

Partners in PCI DSS Compliance

Joan K Piscitello, Iowa State University
Marsha Lovell, UCLA
Mark Welch, University of Notre Dame
Todd Abbott, Bank of America



Highlighted Topics

- ◆ Campus Partnerships
- ◆ Third Party Partnerships
 - ASP Solutions
 - Contract Language
 - Qualified Assessor
 - Scan Vendor
- ◆ Partnership between Merchant Bank and Merchant (University)
- ◆ Responsibilities of Partners

Reference Materials

- ◆ UCLA Terminal Merchant Agreement
- ◆ UCLA Points of Contact
- ◆ Sample Contract Language
 - For reference only. Contact your legal counsel.
- ◆ Cardholder Information Security Program (CISP)
http://usa.visa.com/business/accepting_visops_risk_management/cisp.html?it=wb/|Learn%20More

Terminal Merchant Agreement

Terminal Merchant Agreement	1
I. Introduction	1
II. General Responsibilities	1
III. Account Setup, Testing, & Maintenance.....	2
IV. Security	2
VI. Support	3
VII. Reporting	3
VIII. Cost and Billing	3
IX. Signature Page.....	4

I. Introduction

A credit card terminal is a device (wired or wireless) used to process credit card point-of-sale transactions.

Terminal processing allows for flexibility to collect payments when using the Departmental Deposit credit card process is not feasible or practical. Payments may be processed with the cardholder present, or on a mail/telephone order (MOTO) basis, per the needs of the merchant. The Terminal process:

- ❖ Verifies credit cards.
- ❖ Authorizes credit card payments.
- ❖ Deposits credit card funds to the University's depository bank.

1. Purpose of this document

This agreement provides the basis for a partnership between Student Financial Services (SFS) and the _____ (merchant). It details the services provided by SFS and outlines the basic responsibilities of each party involved. Throughout this document the term *Merchant* refers to the department named above.

2. Dispute resolution

The primary point of contact is the Terminal Support Team (terminal@finance.ucla.edu). If a satisfactory resolution has not, or cannot be reached, the problem will be brought to the attention of the Manager of Customer Service & Support within SFS. Further problem resolution will be addressed by the Director of SFS. For current contacts, please refer to the list of contacts provided by the Terminal Support Team.

SFS plays a primary role in interpreting the policies and procedures outlined in this document and other University communications pertaining to terminal processing. They are also the only area with employees authorized to contact our credit card processor. Chase Payment Services (CPS), UCLA's preferred merchant services provider, provides equipment and other operational assistance to our merchants.

II. General Responsibilities

SFS agrees to:

- ❖ Set up and maintain merchant account(s) with the credit card processor.
- ❖ Notify merchants on a regular and timely basis about service availability, product features and upgrades and changes to University and credit card association policies.
- ❖ Provide customer support via telephone and e-mail during normal business hours (Monday thru Friday, 9 AM - 5 PM).

CPS will:

- ❖ Lease and/or sell terminal equipment to the merchant. General Accounting will charge the ledger account you specify for this charge directly
- ❖ Test merchant accounts and equipment to verify data integrity and payment card industry (PCI) compliance.
- ❖ Provide 24/7 support for processing problems relating directly to the actual credit card transaction.

Merchant agrees to:

- Keep equipment in reasonable working order.
- Contact SFS directly with any terminal equipment or merchant set up needs.
- Attend annual campus credit card training meetings and implement any changes expected by the card processor. Information about these will be provided by SFS.
- Meet connectivity and security requirements as provided herein.
- Follow University policies and procedures for ensuring data security and comply with guidelines for credit card acceptance.
- Complete an annual Terminal PCI Compliance questionnaire before June of each year certifying their compliance with credit card industry regulations.
- Settle transactions daily and make corresponding entries to the General Ledger using DDF or other approved depository mechanism.

III. Account Setup, Testing, & Maintenance

1. Account Setup
 - a. Upon receipt of signed, completed Merchant Request Form, SFS will initiate the creation of a merchant account with a credit card processor contracted by the Office of the President (UCOP).
 - b. Before the account can be enabled, the merchant must complete the Terminal PCI Compliance questionnaire and read the UCLA Retail Operating Guide. The PCI questionnaire must be completed satisfactorily before the account is activated.
 - c. Upon creation of the merchant account, SFS will communicate the merchant setup to CPS, General Accounting, and the department.
2. Testing
 - a. Merchant will be notified by SFS when the account setup is completed. Accounts will take a minimum of 2 weeks to set up unless a rush order is placed. There is a \$75 charge for rush set ups.
 - b. Your equipment will arrive pre-programmed to process credit card transactions.
3. Merchant Training
 - a. SFS will provide basic documentation outlining the transaction authorization and settlement process.
4. Account Maintenance
 - a. SFS will act as a liaison to the bank and processor.
 - b. Refunds/credits to an account will be processed by the merchant directly.
 - c. Requests to activate/deactivate/suspend a merchant account must be received in writing from an authorized user(s) via Terminal@finance.ucla.edu.

