UCSB Audit and Advisory Services

Internal Audit Report

Credit Cards
PCI Compliance

July 1, 2016

Performed by:
Jessie Masek, Associate Director
Antonio Manas-Melendez, Principal Auditor
Laurie Liao, Staff Auditor

Approved by:
Robert Tarsia, Director

Report No. 08-16-0013

This page intentionally left blank.

University of California, Santa Barbara

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
SANTA BARBARA, CALIFORNIA 93106-5140
Tel: (805) 893-2829
Fax: (805) 893-5423

July 1, 2016

To: Jim Corkill, Controller and Director
Business and Financial Services

Distribution

Re: **Credit Cards: PCI Compliance**
Audit Report No. 08-16-0013

As part of the 2015-16 annual audit services plan, Audit and Advisory Services has completed an audit of Payment Card Industry Data Security Standards (PCI DSS) compliance. Enclosed is the report detailing the results of our review.

The primary purpose of this review was to determine whether the plan developed by Business and Financial Services would bring UCSB practices in compliance with PCI DSS, and to provide assurance that practices in place or planned are consistent with UC and UCSB policies and procedures. We also evaluated the progress of PCI DSS compliance efforts and progress reporting.

We found that Business and Financial Services has made significant progress in bringing the campus into compliance with PCI DSS requirements, and that the compliance plan it has developed includes the necessary elements for further progress. We did note opportunities for enhancement, including better documentation of the project plan, procedures, guidelines, and other documentation needed to provide adequate guidance to campus merchants.

Detailed observations and management corrective actions are included in the following sections of the report. The management corrective actions provided indicate that each audit observation was given thoughtful consideration, and that positive measures have been taken or planned to implement the management corrective actions.

We sincerely appreciate the cooperation and assistance provided by Business and Financial Services personnel during the review. If you have any questions, please feel free to contact me.

Respectfully submitted,

Robert Tarsia
Director
Audit and Advisory Services

Enclosure

Distribution:

Finance and Resource Management
Kimberly Ray, Associate Director of Controls, Business and Financial Services
Matt Coy, Banking Services Administrator - Campus Credit Card Coordinator, Business and Financial Services

Enterprise Technology Services
Sam Horowitz, Chief Information Security Officer

cc: Chancellor Henry Yang
Vice Chancellor Administrative Services Marc Fisher
UCSB Audit Committee
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca

PURPOSE

The purpose of our audit was to review the plan developed by Business and Financial Services to bring University of California, Santa Barbara (UCSB) practices in compliance with Payment Card Industry Data Security Standards (PCI DSS) version 3.1, and to provide assurance that practices in place or planned are consistent with University of California (UC) and UCSB policies and procedures. We also evaluated the progress of PCI DSS compliance efforts and progress reporting. This audit is part of UCSB's fiscal year 2015-16 audit services plan.

SCOPE, OBJECTIVES AND METHODOLOGY

The scope of this review was limited to activities and documentation available through May 2016, and to campus merchants identified by Business and Financial Services as merchants for which the campus has compliance responsibility. Third party merchants and campus merchants not using University of California Regental merchant accounts or funds were not included in the scope of this review.

The objectives of this limited scope audit were to determine whether:

- The campus PCI DSS compliance plan includes sufficient elements to provide reasonable assurance that, at the end of the plan timeline, campus merchant environments will comply with PCI DSS requirements and UC and campus policies and procedures regarding credit card payments.

- Progress against the plan to date has been consistent with the established timeline.

To accomplish our objectives, our work included interviews, direct observations, review of documentation, testing of progress reporting, and other steps. Specifically, we:

- Researched and reviewed previous UC and California State University (CSU) audits related to PCI DSS, including:

    - *Internal Audit of PCI Compliance*, UC Riverside audit report dated June 19, 2013.
    - *Payment Card Industry (PCI) Merchant Compliance*, UC Santa Cruz audit report dated May 8, 2014.
    - *Payment Card Processing*, CSU Long Beach audit report dated February 24, 2016.

- Researched and reviewed UC and UCSB policies, best practices, and other guidance concerning PCI DSS, including:

    - Business and Finance Bulletin BUS-49, *Policy for Cash and Cash Equivalents Received* (Policy BUS-49).
    - *PCI DSS Requirements and Security Assessment Procedures v3.1*, published by PCI Security Standards Council, LLC.
    - *SAQ Instruction Guidelines v3.1*, published by PCI Security Standards Council, LLC.
    - *PCI DSS Mapped onto COBIT Processes Table*, published by ISACA.[1]

[1] ISACA is an international professional association focused on IT Governance.

- Reviewed and analyzed documentation available as of May 2016, including progress reports from the Navis PCI compliance self-assessment tool[2], progress reports presented to the UCSB Audit Committee, merchant terminal inventory, the *UCSB Payment Device Inspection Policy and Guidelines*, presentations, and other documents.

