

March 25, 2008

TO: CHIEF ADMINISTRATIVE OFFICERS (CAOS) AND CHIEF FINANCIAL OFFICERS (CFOS)

RE: UCLA Guidelines for Credit/Debit Card Processing

Dear Colleagues:

There has been a growing interest in the use of credit and debit cards as payment options for online and in person transactions. This methodology is encouraged by Corporate Financial Services (CFS) because it reduces cash handling on campus, funds are deposited faster and it greatly enhances the University's ability to serve its customers. However, it is critical that campus entities are aware of the various policies, procedures, and guidelines that govern all payments to the U.C. Regents, as well as recent payment card industry compliance mandates.

The delegation for banking services is restricted by the Standing Orders of The Regents to the UC Banking Services Group at the Office of the President (this was formerly in the Treasurer's Office). They, in turn, have appointed a single liaison at each campus, which is typically the Campus Controller. Each campus also has a designated Credit/Debit Card Coordinator that works with the UC Banking Services Group to establish new credit/debit card merchants and ensure that credit/debit card requirements are met. At UCLA, the Director of Student Financial Services, Marsha Lovell, is the UCLA Credit/Debit Card Coordinator. Campus departments that wish to accept credit or debit card payments must seek approval from the UCLA Credit/Debit Card Coordinator (who will coordinate with the Campus Controller, General Accounting, and UCOP Banking Services Group) to establish their merchant privileges. This means that Internet payment sites may not be developed, third party contracts may not be signed, nor may credit or debit cards be accepted for any purpose, in any manner without the approval of the UC Banking Services Group through its campus designee.

New Payment Card Industry Data Security Standard (PCI) regulations have mandated a standard of privacy and security policies and annual reporting requirements that must be followed for all credit/debit card processes. These standards must be adhered to by any merchant processing card payments on behalf of UCLA and all reporting requirements must be completed annually prior to June 30. PCI compliance has been accomplished on a campus-wide level for CyberPay internet payments and since the Departmental Deposit Form (DDF) program processes through CyberPay this has also obtained compliant status. All payment card processes must certify compliance with these new regulations, details of which are documented in Appendix A. All card merchants must now also attend annual PCI training. ***Annual mandatory training sessions for 2008 will occur April 10, 2008 from 1-3 PM in the NPI Auditorium and April 16, 2008 from 10-Noon in the Bradley Center.*** Merchants will be required to attend one of the two sessions. Additional information will be forthcoming from Student Financial Services directly to campus credit card merchant contacts.

Several years ago, CFS anticipated the demand for e-payments and, in collaboration with Administrative Information Systems (AIS), developed CyberPay, an Internet payment gateway system. CyberPay complies with all requirements imposed by the UC Banking Services Group, UC Business and Finance Bulletin BUS-49, ***Policy for Cash and Cash Equivalents Received***, and the University of California's Accounting Manual. CyberPay also complies with the new

PCI requirements. This system has been enhanced to help departments develop and operate unique, customized, function-specific websites while ensuring the timely, accurate and secure transmission of payment transactions to the bank and to the campus Financial System (FS). The system also provides protection for cardholders ensuring that card numbers and transaction information is properly encrypted and is not stored or made accessible for possible misuse. CyberPay has been reviewed and approved by the UC Banking Services Group.

Recently the online DDF program was enhanced and credit cards can now be authorized through this system. DDF is routed through the CyberPay back end processor so it complies with all PCI requirements. It was developed to provide a Mail Order, Telephone Order (MOTO) environment online for departments to aid in PCI compliance. All the security features of CyberPay are available through this system, so merchants who use this process must focus on secure storage of any credit/debit card hard copy medium they may have in their office, and it is encouraged that this be kept to a minimum. If DDF merchants retain hard copy information with cardholder data on it they will need to complete PCI Self-Assessment Questionnaire (SAQ) "B" annually. It is strongly recommended that disposal of sensitive data occur after six months. DDF merchants may NOT keep electronic files containing cardholder data. If merchants wish to do this they must complete PCI SAQ "D" and submit their networks to quarterly scans.

Terminal merchants must establish merchant IDs through Student Financial Services and use the UC approved processor. The PCI standards now dictate that PCI SAQ "B" must be completed annually for all entities using a terminal or imprint machine.

Agreements with third party processors require additional approvals to ensure that they incorporate UC banking requirements and are approved by the UC Banking Services Group and that the accounting for funds collected by the agency are consistent with University guidelines. Before a department may contract with a third party to process their payments, a variance must be issued by Student Financial Services after they receive approval from the Banking Services Group and the Controller's office. University depository requirements must be discussed and approved, the PCI status of the Third Party must be verified, contracts must include approved PCI language, and the business need must be justified to support a variance. Additionally, PCI standards now require that PCI SAQ "A" must be completed annually by the department and that the Third Party Processor must report compliance through a PCI Qualified Security Assessor (QSA).

Credit/debit cards at UCLA is a payment option we must work together to safeguard. Adherence to the PCI requirements and security of personal information must be our utmost concern. If there are campus entities processing credit/debit card payments using a merchant ID that was not established through Student Financial Services, these units need to contact Marsha Lovell, Director of Student Financial Services, at extension 66034 immediately to discuss compliance requirements.