IV. Security

Security is a top priority for credit card transactions. The terminal has been designed around the latest secure protocols for transferring, storing and managing sensitive data.

Terminals should be located in a secured environment with limited physical access.

Your new credit card terminal is equipped with a variety of features that protect cardholder data and comply with state and federal law. Some of these features include:

- ❖ Dedicated authorization and settlement phone numbers only allows your terminal to communicate with the credit card processor.
- ❖ PIN data for debit transactions are encrypted on the PIN pad as the cardholder enters his/her PIN, preventing any theft of this number.
- ❖ Full 16-digit credit card numbers are truncated, with only the last 4-digits printed on receipts.

1. Merchant-level Security

It is the merchant's responsibility to maintain a secure environment for credit card processing.

- a. Merchant agrees to take sufficient measures to ensure security of a cardholder's information. These include, but are not limited to:

- i. State and federal data privacy and security laws, including:
 - 1. SB1386 (CA Civil Code 1798.29 & 1798.82-1798.84),
 - 2. Gramm-Leach-Bliley Act of 1999, and
 - 3. California Financial Information Privacy Act
 - b. Restrict access to authorized administrative users.
 - c. Merchant must *never*:
 - i. Transmit credit card information via unencrypted e-mail.
 - ii. Store card information in an unsecured database or other digital medium.
- 2. SFS reserves the right to suspend or terminate service at any time if sufficient security measures are not employed by the merchant.

VI. Support

- 1. Technical
 - a. CPS provides limited support to Merchants. Support for Terminal is limited to:
 - i. Service availability.
 - ii. Interpretation of authorization messages and error codes.
 - b. Merchant is responsible for:
 - i. Establishing and maintaining connection to processor.
 - c. SFS does not provide any technical assistance to the Merchant. If it is determined that there may be a connectivity problem or other equipment-related problem, SFS will request a replacement terminal from CPS.
- 2. Administrative
 - a. SFS interfaces with General Accounting and the processor, and will:
 - i. Deposit funds daily at the bank. Batches settled on weekends or University holidays will be posted to the ledger the next business day.
 - ii. Reconcile bank deposit to the ledger.
 - iii. Notify the Merchant about any reconciliation or deposit problems.
 - b. Merchant interfaces with the credit card processor and SFS, and will:
 - i. Settle credit card transactions **daily** to guarantee the best processing rate.
 - ii. Promptly deposit these funds to FS using DDF or other approved depository mechanism.
 - c. The SFS Support Team is the Merchant's first line of contact for support. Support Team members can answer questions about:
 - i. Deposits to the ledger.
 - ii. Merchant setup and maintenance.
 - iii. Billing questions.
 - iv. General processing questions.
 - d. General Accounting can assist the Merchant to interpret ledger entries and NCR code maintenance.

VII. Reporting

A variety of reporting options are currently available to the Merchant. AIS will provide:

- If DDF is used, merchant will receive:
 - PAN notices containing deposit information.
 - QDB data warehouse - transactional detail and summary information from FS.
 - Web reports - available via OFSR (Online Financial System Reporting) website.
- CPS also provides online access to your credit card transactions. This access may require an additional fee.

VIII. Cost and Billing

- 1. Bank Fees
 - a. All bank fees (access, interchange, processor, etc.) are negotiated by UCOP and are subject to change without notice.
 - b. Bank fees will be recharged directly to the Merchant by SFS.
 - c. Please see current rate sheet for the most current rates charged by the processor.

2. Recharge Fees

- a. Merchants who choose to authorize credit cards via DDF will be recharged per transaction. Please see the current rate sheet to determine how fees are calculated.

IX. Signature Page

The parties listed below agree to the terms and conditions listed in the Terminal Merchant Agreement. Any updates to the original agreement shall be considered part of the original agreement entered into unless written notification within 30 days is provided by party, thereby nullifying said agreement.