- Gained and documented an understanding of the PCI DSS compliance project's status through detailed interviews with Business and Financial Services personnel.

- Evaluated the campus PCI DSS compliance plan and determined whether the plan includes necessary elements to bring the campus into compliance with PCI DSS requirements, such as a clear and appropriate scope, timeline, objectives, procedures and other needed documentation, training initiatives, self-assessments, an incident response plan, and periodic progress reporting.

- Determined whether the progress of PCI DSS compliance self-assessment work is consistent with the timeline defined by Business and Financial Services.

- Reviewed and evaluated whether the status information reported to the UCSB Audit Committee at a February 29, 2016, meeting was consistent with the status of the self-assessment reflected by the Navis self-evaluation tool (discussed later).

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

BACKGROUND

As a result of growing concerns over credit card data security, five major credit card associations joined forces to establish the PCI Security Standards Council, LLC, in 2006. The organization serves as a global open body to develop, enhance, and disseminate security standards for payment account security.

The Payment Card Industry Data Security Standard

PCI DSS is a multifaceted security standard that sets the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions. PCI DSS was developed to encourage and enhance cardholder data security, and to facilitate the broad adoption of consistent data security measures globally. PCI DSS requirements are based on 12 core requirements; see Table 1 for a high-level overview.

PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, service providers, and all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. PCI DSS version 3.1 is currently in effect and will be retired on October 31 2016. PCI DSS version 3.2 was released in April 2016, and includes enhanced compliance requirements.

Failure to comply can result in significant fines, additional reporting requirements, or even loss of the ability to process credit card transactions. A security breach resulting from non-compliance could result in financial liability, loss of reputation, and potential reduction of alumni donations.

[2] A system provided by Coalfire, a qualified security assessor for Bank of America, engaged to help monitor and maintain the campus PCI DSS compliance plan.

UC Policy Requirements

According to Policy BUS-49, compliance with PCI DSS requirements is mandatory for all University units accepting credit/debit cards for payment. University units processing card transactions must understand the data security rules applicable to their processing environment. University units also must obtain approval to accept credit or debit cards in payment for goods or services. Upon approval, the unit is designated as a "Credit/Debit Card Merchant".

Table 1	**PCI Data Security Standards**
Core Requirements	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by businesses with a need-to-know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Source: Payment Card Industry (PCI) Security Standards, v3.1

Status of PCI DSS Compliance at UCSB

In 2014, a high percentage of the campus processing environments were not validated as compliant with the PCI DSS. In addition, some merchants had validated their compliance to an incorrect and less rigorous set of requirements. Business and Financial Services has since filled a Campus Credit Card Coordinator position and developed a plan to bring the campus into compliance.

50 campus merchant environments that must comply with PCI DSS requirements have been identified. As of May 31, 2016, 31 merchants had completed their validations of compliance, and 19 merchant environments were in various stages of completion. Business and Financial Services has set a "self-imposed" target compliance date of May 31, 2016, for all campus merchants. Merchants with a clear and imminent path to compliance through signed contracts with suppliers for more secure processing have an extension to July 31, 2016. By 2017, UCSB is

required to begin formal reporting on compliance to Bank of America Merchant Services, UCSB's acquiring bank.[3]

Business and Financial Services has reduced the number of core requirements by moving towards Point-to-Point Encryption (P2PE). By using P2PE, risk is reduced because data is instantly encrypted in the hardware and securely transmitted to the processor. However, payment card devices must be periodically examined by qualified inspectors to ensure that the equipment is not compromised.

Business and Financial Services has taken steps to qualify as an inspector to provide periodic checkups of payment card devices, and has also started to use SpotSkim[4] to help ensure the completeness of its monitoring activities. This software automatically sends a notification every 90 days to check the equipment.

Table 2	**PCI Merchant Levels and Self-Assessment Types**
Overview	
VISA Merchant PCI Level Criteria	**Level 1:** Merchants processing over 6 million VISA or Master Card (MC) transactions annually (all channels) or Global Merchants identified as Level 1 by any VISA Region. **Level 2:** Merchants processing 1 million to 6 million VISA or MC transactions annually (all channels). **Level 3:** Merchants processing 20,000 to 1 million VISA or MC e-commerce[5] transactions annually. **Level 4:** Merchants processing less than 20,000 VISA or MC e-commerce transactions annually and all other merchants processing up to 1 million VISA transactions annually.
Relevant PCI DSS Self-Assessment Types*	**SAQ A**: Card-not-present merchants that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. **SAQ B:** Merchants using only imprint machines and/or standalone, dial-out terminals with no electronic cardholder data storage. **SAQ P2PE-HW:** Merchants using only hardware payment terminals included in and managed via a validated, PCI P2PE solution, with no electronic cardholder data storage. **SAQ D for Merchants:** All merchants not included in descriptions for the above SAQ types.

