RIVERSIDE: AUDIT & ADVISORY SERVICES

June 19, 2013

To: Bobbi McCracken, Associate Vice Chancellor
Financial Services

Subject: Internal Audit of PCI Compliance

Ref: R2013-03

We have completed our audit of Payment Card Industry (PCI) Compliance in accordance with the UC Riverside Audit Plan. Our report is attached for your review.

We will perform audit follow-up procedures in the future to review the status of management action. This follow-up may take the form of a discussion or perhaps a limited review. Audit R2013-03 will remain open until we have evaluated the actions taken.

We appreciate the cooperation and assistance provided by the departments reviewed. Should you have any questions concerning the report, please do not hesitate to contact me.

Gregory Moore
Director

cc: Audit Committee Members
SBS Director Asirra Suguitan
Associate Vice Chancellor & CFAO Danny Kim
Associate Vice Chancellor & CFAO Georgianne Carlson
Assistant Vice Chancellor Andy Plumley
Director Scott Campbell
Director Russ Harvey
Manager Cindy Flannery

UNIVERSITY OF CALIFORNIA AT RIVERSIDE

AUDIT & ADVISORY SERVICES

MEMBER OF ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INTERNAL AUDIT REPORT R2013-03

PCI COMPLIANCE

JUNE 2013

Approved by:

_____
Gregory Moore
Director

_____
Noahn Montemayor
Principal Auditor

_____
Michael R. Jenson
Past Director

UC RIVERSIDE
PCI COMPLIANCE
INTERNAL AUDIT REPORT R2013-03
JUNE 2013

I. MANAGEMENT SUMMARY

In November 2011, a security breach occurred that involved unknown individuals who remotely penetrated UCR's Dining Services point-of-sale (POS) devices. The security breach resulted in unauthorized access to credit/debit card numbers, cardholder names, card expiration dates, and encrypted personal identification numbers (PINs). Upon learning of the penetration, the University immediately conducted an investigation and took action to prevent further breaches.

The Payment Card Industry Data Security Standards (PCI DSS) developed by the major credit card companies come with serious consequences. Failure to comply with PCI-DSS requirements can result in stiff contractual penalties or sanctions from members of the payment card industry. Another credit card breach will subject the University to the following penalties by each credit card brand.

- 1st occurrence in a rolling 12-month period: up to $50,000
- 2nd occurrence in a rolling 12-month period: up to $100,000
- 3rd occurrence in a rolling 12-month period: Fines at the discretion of the credit card issuers or termination of merchant accounts or both
- Liability for all fraud losses incurred from compromised account numbers
- Liability for the cost of re-issuing cards associated with the compromise
- Liability for the cost of any additional fraud prevention/detection costs incurred by credit card issuers associated with the compromise
- Additional fines related to the violation of improper storage of Cardholder data up to $500,000.

Additionally, the campus would be subject to additional reporting including an annual Report of Compliance (ROQ) completed by a PCI Qualified Security Assessor (QSA) for all campus merchants. The estimated cost is $19,800 - $49,500 per year.

The work performed within the scope of this audit was designed to help evaluate the effectiveness of management practices and internal controls implemented to achieve compliance with PCI DSS as well as federal, state and local regulations, and University policy and procedures.

Positive observations included:

* Financial Services and Computing & Communications (C&C) continue to provide technical and business process oversight to campus departments accepting credit/debit cards.

* To facilitate compliance with PCI DSS, the campus engages the services of an independent QSA and Approved Scanning Vendor (ASV) certified by the PCI Security Standards Council. This agreement provides the required annual PCI training via an on-line format.

* Management has consolidated cardholder data into fewer, more controlled locations by establishing private networks for POS systems that are isolated from the rest of the Campus network.

* External vulnerability scans are conducted monthly by an ASV on Secure Pay, private networks for campus POS systems, and departmental or third party sites not using Secure Pay for internet payment processing.

* C&C performs quarterly internal vulnerability scans on departmental storefronts utilizing Secure Pay for their internet credit card processing.

* In FY2012, Financial Services and C&C shared lessons learned from the Housing, Dining, & Residential Services (HDRS) breach with campus merchants, CFAOs, and campus merchant's IT units. C&C has developed a website with presentations from previous meetings, general campus IT requirements, and information on what to do in case of a data security breach.

We observed some areas that need enhancement to strengthen internal controls and/or effect compliance with University policy.

1) After the November 2011 breach, a "Gap Analysis" was conducted by a QSA of the HDRS cardholder data environment to the PCI DSS requirements. It was determined that "UCR (HDRS) would be non-compliant if PCI compliance validation were pursued." (Section III.A.)

2) The Campus Store, UCR Card Services, and SecurePay were out of compliance based on the results of the most recent annual PCI DSS self-assessment performed using the Self-Assessment Questionnaire (SAQ). (Section III.B.)