Department Name: _____

Dept. Code: _____

Merchant Name: _____

Marsha Lovell
Director, Student Financial Services

Date

User/Merchant Representative

Date

Terminal Credit Card Information

Points of Contact: Terminal@finance.ucla.edu, x56347 Shirley Rayner, x53739 Chenda Seng

Merchant ID (MID) Setup Requirements: Terminal Merchant Agreement, UCLA Operating Guide, PCI Questionnaire

Hardware Requirements: Order and return through SFS for tracking and correct processing

Annual Expectations: Credit Card User Meetings – PCI update in Spring, Overview and Training in Fall

Costs: Pass through costs for bank charges and interchange charges
PCI Compliance must be certified by each merchant before May 31.

CyberPay Credit Card Information

Points of Contact:

CyberPay@finance.ucla.edu, x63377

Gabi Jones, x52094 Johnny Pugh

Merchant ID (MID) Setup

Requirements: CyberPay Merchant Agreement, UCLA Operating Guide

Annual Expectations: Credit Card User Meetings – PCI update in Spring,

Overview and Training in Fall

Costs: Pass through costs for bank charges and interchange charges; \$.24 per transaction for CyberPay User fee

PCI Compliance will be certified by

UCLA and not expected of each merchant.

DDF Credit Card Information

Points of Contact:

CyberPay@finance.ucla.edu, x52181 Anita

Chua, x52251 Magaly Pitterson

Merchant ID (MID) Setup Requirements:

CyberPay Merchant Agreement, UCLA Operating Guide, Departmental Financial

Deposit Process Course

Annual Expectations: Credit Card User Meetings – PCI update in Spring, Overview

and Training in Fall

Costs: Pass through costs for bank charges and interchange charges; \$.24 per

transaction for CyberPay User fee

PCI Compliance will be certified by UCLA and not expected of each merchant.

Non-CyberPay Internet Merchant Credit Card Information

Point of Contact: mlovell@finance.ucla.edu, x 66034 Marsha Lovell

In order to process with a Third Party (Not CyberPay) a variance must be received from Student Financial Services (SFS) and UCOP Banking Services Group. This must be coordinated by the Director of SFS, see contact above.

Annual Requirement: Updated certificate of PCI compliance from Third Party Process filed with SFS and UCOP.

Annual Recommendations: Credit Card User Meetings – PCI update in Spring, Overview and Training in Fall

Costs: Determined by Processor

FOR REFERENCE ONLY. CONTACT YOUR LEGAL COUNSEL.

Formatted: Left, Indent: Left: 0", First line: 0"

TEMPLATE LANGUAGE RE: CONFIDENTIALITY AND SECURITY

1.0 CONFIDENTIALITY AND SECURITY:

- 1.1 The term "Confidential Information" shall mean this Agreement and all proprietary information, data, trade secrets, business information, any personally identifiable information regarding students, employees or other individuals or entities, including but not limited to, Social Security numbers, other tax identification numbers, credit card, bank account and other financial information, and other information of any kind whatsoever which: (a) a Party ("Discloser") discloses, in writing, orally or visually, to the other Party ("Recipient") or to which Recipient obtains access in connection with the negotiation and performance of this Agreement, and which (b) relates to: (i) the Discloser, or (ii) in the case of Service Provider as Recipient, University, its students and employees, and its third-party vendors or licensors who have made confidential or proprietary information available to University. University Confidential Information shall include Personally Identifiable Information, as described below. Service Provider acknowledges that University has a responsibility to its students and employees to keep information about its students and employees and their records and accounts ("Personally Identifiable Information") strictly confidential. Service Provider represents and warrants that it will keep such Personally Identifiable Information strictly confidential both during the Term and after the termination of the Agreement.
- 1.2. Service Provider shall not disclose or use University Confidential Information other than to carry out the purposes for which University or one of its Affiliates disclosed such University Confidential Information to Service Provider. Service Provider shall not disclose any University Confidential Information other than on a "need to know" basis and then only to: (a) its employees or officers, provided, however that each such employee or officer have entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof; (b) Affiliates of Service Provider, only if approved by University and provided that such Affiliates shall be restricted in use and redisclosure of University Confidential Information to the same extent as Service Provider, and provided further that the Affiliate's employees or officers have each entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof; (c) to Subcontractors, only if approved by University and provided further that such Subcontractors and each of their employees and officers have entered into a confidentiality agreement, that is enforceable under the laws of each applicable jurisdiction, with terms no less restrictive than the terms hereof; (d) to independent contractors, agents, and consultants hired or engaged by University, provided, however, that University has instructed Service Provider to provide such information or if Service Provider has confirmed that all such persons are subject to a confidentiality agreement, enforceable under the laws of the United States, California and each applicable non-U.S. jurisdiction, which shall be no less restrictive than the provisions of this Section; or (e) as required by applicable law and regulation, order of any court or government

