional review by Audit and Advisory Services, the campus Policy Coordinator, and campus counsel
- The UC Data Security and IT Security language will need to be incorporated
- Other issues include late fees and automatic renewal options
UC Agreements and Policies

- UC has negotiated contracts with Authorize.net, Cybersource and others
- BUS 49 mandates use of those contracts
- Use of 3rd party vendors requires a full review of the contract
- Exception process requires letter from Campus Credit Card Coordinator and Controller; has to be approved by UCOP
Use of Vendor Logo

• Can I post a credit card logo on a University Web page? Yes.
• Where? On the Web page that lists payment options, as near to the purchase transaction as possible.
Use of Vendor Logo

- Do NOT post a vendor’s or credit card’s name or logo on your department’s main Web page.
- For more information on acknowledging, advertising, or sponsors see http://www.policy.ucsb.edu/policies/policy-docs/advertising-guide.pdf
Use of Vendor Logo

• If you post a credit card logo, you must have permission (a written agreement) with the credit card company to post their copyrighted mark.

• If you post a credit card logo that links to the credit company, you must have a “Terms of Use” link on either your department’s main Web page or on the page on which the logo/link appears.
Use of Vendor Logo

• For “Terms of Use” see:
  http://www.policy.ucsb.edu/terms_of_use/
Use of University Name

• The University’s name or “brand” is teaching, research, and public service.

• The University’s name is not for endorsing, advertising, or promoting commercial companies, products, or services.

• If a credit card company or vendor wants to use the University’s name, they must obtain written approval from the University’s delegated authority. Contact policy@ucsb.edu.
Reconciliation Process

- All campus credit card revenue is deposited into one central Bank of America account, which then goes to a balance sheet account for campus.

- Based on the Bank of America statement, Accounting clears our account by distributing the income and fees to departments using a financial journal.

- Accounting e-mails to the department the Bank of America merchant statement and the journal on the first business day of the month.
Reconciliation Process

- On the financial journal, Accounting debits the department/merchant’s clearing account for the deposits (revenue) and credits the department/merchant’s clearing account for the fees.
Reconciliation Process

- The department debits their clearing account, and credits the appropriate department account for the income.
- The department credits their clearing account, and debits the appropriate department account for the fees.
Reconciliation Process

- The department should reconcile the transactions between the Bank of America statement, the First Data Merchant Services statement and any internal records, such as 3rd party vendor reports, or reports from Authorize.net, etc.

- Approval of balance sheet reconciliation must be done in the online GL, due to SAS 112 requirements.
Credit Card Processing - Retail

Card Present Examples

Industry: *Department store*
UCSB: *Bookstore*

Merchant has a Point of Sale (POS) system, and some type of terminal device to swipe cards
Credit Card Processing - Ecommerce

Card Not Present Examples

Industry: Amazon.com
UCSB: Conference Registrations

Merchant has a website and sells goods or services.
Often utilizes the “Click to Pay” model.
Becoming an Ecommerce Merchant
(not using a 3rd party vendor)

1. Approval from the Chancellor
2. Complete PCI Questionnaire
3. Establish a new merchant account with BAMS
4. Choose Gateway and establish account
5. Establish clearing/balance sheet account within Accounting
PCI Data Security Standards

- What is it?
- SAQs
- Security Scanning
- Penetration Testing
- Trustkeeper
- Virtual Terminals
Payment Card Industry Data Security Standards

• Developed by the major Card brands to reduce the amount of fraud
• PCI now overseen by the Payment Card Industry Security Standards Council (https://www.pcisecuritystandards.org/)
• Holds the merchants accountable by requiring specific levels of security
Payment Card Industry Compliance

- New PCI Data Security Standards, v 2.0, eff. October 1, 2010
- All merchants required to complete a “Self Assessment Questionnaire (SAQ)”.
- Five SAQ categories, A, B, C, C-VT or D
- UC Office of the President requires all campuses to be compliant
PCI Core Standards

• Build and Maintain a Secure Network
  • Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  • Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
PCI Core Standards

- **Protect Cardholder Data**
  - *Requirement 3*: Protect stored cardholder data
  - *Requirement 4*: Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program**
  - *Requirement 5*: Use and regularly update anti-virus software or programs
  - *Requirement 6*: Develop and maintain secure systems and applications
PCI Core Standards

- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
PCI Core Standards

• Regularly Monitor and Test Networks
  • Requirement 10: Track and monitor all access to network resources and cardholder data
  • Requirement 11: Regularly test security systems and processes

• Maintain an Information Security Policy
  • Requirement 12: Maintain a policy that addresses information security for all personnel
## Self Assessment Questionnaires

<table>
<thead>
<tr>
<th>SAQ</th>
<th>Description</th>
</tr>
</thead>
</table>
| A     | Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced  
This would not apply to 100% face to face merchants |
| B     | Imprint-only merchants with no electronic cardholder data storage; Stand-alone terminal merchants, no electronic cardholder data storage      |
| C-VT  | Merchants using only web-based virtual terminals, no electronic cardholder data storage                                                     |
| C     | Merchants with POS systems connected to the Internet, no electronic cardholder data storage                                                   |
| D     | All other merchants (not included in SAQ A-C) and all service providers defined by a payment brand as eligible to complete an SAQ            |
Security Scanning

- PCI Security Scans are scans conducted over the Internet by an ASV
  - Scans help identify vulnerabilities and misconfigurations
  - Scan results provide valuable information
- PCI Security Scans may apply to all merchants with Internet-facing IP addresses
  - Even if an entity does not offer Internet-based transactions, other services may make systems Internet accessible
- The PCI DSS requires all Internet-facing IP addresses to be scanned for vulnerabilities
- In some instances, companies may have a large number of IP addresses available
  - In these cases, scan vendors can help merchants define the appropriate scope of the scan required
- In general, the following segmentation methods can be used to reduce the scope of the Security Scan
  - Providing physical segmentation between the segment handling cardholder data and other segments
  - Employing appropriate logical segmentation
  - Merchants have the ultimate responsibility for defining the scope of their PCI Security Scan, though they may seek expertise from ASVs
Penetration Testing

- Required for all SAQ “D” merchants
- Can be done in-house or by an Approved Scanning Vendor (ASV)
Trustkeeper

- Trustkeeper provides a way to monitor and track PCI Compliance.
- All UCSB Merchants will be re-registered in the program, Trustkeeper.
- Annual fee is recharged to departments.
Data Security

- Do not accept credit card information via fax or email.
- All authorization forms that include customer account information should be stored securely.
- Restrict access to cardholder data.
- Develop/maintain security policies.
Services and Equipment

- Conference Registrations
  - Regonline
    - PCI Compliant, Uses UCSB Merchant Account
- Reporting
  - Access to Clientline Reports
- Variety of Terminals
Suspected Breach of Credit Card Data

- Notify Campus Credit Card Coordinator, Sandra Featherson, x7667
- Notify Campus Chief Information Security Officer, Karl Heins, x8843
Consequences of Breach of Credit Card Data

- Fines levied by Card Brands and/or acquiring Bank
- As example, fines could be up to $500K just from Visa if found not compliant at time of breach.
Next Steps

- Campus PCI Work Group
- SAQ Review for Merchants
- Trustkeeper Annual Update
- Site Visits to Merchants
- Credit Card Web Page
Department Responsibilities

• Understand the Credit Card process
• Understand and implement BUS 49 procedures and guidelines
• Maintain PCI Compliance
• Monthly reconciliation of accounts
Questions?