These items are discussed below. Minor items that were not of a magnitude to warrant inclusion in the report were discussed verbally with management.

II. INTRODUCTION

A. PURPOSE

UC Riverside Audit & Advisory Services (A&AS), as part of its Audit Plan, reviewed the effectiveness of management practices and internal controls implemented to achieve compliance with PCI DSS as well as

federal, state and local regulations, and University policy, procedures, service contracts and agreements.

B. BACKGROUND

In 2006, the 5 leading PCI payment brands – American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International – jointly announced the formation of an independent council, the PCI Security Standards Council (The Council), to manage the ongoing evolution of PCI DSS, a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

PCI DSS encourages enhanced cardholder data security and facilitates the broad adoption of consistent data security measures. It provides a baseline of technical and operational requirements designed to protect cardholder data. It applies to all entities involved in payment card processing – merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS is a set of 12 minimum requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.

The Council provides training and certification programs for two kinds of independent experts to help with PCI compliance: QSA and ASV. QSAs are approved by the Council to assess and validate compliance with PCI DSS. ASVs are approved by the Council to validate adherence to PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers. The proficiency with which QSAs and/or ASVs conduct assessments has enormous impact on the consistent and proper application of PCI DSS and its effectiveness to provide a defense against data exposure and compromise.

The University has engaged the services of a new QSA and ASV effective May 22, 2013. The new vendor will provide PCI consulting services and assist departments in completing SAQs.

Campus Policy No. 200-17 governs departments' roles and responsibilities with accepting credit/debit cards payments.

C. SCOPE

A&AS reviewed overall campus and departmental business processes and operating practices that support compliance with PCI DSS as well as University policy and procedures related to accepting credit/debit cards as a form of payment.

Procedures performed included interviews of selected personnel, the use of questionnaires, and review and analysis of particular elements of credit

card processing operations. Review procedures were designed to evaluate the following assertions:

- Campus management practices and control activities to achieve compliance with PCI DSS are effective, and related policy, procedures, roles, and responsibilities are defined and adequately communicated.
- Department management adequately oversees business processes and operating practices related to credit/debit card payment processing to ensure the confidentiality and integrity of financial transactions and cardholder information as well as compliance with PCI DSS and applicable University policy and procedures.
- Credit/Debit card processing policies, procedures, guidelines, and recommended practices are in writing, available, clear, and well understood and implemented by department staff.
- Information security measures, including physical security, application and user access controls, and network security are implemented to support security objectives and manage risks generally associated with computing and communication.

Three (3) campus departments, together responsible for 539,400 or 87% of the 616,900 total number of campus credit/debit card transactions in fiscal year 2011-2012, were selected for a closer review of department activities related to PCI compliance in general and the cardholder data environment in particular. These departments are the Campus Store (Bookstore), HDRS, and Transportation & Parking Services (TAPS).

D. INTERNAL CONTROLS AND COMPLIANCE

As part of the review, internal controls were examined within the scope of the audit.

Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the achievement of objectives in the following categories:

* effectiveness and efficiency of operations
* reliability of financial reporting
* compliance with applicable laws and regulations

Substantive audit procedures were performed during September 2012 through February 2013. Accordingly, this evaluation of internal controls is based on our knowledge as of that time and should be read with that understanding.

III. OBSERVATIONS, COMMENTS, AND RECOMMENDATIONS

A. PCI Compliance Validation

In May 2012, UC engaged an independent QSA to conduct a "Gap Analysis" to analyze the current status of the HDRS cardholder data environment against PCI DSS requirements. It was determined that "UCR (HDRS) would be non-compliant if PCI compliance validation were pursued."

COMMENTS

The Council sets the PCI security standards, but each payment card brand has its own program for compliance, validation levels, and enforcement, including provisions for performing self-assessments and when to engage a QSA. Acquiring financial institutions assign compliance validation requirements to merchants. Due to past data compromise, in addition to submitting a passing SAQ, HDRS is required to submit an annual Report on Compliance (ROC) as well as documentation of successful performance of quarterly network perimeter scans by a qualified scan vendor annually to merchant bank as required by Visa card brand.

The PCI Gap Analysis report was prepared by a QSA authorized to perform assessments for all the major payment card brands. The report provides details of the areas of non-compliance determined as a result of applying PCI DSS Security Audit Procedures to the credit card processing environment prevailing at HDRS within the scope of the analysis.

HDRS management and the Office of the Vice Chancellor for Student Affairs (VCSA) Technology Services department have been working appropriately to resolve data security issues identified in the PCI Gap Analysis report.