agency or rule of a self-regulatory agency (collectively, "Legal Process"), or as otherwise permitted by this Agreement, either during the Term of this Agreement or after the termination of this Agreement. The restrictions set forth herein shall apply during the Term and after the termination of this Agreement.

- 1.3 Prior to any disclosure of Confidential Information as required by Legal Process, the Recipient shall: (i) notify the Discloser of any, actual or threatened legal compulsion of disclosure, and any actual legal obligation of disclosure immediately upon becoming so obligated, and (ii) reasonably cooperate with the Discloser's reasonable, lawful efforts to resist, limit or delay disclosure.
- 1.4. All Work Product, works-in-progress, notes, data, reference materials, memoranda, documentation and records in any way incorporating or reflecting any of University Confidential Information and all proprietary rights therein, including copyrights, will belong exclusively to University. Upon the termination or expiration of this Agreement, or at any time upon the request of University, Service Provider shall return all University Confidential Information (and all copies and derivative works thereof made by or for Service Provider), including Personally Identifiable Information, in the possession of Service Provider or in the possession of any third party over which Service Provider has or may exercise control and further shall delete or erase such Confidential Information, copies and derivative works thereof, from computer systems in the possession or control of Service Provider or any third party acquiring University's Confidential Information from Service Provider. University shall have the right to require Service Provider to verify, to University's satisfaction, that all University Confidential Information has been returned. Service Provider agrees to fully cooperate with University's requests for verification. Verification may include University conducting an on-site audit of Service Provider's systems and facilities and/or Service Provider executing a sworn affidavit stating that it does not have in its possession or under its control any other documents, contracts, computer code, computer data or other materials, in tangible or electronic form, that pertain to University Confidential Information.
- 1.5. **Exceptions to Obligations of Confidentiality.** With the exception of the obligations related to Personally Identifiable Information, the obligations of confidentiality in this Section shall not apply to any information that (a) Recipient rightfully has in its possession when disclosed to it, free of obligation to Discloser to maintain its confidentiality; (b) Recipient independently develops without access to Discloser's Confidential Information; (c) is or becomes known to the public other than by breach of this Section; (d) Discloser or its agent releases without restriction; or (e) Recipient rightfully receives from a third party without the obligation of confidentiality. Any combination of Confidential Information disclosed with information not so classified shall not be deemed to be within one of the foregoing exclusions merely because individual portions of such combination are free of any confidentiality obligation or are separately known in the public domain.
- 1.6. Service Provider agrees that under no circumstances shall any of Service Provider's employees, officers, Affiliates or Subcontractors, whether full-time or part-time,

connect to any University system or handle any University data, for purposes of downloading, extracting, storing or transmitting information through personally owned, rented or borrowed equipment including, but not limited to, laptops, Blackberries/palm pilots and cell phones. Any exceptions are at variance with University policy and must be approved in advance according to University policy guidelines.

- 1.7. **No License Conferred.** All Confidential Information shall remain the property of the Discloser or its licensors. Except to the extent expressly provided herein, this Agreement shall not be construed as conferring on a Recipient an express or implied license or an option for a license for any patent, copyright, trademark, license right or trade secret owned or obtained by the Discloser.
- 1.8. **Media Releases.** All media releases, public announcements and public disclosures by either Party, or their Representatives, employees or agents, relating to this Agreement or the name or logo of University, any University Affiliate, any other business entity under common control with University, or Service Provider, including, without limitation, promotional or marketing material, but not including any disclosure required by legal, accounting or regulatory requirements beyond the reasonable control of the releasing Party, shall be coordinated with and approved by the other Party in writing prior to the release thereof.
- 1.9. **Information Security Plan.** Service Provider acknowledges that University is required to comply with information security standards for the protection of Personally Identifiable Information and other Confidential Information required by law, regulation and regulatory guidance, as well as University's internal security program for information and systems protection.