Source: Bank of America site and Payment Card Industry (PCI) Security Standards, v3.1.
* SAQ stands for self-assessment questionnaire. Table only includes SAQ types applicable to the campus.

[3] The bank or financial institution that holds the merchant's bank account that is used for collecting the proceeds for credit card processing.
[4] This software helps to perform physical inspections of payment card devices.
[5] Electronic commerce, commonly known as e-commerce, is the buying and selling of products or services over electronic systems such as the Internet.

Self-Assessment Questionnaires for PCI DSS version 3

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers in reporting the results of their PCI DSS self-assessments. The different SAQ types are shown in Table 2. Merchants are assigned an applicable SAQ based upon the defined eligibility criteria for each SAQ, and according to instructions from their acquirer or payment brand(s).[6]

Coalfire

The campus has contracted with Coalfire Systems Inc., the systemwide PCI qualified security assessor that provides information technology audit and compliance services, and serves as qualified assessor for Bank of America.

CoalfireOne[7] was created for colleges and universities with departments that have hundreds of merchant accounts and decentralized systems. To facilitate achieving and monitoring compliance across multiple departments, CoalfireOne offers a robust self-assessment questionnaire and scanning solution for managing multiple merchant sites. This tool also provides reporting facilities to track the progress of the self-assessment process.

SUMMARY OPINION

We found that Business and Financial Services has made significant progress in bringing the campus into compliance with PCI DSS requirements, and that the compliance plan it has developed includes the necessary elements for further progress, such as a clear and appropriate, scope, timeline, objectives, training initiatives, self-assessment process, an incident response plan, and progress reporting. We did note opportunities for enhancement, including better documentation of the project plan, procedures, guidelines, and other documentation needed to provide adequate guidance to campus merchants.

Audit observations and management corrective actions are detailed in the remainder of the audit report.

[6] According to the PCI Security Standards Council, LLC.
[7] Coalfire Systems, Inc. application provides organizations with the testing, documentation, reporting tools, and support needed to manage SAQ and scanning.

DETAILED OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. PCI DSS Compliance Plan

We found that the plan developed by Business and Financial Services includes the necessary elements to bring the campus into compliance with PCI DSS requirements, such as a clear and appropriate, scope, timeline, objectives, training initiatives, self-assessment process, an incident response plan, and progress reporting. However, we did note opportunities to enhance the plan. Table 3 summarizes the results of our evaluation.

Table 3 Project Plan Evaluation

	Status
Project Plan	The plan has a clearly defined scope, timeline, and objectives. However, some aspects have not been fully documented.
Procedures and Guidelines	Procedures, guidelines, and other needed documentation to provide adequate guidance to campus merchants in completing self-assessments are located in several places, and may not provide clear enough common guidance to understand and answer self-assessment questions from a campus merchant perspective.
Training	Training courses are available in the UC Learning Center. However, Business and Financial Services has limited ability to ensure that all required personnel take the training.
Oversight	Business and Financial Services performs high-level oversight of the self-assessment process and does not validate that each answer is accurate. Next year, Business and Financial Services will have a plan to certify that self-assessments are accurate.
Incident Response	The existing UC incident response plan would qualify for PCI Compliance purposes. However, it is not specific to credit cards.
Progress Reporting	The Navis self-assessment tool provides real-time progress reports of merchants' efforts in reaching compliance with PCI DSS. Business and Financial Services has presented at least one progress report to the UCSB Audit Committee.
Enhancement Plan	The first priority this calendar year is to be sure that campus complies with PCI DSS. Next year, Business and Financial Services will focus on improving the process, and this will include improving the documentation and the incident response plan.

Source: Auditor analysis.

We found that:

- The project plan and other written guidance such as procedures and guidelines are not fully documented or require improvement to provide adequate guidance for full implementation:

    - Available supporting documentation provides a broad understanding of PCI DSS requirements. However, it does not focus on providing adequate guidance to campus merchants to understand self-assessment questions and provide consistent answers.

    - Business and Financial Services is working on improved documentation, including FAQs, procedures, and standard forms.

- Business and Financial Services has limited ability to ensure that all required personnel take the mandatory training available on the UC Learning Center. It is the merchants' responsibility to ensure that their employees complete the training; Business and Financial Services can only monitor that personnel who initiated the training have completed it.

- Business and Financial Services provides technical support and performs high-level oversight of the self-assessment process. However, it is the merchants' responsibility to accurately complete the self-assessment questionnaire, and there is no formal process to validate self-assessments. Certifications of self-assessment questionnaires by Business and Financial Services will be required next year.