Thank you for your cooperation.

Sincerely,



Susan K. Abeles
Associate Vice Chancellor/Controller
Corporate Financial Services

cc: Director Marsha Lovell

Appendix A

Due to the various requirements expected for credit/debit card processing entities, the following table has been developed to help enhance your understanding of the expectations at UCLA.

UCLA Credit/Debit Card Requirements

Payment Types	Options Available	PCI Requirements
Online Payment Acceptance using CyberPay	CyberPay is the UCLA designated payment option for all campus departments. CyberPay is PCI compliant for credit/debit card input, processing, and storage of card information.	Student Financial Services certifies PCI compliance for all CyberPay merchants. The only requirement expected of CyberPay merchants is attendance at annual PCI training, which has been mandated by the card industry.
Online Payment Acceptance for Third Party vendors using CyberPay	Departments who have a business need that cannot be met by the regular CyberPay connection may be able to use a direct Web Service connection with CyberPay for PCI compliant third party vendors. Specifications are strict in order to protect sensitive data. Contracts with any Third Party must contain PCI related disclosures.	The PCI compliance Self Assessment Questionnaire (SAQ) "A" must be completed annually by the department. The contract language with the third party processor must be updated to incorporate PCI requirements. The PCI compliance questionnaire SAQ "D" must be completed annually by the vendor with mandatory quarterly perimeter scans conducted. The results of the vendor's SAQ "D" must be visible on the VISA PCI compliance website. Attendance at annual PCI training is required for the department, as it has been mandated by the card industry.
Online Payment Acceptance – Third Party vendors not using CyberPay	Departments who have a business need that cannot be met by processing through the regular or Web Service CyberPay options must have their proposed payment solution approved by the UCOP Banking Services Group and a variance must be issued by Student Financial Services. Both UC banking expectations and PCI compliance are required with annual variance renewal. Contracts with any Third Party must contain PCI related disclosures, updated based on current SAQ "A" requirements.	The PCI compliance questionnaire SAQ "A" must be completed annually by the department. The PCI compliance questionnaire SAQ "D" must be completed annually by the vendor and mandatory quarterly perimeter scans must be conducted. The results of the vendor's SAQ "D" must be visible on the VISA PCI compliance website. Attendance at annual PCI training is required for the department, as it has been mandated by the card industry.

Mail Order / Telephone Order (MOTO)	The Departmental Deposit Form (DDF) online system is the UCLA designated payment option for all campus departments for credit card input, processing, and storage of card information when payments are received by phone or by mail.	If DDF merchants retain hard copies with cardholder data on them they will need to complete SAQ "B". It is strongly recommended that disposal of sensitive data occur after 6 months. DDF merchants may NOT keep electronic files of cardholder data. If merchants wish to do this they must complete SAQ "D" and submit to quarterly scans. Attendance at annual PCI training is required for the department, as it has been mandated by the card industry.
Mail Order / Telephone Order (MOTO)	Departments who have a business need that cannot be met by processing through the Departmental Deposit Form (DDF) must have their proposed payment solution approved by the UCOP Banking Services Group and a variance must be issued by Student Financial Services. Both UC banking deposit expectations and PCI compliance are required with annual variance renewal. Contracts with any Third Party must contain PCI related disclosures, updated based on current SAQ "A" requirements.	The appropriate PCI compliance questionnaire SAQ must be completed annually by the department based on system configuration, in coordination with the Campus Cashier Coordinator. The PCI compliance questionnaire SAQ "D" must be completed annually by the vendor and mandatory quarterly perimeter scans conducted. The results of the vendor's SAQ "D" must be visible on the VISA PCI compliance website. Attendance at annual PCI training is required for the department, as it has been mandated by the card industry.
Point of Sale Credit Card Merchants	Any merchant processing credit/debit cards via a Point of Sale (POS) system must establish their merchant ID (MID) through Student Financial Services and process through the UC approved processor. Departments who have a business need that cannot be met by processing through the UC approved processor must have their proposed processor approved and a variance must be issued by Student Financial Services. UC banking expectations is required with annual variance renewal. All POS systems must be approved by General Accounting and Student Financial Services prior to purchase with	If the POS system collects, stores, or transmits credit card information to the processor, PCI compliance questionnaire SAQ "C" must be completed annually and mandatory quarterly perimeter scans conducted. If a separate terminal is used to process credit cards, and just payment amounts are input into the POS system, SAQ "B" must be completed. This must be coordinated with the assistance of the Director of Student Financial Services.

	appropriate contractual disclosures required by PCI as noted in SAQ “C”.	Attendance at annual PCI training is required for the department, as it has been mandated by the card industry.
Terminal or Imprint Credit Card Merchants	Any merchant processing payments through a credit/debit card terminal must establish their merchant ID (MID) through Student Financial Services and process through the UC approved processor.	Annual completion of SAQ “B” is required. Daily settlement or auto-settlement is expected to ensure PCI compliance. Attendance at annual PCI training is required for the department, as it has been mandated by the card industry.

Please direct questions to Marsha Lovell at mlovell@finance.ucla.edu or at extension 66034.