Within thirty (30) days of the Effective Date of the Agreement and subject to the review and approval of University, Service Provider shall establish, maintain and comply with an information security plan ("Information Security Plan"), which shall contain such elements that University may require after consultation with Service Provider.

On at least an annual basis, Service Provider shall review, update and revise its Information Security Plan, subject to University's review and approval. At University's request, Service Provider shall make modifications to its Information Security Plan or to the procedures and practices thereunder to conform to University's security requirements as they exist from time to time.

Service Provider's Information Security Plan shall be designed to:

- Ensure the security, integrity and confidentiality of Confidential Information;
- Protect against any anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the person that is the subject of such information; and

- Comply with all applicable legal and regulatory requirements for data protection.

The parties expressly agree that Service Provider's security procedures shall require that any Personally Identifiable Information transmitted or stored by Service Provider only be transmitted or stored in an encrypted form approved by University.

- 1.10 **Notice of Security Breach.** Service Provider shall notify University's Relationship Manager and its designated principal security officer of any known or suspected security breach of its system or facilities containing University Confidential Information or any other breach of Confidential Information relating to this Agreement immediately, but not later than within twenty-four (24) hours after discovery, if the information was, or is reasonably believed to have been, acquired by an unauthorized person. Service Provider agrees to fully cooperate with University with the preparation and transmittal of any notice, which University may deem appropriate or required by law, to be sent to customers or other affected third parties regarding the known or suspected security breach, and to further take appropriate remedial action with respect to the integrity of its security systems and processes. Service Provider's Information Security Plan shall include a written response program addressing the appropriate remedial measures it shall undertake in the event that there is an information security breach.
- 1.11 Service Provider shall cause all Subcontractors and other persons and entities whose services are part of the Services which Service Provider delivers to University or who hold University Confidential Information and Personally Identifiable Information, to implement an information security program and plan substantially equivalent to Service Provider's.

In addition, Service Provider represents and warrants that in performing the Services, it will comply with all applicable privacy and data protection laws and regulations of the United States including, as applicable, the provisions in the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq., the Family Education Rights and Privacy Act ("FERPA"), 20 USC Section 1232(g) et seq., and of any other applicable non-U.S. jurisdiction, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission and other applicable guidance, to protect University's Personally Identifiable Information from identity theft, fraud and unauthorized use.

- 1.12 Service Provider represents and warrants that it shall implement and maintain certification of Payment Card Industry ("PCI") compliance standards regarding data security and that it shall undergo independent third party quarterly system scans that audit for all known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (*i.e.*, viruses and worms) to gain access to or disrupt the network devices. In connection with credit card transactions processed for University, Service Provider will provide reasonable care and efforts to detect fraudulent credit card activity. In performing the Services, Service Provider

shall comply with all applicable rules and requirements, including security rules and requirements, of University's financial institutions, including its acquiring bank, the major credit card associations and credit card companies. If during the term of the Agreement, Service Provider undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI standards and/or other material payment card industry standards, it will promptly notify the University of such circumstances.

- 1.13 Failure by Service Provider to comply with any provision of this Section shall constitute a material breach of the Agreement.

2.0 SUPPLIER PERSONNEL:

- 2.1 Service Provider's personnel are not eligible to participate in any of the employee benefit or similar programs of University. Service Provider shall inform all of its personnel providing Services pursuant to this Agreement that they will not be considered employees of University for any purpose, and that University shall not be liable to any of them as an employer for any claims or causes of action arising out of or relating to their assignment.
- 2.2 Upon the written request of University for cause pursuant to this Agreement, Service Provider agrees to promptly review the conduct of and remove, as necessary, any of Service Provider's Representatives or Subcontractors performing Services under this Agreement and replace such Representative or Subcontractor as soon as practicable.
- 2.3 As a general matter, Service Provider shall not engage its Affiliates or Subcontractors for the performance of the Services. The engagement of an Affiliate or Subcontractor by Service Provider shall be subject to University's prior written consent and sole discretion, and shall not relieve Service Provider of any of its obligations under this Agreement. Service Provider shall require all Affiliates and Subcontractors, as a condition to their engagement, to agree to be bound by provisions substantially the same as those included in this Agreement, and in particular, the Sections regarding Service Provider personnel, insurance, and confidentiality and security. Upon University's request, Service Provider shall provide documentation evidencing its Affiliates' and Subcontractors' compliance with these provisions. Service Provider shall further provide University with a listing, which it shall update from time to time, identifying each location or facility of it, its Affiliates, and its Subcontractors, at which Services are performed or University Confidential Information is stored. Any work to be performed in connection with this Agreement by Service Provider, its Affiliates or Subcontractors must be performed in the United States, unless the prior written consent of the University is received to perform work outside the United States. Further, University Confidential Information may not be transmitted or stored outside the United States without the prior written consent of University.
- 2.4 Service Provider shall comply and shall cause its Representatives, Affiliates and Subcontractors to comply with all personnel, facility, safety and security rules and regulations and other instructions of University, when performing work at a University

