November 13, 2015

Dr. Horace Mitchell, President
California State University, Bakersfield
9001 Stockdale Highway
Bakersfield, CA 93311-1022

Dear Dr. Mitchell:

Subject: Audit Report 15-42, Payment Card Processing, California State University, Bakersfield

We have completed an audit of Payment Card Processing as part of our 2015 Audit Plan, and the final report is attached for your reference. The audit was conducted in accordance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

I have reviewed the management response and have concluded that it appropriately addresses our recommendations. The management response has been incorporated into the final audit report, which has been posted to the Office of Audit and Advisory Services’ website. We will follow-up on the implementation of corrective actions outlined in the response and determine whether additional action is required.

Any observations not included in this report were discussed with your staff at the informal exit conference and may be subject to follow-up.

I wish to express my appreciation for the cooperation extended by the campus personnel over the course of this review.

Sincerely,

Larry Mandel
Vice Chancellor and Chief Audit Officer

c: Timothy P. White, Chancellor
PAYMENT CARD PROCESSING

California State University,
Bakersfield

Audit Report 15-42
October 13, 2015
EXECUTIVE SUMMARY

OBJECTIVE

The objectives of the audit were to review campus payment card processing activities to determine whether the campus had assessed the risks and exposures related to payment card processing and established a program to ensure compliance with applicable laws and payment card industry (PCI) regulations; and, if applicable, to ascertain the effectiveness of controls implemented to protect payment card information and adhere to PCI regulations.

CONCLUSION

Based upon the results of the work performed within the scope of the audit, except for the effect of the observations described below, the controls in effect as of June 26, 2015, taken as a whole, were sufficient to meet some of the objectives of this audit.

The controls and processes established over payment credit card processing at California State University, Bakersfield (CSUB) included a risk assessment for credit card processing provided on campus. In addition, the campus had recently established a program to assess payment card processing, and had identified the controls required to meet PCI compliance. However, some opportunities to improve governance and oversight and ensure compliance by outsourced entities were identified.

Specific observations, recommendations, and management responses are detailed in the remainder of the report.
OBSERVATION

The campus did not have a formal governance and oversight structure to ensure that all PCI requirements were being addressed on an annual and ongoing basis.

Specifically, the existing structure did not ensure that the following PCI requirements were being met:

- Documentation of all payment process flows and corresponding self-assessment questionnaires, including outsourced vendor operations.
- Documentation that procedures are in place to satisfy compliance with recommended controls in third-party vendor instruction manuals.
- Assurance of PCI compliance in all products used in credit card processing prior to procurement.

RECOMMENDATION

We recommend that the campus implement formal governance and oversight to provide ongoing oversight to ensure that all PCI requirements are being addressed on an annual and ongoing basis.

MANAGEMENT RESPONSE

The university will implement a formal governance structure charged with oversight that ensures all PCI requirements are being addressed on an annual and ongoing basis.

The expected date of completion is February 29, 2016.
GENERAL INFORMATION

BACKGROUND

The Integrated California State University Administrative Manual (ICSUAM) §8000, Information Security Policy, requires the California State University (CSU) to protect the confidentiality, integrity, and availability of CSU information assets and applies to all categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).

In order to safeguard the personal information of individuals who hold credit cards, the five major payment card brands have endorsed the PCI Data Security Standard (DSS). The PCI Security Standards Council owns, develops, maintains, and distributes the PCI DSS. As a global standard, the PCI DSS applies to any entity worldwide that stores, processes, or transmits credit card-holder data. This includes financial institutions, merchants, and service providers in all payment channels.

Each payment card brand has PCI auditing and reporting requirements that merchant banks must meet in order to gain access to the payment network. The merchant banks must provide evidence that merchants using their bank, and any service providers used by those merchants, are PCI-compliant. This chain of liability at each level is designed to protect credit card-holder data by using PCI DSS to mitigate the risk of data breaches in the rapidly evolving threat landscape.

Although the PCI has defined compliance standards for data security, the CSU has not provided any specific guidance regarding oversight, governance, or assurance that annual compliance is achieved and maintained. It is the policy of the CSU that campuses be given the choice of credit card-processing vendors that best meet individual or unique campus hardware, service, and application requirements.

At CSUB, the vice president of finance and administration has primary oversight responsibility for credit card processing activities on campus. An informal compliance structure exists for ensuring that all credit card processing contracts and purchases are properly initiated, that compliance questionnaires are completed, and that controls are appropriate to ensure compliance with the PCI DSS. In addition, to minimize the burden on the campus to perform compliance and reporting requirements, CSUB has outsourced many of the credit card processing activities.

SCOPE

We visited CSUB from June 15, 2015, through June 26, 2015. Our audit and evaluation included the audit tests we considered necessary in determining whether payment card processing controls are in place and operative. The audit focused on procedures in effect from January 1, 2014, through June 30, 2015.
Specifically, we reviewed and tested:

- Processes to identify all credit card-processing activities on the campus and establishment of plans to address the associated risks.
- Establishment of a campuswide PCI compliance program that includes completion of PCI compliance reports, validation of applicable system and network controls, and scanning.
- Processes to ensure that the control framework for payment card processing is complete, and that controls are operating effectively.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our testing and methodology was designed to provide a managerial-level review of payment card processing activities, which included detailed testing on a limited number of payment card processing controls. Our review was not intended to formally assess or validate campus compliance with PCI DSS.

CRITERIA

Our audit was based upon standards as set forth in CSU Board of Trustee policies; Office of the Chancellor policies, letters, and directives; campus policies and procedures; and other sound administrative practices. This audit was conducted in conformance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

This review emphasized, but was not limited to, compliance with:

- ICSUAM §8000, Information Security
- PCI DSS 3.1, Requirements and Security Assessment Procedures, dated April 2015

AUDIT TEAM

Senior Director: Mike Caldera
Audit Manager: Greg Dove