The Campus Store cardholder data environment was not included in the scope of the QSA's Gap Analysis. However, we note some technology and process vulnerabilities similar to those identified at HDRS. Although not required at this time, cardholder data captured using card swipe machines is not encrypted while on the private network. Business system components and software may not be current with the latest vendor-supplied updates and security patches. Logging mechanisms, audit trails, or other means that enable tracking of user activities to prevent, detect, or minimize potential cardholder data compromise are not yet in place. Campus Store management and VCSA Technology Services are aware of these issues and are working towards remediation.

RECOMMENDATIONS

All instances of PCI DSS non-compliance identified in the Gap Analysis Report as existing in HDRS should be corrected as soon as possible. Where appropriate, lessons learned should be applied to other VCSA POS merchants.

VCSA MANAGEMENT RESPONSE

Post the November 2011 compromise, UCR engaged Trust Wave, as a QSA. VCSA implemented the required elements during 2012. In March 2013, HDRS prepared and reviewed with Bank of America a passing SAQ-C. HDRS is now operating under a framework focused on continued compliance.

On applying lessons learned to other VCSA POS merchants, management must review merchants subject to PCI- DSS annually or when a new merchant comes on line to ensure:

1. Merchants are completing the correct SAQ as required by PCI-DSS.
2. Merchants are aware of, operating under and following approved division, campus and system policies.
3. Merchants use an evidence-based method of determining compliance when completing the SAQs.
4. Merchants review SAQs with the responsible technology department.

B. <u>PCI DSS Self-Assessment Questionnaire</u>

The Campus Store, UCR Card Services, and SecurePay were out of compliance based on the results of the most recent annual PCI DSS self-assessment performed using the SAQ.

COMMENTS

The SAQ is a validation tool for all entities involved in payment card processing that are not required to undergo onsite assessments and submit ROCs. It assists in self-evaluating compliance with PCI DSS and consists of two components: (1) Questions relating to PCI DSS requirements, and (2) an Attestation of Compliance, a self-certification of eligibility to perform and actual performance of the self-assessment.

All 20 campus departments (merchants) accepting credit/debit cards as a form of payment and SecurePay, UCR's Internet credit card gateway, are required to self-assess compliance with PCI DSS using the SAQ. During the conduct of the audit, the Campus Store, UCR Card Services, and SecurePay were out of compliance, based on the results of their most recently completed SAQs.

RECOMMENDATIONS

The Campus Store, UCR Card Services, and SecurePay should immediately remediate any areas of non-compliance identified during the self-assessment process and update the SAQs.

Management should consider campus sanctions for non-compliance, such as suspending merchant ids, to mitigate the risks associated with potential security breaches.

CAMPUS STORE MANAGEMENT RESPONSE

In 2012, VCSA initiated a review of the Book Store credit card operations. As a result, we self-reported a non-passing SAQ-C and outlined an action plan. On May 30, 2013, the Book Store completed a passing SAQ-C. The IT policies and local practices associated with this plan are in place. The Book Store is now operating under a framework focused on continued compliance.

UCR CARD OFFICE MANAGEMENT RESPONSE

In 2012, VCSA initiated a review of the Card Office credit card operations. As a result, VCSA self-reported a non-passing SAQ-C and outlined an action plan. On May 30, 2013, the Card Office completed a passing SAQ-C. The IT policies and local practices associated with this plan are in place. The Card Office is now operating under a framework focused on continued compliance.

C&C (FOR SECUREPAY) MANAGEMENT RESPONSE

C&C has always operated SecurePay within a very secure, robust technical environment and has remediated any technical compliance issues immediately upon notification or often times in advance of any external discover (e.g. via scanning). During early 2013, C&C completed an internal review relating to SecurePay firewalls, host based security, network security, physical security, and logical security. The Director of Computing Infrastructure and Security provided UCR's CIO a positive attestation relating to the robustness of SecurePay security. Moreover, in recent months, SecurePay has successfully passed both internal and external (TrustKeeper) vulnerability scans. Finally, C&C completed a PCI Self-Assessment Questionnaire C on April 22, 2013 and subsequently submitted it to the appropriate campus oversight group.

In July of 2013 the SecurePay method of cardholder data handling will change. UCR will utilize an approval methodology that removes ALL campus servers from the transaction processing process. As such, C&C anticipates that future SecurePay SAQ surveys will be conducted at the "SAQ-A" level.

FINANCIAL SERVICES MANAGEMENT RESPONSE

A new system-wide contract was issued in April 2013 to a PCI QSA/ASV vendor, Coalfire. In May 2013, the campus engaged with Coalfire on a campus PCI Needs Assessment. Coalfire leads individual sessions with campus merchants and their IT staff to complete the more complex SAQs (C and D formats). Coalfire will provide general training on completion of SAQ A's & B's. Beginning FY2014, the campus will require an annual acknowledgement from all campus merchants regarding their responsibilities related to PCI compliance. The acknowledgement will inform the merchant of possible consequences, including the suspension of merchant ids as necessary.