facility, and shall conduct its work at University facilities in such a manner as to avoid endangering the safety, or interfering with the convenience of, University Representatives or customers. Service Provider agrees that it, its Representatives and Subcontractors providing Services hereunder, shall possess any licenses, approvals or certifications required by any applicable law or regulatory agency or self-regulatory organization.

- 2.5 Service Provider shall not knowingly permit a Representative or Subcontractor to have access to the records, data or premises of University when such Representative or Subcontractor: (a) has been (i) convicted of a crime or has engaged in (ii) a dishonest act or a breach of trust; or (b) uses illegal drugs.
- 2.6 Service Provider represents that it maintains comprehensive hiring policies and procedures which include, among other things, a background check for criminal convictions, and pre-employment drug testing, all to the extent permitted by law. Service Provider shall conduct thorough background checks and obtain references for all its Representatives and Subcontractors performing the Services. Service Provider further represents that through its hiring policies and procedures, it uses commercially practicable efforts to hire candidates with appropriate character, disposition, and honesty. Service Provider shall require all Subcontractors, as a condition to their engagement, to be bound by the provisions of this Section. To satisfy Service Provider's obligations under this Section, University may require Service Provider to utilize the services of a third party service provider designated by University to obtain the required background investigations.
- 2.7 University shall notify Service Provider of any act of dishonesty committed against University which may involve a Service Provider Representative or Subcontractor, and Service Provider shall promptly notify University if it becomes aware of any such offense. Following such notice, at the request of University and to the extent permitted by law, Service Provider shall cooperate with investigations conducted by or on behalf of University. Service Provider agrees to pursue all available legal action against any employee who has committed a crime, fraud or tort during the course of performing Services for University.
- 2.8 Service Provider shall provide University with an escalation list of names and contact information for middle and senior management responsible in each jurisdiction for the oversight and monitoring of the employees performing the Services. Service Provider further represents and warrants that it will commit sufficient management resources and staff to meet the performance requirements for the Services set forth in this Agreement.

3.0 FINANCIAL RESPONSIBILITY AND AUDIT:

- 3.1 **Retention of Records.** Service Provider shall maintain at no additional cost to University, in a reasonably accessible location identified to University, all records pertaining to the Services provided to University under this Agreement for a period of two (2) years or longer after termination of the Agreement, if required by applicable

law or regulation. Service Provider further agrees to provide to University, at its request, a full copy of all such records for University to maintain at a U.S. location which University shall designate.

- 3.2 **Annual Financial and Operational Audits.** Within thirty (30) days of the Effective Date of the Agreement, Service Provider shall provide University with copies of its latest financial audit and its operational audits for the facilities being used to provide Services under this Agreement. Thereafter, Service Provider shall conduct such audits at least annually, at its sole cost and expense. Service Provider shall provide University with a copy of each report prepared in connection with each such audit within thirty (30) calendar days after it prepares or receives such report. The audits must be performed as full SAS 70 audits and if specified by University, Service Provider must be able to meet other key international security and audit certifications (e.g., ISO 17799 or BS 7799). Notwithstanding the foregoing, Service Provider shall notify University immediately in the event there is a change of control or material adverse change in its business or financial condition that may affect Service Provider's ability to perform the Services.
- 3.3 During regular business hours, University may, at its sole expense and on a mutually agreed upon date (which shall be no more than fourteen (14) days after written notice), time, location and duration perform or arrange for a site visit and/or confidential audit of Service Provider's operations, facilities, financial records, and security and business continuity systems which pertain specifically to the Services. If Service Provider is not in substantial compliance with the requirements of the performance requirements set forth in this Agreement, University shall be entitled, at Service Provider's expense, to perform additional such audits. University will provide to Service Provider a copy of each report prepared in connection with any such audit within thirty (30) calendar days after it prepares or receives such report. Service Provider agrees to promptly take action at its expense to correct those matters or items that require correction as mutually agreed. If any audit discloses material variances from the performance requirements set forth in this Agreement or a material breach by Service Provider of the provisions of this Agreement, Service Provider shall be deemed in default of this Agreement.
- 3.4 Service Provider will give prior notice to University of requests by regulatory authorities to examine Service Provider's records regarding University. At University's written request, Service Provider shall reasonably cooperate with University in seeking a protective order with respect to such records. Service Provider agrees to submit to and cooperate with any requests for information or examination by regulatory entities with supervisory authority over University.
- 4.0 **NON-ASSIGNMENT:** Neither Party may assign this Agreement or any of the rights hereunder or delegate any of its obligations hereunder, without the prior written consent of the other Party, and any such attempted assignment shall be void.
- 5.0 **COMPLIANCE WITH LAWS:**