- The plan does not address the measures to be taken by the campus for merchant environments that do not comply with PCI DSS requirements by December 31, 2016. Non-compliance may result because merchants have not completed the self-assessment questionnaire, or because Coalfire determines that some merchant environments do not comply with PCI DSS requirements. To minimize potential disruptions, these measures should be documented and communicated to campus merchants.

- The existing UC incident response plan is acceptable as a credit card incident response plan. However, it is not specific to credit cards, so Business and Financial Services is planning to develop an incident response plan specifically for credit cards.

B. Tracking Progress and Reporting

Progress of Self-Assessment

Campus progress on the self-assessment process is generally consistent with the established timeline. Business and Financial Services notes that:

- 31 merchant environments have completed the PCI DSS self-assessment questionnaire, consistent with the established May 31, 2016, milestone. Another 14 merchant environments have requested a time extension until July 31, 2016.

- 6 campus merchant environments did not complete their self-assessment by May 31, 2016, and did not request an extension.

The Banking Services Administrator-Campus Credit Card Coordinator is confident that the self-assessments for most environments will be completed before July 31, 2016.

Transportation and Parking Services is completing the assessments for campus parking permit dispensers with limited participation by Business and Financial Services. There are some concerns regarding technical limitations of campus parking dispensers that could affect the current classification of this environment as SAQ P2PE-HW. If this environment needs to be reclassified, it would require complying with requirements that are more restrictive than initially expected. This would affect the timeline for completing this assessment.

Progress Reporting

We found that progress reporting is sufficient to keep stakeholders informed:

- The Navis self-assessment tool provides real-time progress reports of merchants' efforts in reaching compliance with PCI DSS. Business and Financial Services creates tracking reports to compare this progress with the compliance plan's timeline.

- Business and Financial Services has presented at least one progress report to the UCSB Audit Committee. Our review found only minor differences between progress reported to the UCSB Audit Committee and the status of the self-assessments in Navis.

We recommend that Business and Financial Services continue with the enhancements to its plan already initiated, and evaluate additional measures for improvement, including:

- Continuing with enhancement of project documentation, including the project plan, procedures, guidelines, and other needed documentation to provide adequate guidance to campus merchants.

- A compliance review to help ensure that required personnel take the mandatory training. This could be accomplished by requesting the lists of merchants' employees managing credit cards or cardholders information, and determining that a sample of them have completed the training.

- Evaluating alternatives for implementing a certification process for self-assessment questionnaires.

- Document and communicate to campus merchants the measures to be taken for merchant environments that do not comply with PCI DSS requirements by the required date. Determine alternatives for merchants that are not in compliance by December 31, 2016.

- Evaluate the current PCI compliance plan in Transportation and Parking Services and determine the additional steps required to ensure that the department will be in compliance by December 31, 2016.

- Document a new plan and timeline for any remaining merchants to complete the required self-assessment.

Management Corrective Actions

As the audit notes, Business and Financial Services will continue with the enhancements to its plan already initiated, and evaluate additional measures for improvement, including:

- Continuing with enhancement of project documentation, including the project plan, procedures, guidelines, and other needed documentation to provide adequate guidance to campus merchants.

- A compliance review to help ensure that required personnel take the mandatory training.

- Evaluating alternatives for implementing a certification process for self-assessment questionnaires.

- Documenting and communicating to campus merchants the measures to be taken for merchant environments that do not comply with PCI DSS requirements by the required date; determining alternatives for merchants that are not in compliance by December 31, 2016.

- Evaluate the current PCI compliance plan in Transportation and Parking Services and determine the additional steps required to ensure that the department will be in compliance by December 31, 2016.

- Document a new plan and timeline for any remaining merchants to complete the required self-assessment.

Audit and Advisory Services will perform an initial follow-up on the progress of these issues by December 31, 2016.

Appendix	Definitions
Term	**Description**
Cardholder Data Environment (CDE)	Comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications.
Encryption	Process of converting information into a form that is unintelligible except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure.
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Merchants	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.
Payment Card Industry Data Security Standards (PCI DSS)	A multifaceted security standard that sets the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.
PCI Security Standards Council	A global open body formed to develop, enhance, disseminate, and assist with the understanding of security standards for payment account security. Founding members: American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.
Point-To-Point Encryption (P2PE)	Provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction until the data reaches the solution provider’s secure decryption environment.
Qualified Security Assessor (QSA)	Qualified by PCI SSC to perform PCI DSS on-site assessments.
Report On Compliance (ROC)	Report documenting detailed results from an entity’s PCI DSS assessment.
Self-Assessment Questionnaire (SAQ)	Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.
Sensitive Authentication Data (SAD)	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Source: Payment Card Industry (PCI) Security Standards, v3.1