5.1 Service Provider shall comply with all applicable United States federal, state and local laws, regulations and ordinances, and rules of self-regulatory organizations, including National Automated Clearing House Association ("NACHA") rules, as well as all national, state and local laws, regulations and ordinances, and rules of self-regulatory organizations of any other non-U.S. jurisdiction to which Service Provider, University or the Services are subject. If a charge of non-compliance with such laws, regulations and rules is brought against Service Provider in connection with this Agreement or the Services, Service Provider shall promptly notify University of the charge in writing. Service Provider shall indemnify and hold University harmless from any damages or costs incurred as a result of any finding or ruling by a court or government body or self-regulatory organization that Service Provider's provision of the Services hereunder violates any laws or regulations promulgated under the United States or other jurisdiction.

6.0 DEFINITIONS [add to definitions section in Agreement]

- 6.1 Affiliate - an entity now or hereafter controlled by, controlling or under common control with a Party. Control exists when an entity owns or controls more than 50% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity.
- 6.2 Party - University or Service Provider.
- 6.3 Representative - an employee, officer, director, or agent of a Party.
- 6.4 Relationship Manager - the respective employees of each Party that each Party shall designate to act on its behalf with regard to matters arising under this Agreement; each Party shall notify the other in writing of the name of their Relationship Manager; however, the Relationship Manager shall have no authority to alter or amend any term, condition or provision of the Agreement; further, each Party may change its Relationship Manager by providing the other Party with prior written notice.
- 6.5 Subcontractor - a third party to whom Service Provider has delegated or subcontracted any portion of its obligations set forth herein.
- 6.6 Work Product - All discoveries, inventions, work of authorship or trade secrets, or other intellectual property and all embodiments thereof originated by Service Provider within the scope of Services provided under this Agreement, whether or not prepared on University's premises.

FOR REFERENCE ONLY. CONTACT YOUR LEGAL COUNSEL.

Template Language Re: Service Provider Contract

Provisions for Cardholder Data. The provisions set forth herein apply to a Service Provider that either itself, or through a processor or other agent, stores, processes, handles or transmits cardholder data in any manner. Cardholder Data is information provided to Service Provider to provide a function or service for University, and includes all credit card information, including the credit card number assigned by the card issuer that identifies the cardholder's account or other cardholder personal information.

- A. Service Provider shall at all times comply with the Visa/MasterCard/American Express/Discover card acceptance requirements, (Payment Card Industry or "PCI" standards) as may be periodically updated, and the requirements set forth herein for the handling of Cardholder Data. Service Provider shall provide University either 1) a certificate verifying Service Provider is PCI compliant on an annual basis no later than March 31 of each calendar year, and beginning March 31, 2007, from an accredited auditor of PCI compliance; the entity verifying compliance must be accredited by the Payment Card Industry; or 2) proof of a current, good-standing listing on the Visa Cardholder Information Security Program (CISP), http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp/List_of_CISP_Compliant_Service_Providers.pdf. Service Provider hereby agrees to access the Association Requirements at: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html; and periodically review this site for any updates to the Association Requirements.
- B. Service Provider acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by Visa/MasterCard/American Express/Discover and University, or as required by applicable law.
- C. 1) In the event of a breach or intrusion of or otherwise unauthorized access to Cardholder Data stored at or for Service Provider, Service Provider shall immediately notify University by letter and by email, {insert contact information here}, and provide University or its designee, Visa/MasterCard/American Express/Discover, and the acquiring financial institution and their respective designees access to Service Provider's facilities and all pertinent records to conduct a review of Service Provider's compliance with these requirements. Service Provider shall cooperate fully with any reviews of their facilities and records provided for in this paragraph. Service Provider agrees to keep confidential the fact that any breach of security involved University data, and will defer all public communication to University.
- 2) Service Provider shall immediately notify University of any unauthorized access to any credit card information stored or process by or for Service Provider, even where the data is not from or relating to University; Service Provider does not need

to disclose the identity of the client; but must disclose sufficient information for University to assess the breach and security of Service Provider's services.

- D. Service Provider shall maintain appropriate business continuity procedures and systems to ensure security of Cardholder Data in the event of a disruption, disaster or failure of Service Provider's primary data systems which involve a risk to University data. Service Provider shall provide access to its security systems and procedures, as reasonably requested by University or its designee.
- E. Any subcontractors, agents, successors and/or assigns of Service Provider shall be bound by the obligations set forth herein. The obligations set forth herein shall survive termination of the contract between Service Provider and University. Service Provider and its successors and assigns shall comply with terms after termination of this agreement, with respect to the handling and processing of University data.
- F. University may elect to terminate this Agreement (with no penalty or costs to University) for any breach of these sections A – E relating to security of cardholder data. University may elect to terminate this Agreement (with no penalty or costs to University) where University determines in its reasonable judgment that Service Provider has engaged in conduct or is purported to have engaged in conduct such that University's continuation of business with Service Provider may cause harm to University's reputation.

FOR REFERENCE ONLY. CONTACT YOUR LEGAL COUNSEL.

SAMPLE CONTRACT LANGUAGE. IN THIS CASE, THE SERVICE PROVIDER HAD A MERCHANT LEVEL CERTIFICATION, BUT WAS SEEKING CERTIFICATION AS A SERVICE PROVIDER.

1. SERVICE PROVIDER shall at all times comply with the applicable credit card acceptance requirements established by the Payment Card Industry (“PCI standards”) as may be periodically updated, and the requirements set forth therein for the handling of cardholder data. SERVICE PROVIDER shall provide CLIENT, upon request either 1) a certificate verifying SERVICE PROVIDER is compliant with PCI Standards an accredited auditor of PCI compliance or 2) proof of a current, good-standing with applicable PCI standards, SERVICE PROVIDER acknowledges and agrees that cardholder data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by card issuers and CLIENT, or as required by applicable law or association rules or regulations.
 - 1.1. In the event of a breach or intrusion of or otherwise unauthorized access to cardholder data related to CLIENT’s data stored at or for SERVICE PROVIDER, SERVICE PROVIDER shall promptly notify CLIENT by letter and by email and shall cooperate with CLIENT in the investigation and notifications of such incident. SERVICE PROVIDER agrees to keep confidential, except for disclosures required by law, the fact that any breach of security involved CLIENT data, and will defer, when at all possible, all public communication to CLIENT.
 - 1.2. SERVICE PROVIDER shall promptly notify CLIENT of any unauthorized access to any credit card information stored or processed by or for SERVICE PROVIDER, even where the data is not from or relating to CLIENT; SERVICE PROVIDER does not need to disclose the identity of the CLIENT; but must disclose sufficient information for CLIENT to assess the breach and security of SERVICE PROVIDER’s services.
2. SERVICE PROVIDER shall maintain appropriate business continuity procedures and systems to ensure security of cardholder data in the event of a disruption, disaster or failure of SERVICE PROVIDER’s primary data systems which involve a risk to CLIENT data. SERVICE PROVIDER

shall provide reasonable description of its security systems and procedures, as reasonably requested by CLIENT or its designee. Any subcontractors and agents who have access to CLIENT's cardholder data and are required by PCI to be so compliant, and any successors and/or assigns of SERVICE PROVIDER, shall be bound by the obligations set forth herein. The obligations set forth herein shall survive termination of this Agreement between SERVICE PROVIDER and CLIENT, but for only so long as SERVICE PROVIDER has possession of CLIENT's cardholder data. SERVICE PROVIDER and its successors and assigns shall comply with terms after termination of this Agreement, with respect to the handling and processing of CLIENT's cardholder data.

3. CLIENT may elect to terminate this Agreement (with no penalty or obligations to CLIENT) for any material breach of these covenants relating to security of cardholder data.
4. SERVICE PROVIDER shall make commercially reasonable efforts to obtain certification for any required Merchant or Service Provider level status under the PCI Standards. SERVICE PROVIDER represents to CLIENT that, as of the time of execution of this Agreement, it is seeking certification as Level 1 Service Provider under the PCI Standards.