County of San Diego

Auditor and Controller

Office of Audits & Advisory Services

E-Commerce, Credit Card Payments Audit

Final Report

Chief of Audits: Juan R. Perez
Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Christopher Ellis, CISA, CISSP

Report No. A16-001

May • 2017

Intentionally Left Blank

County of San Diego

TRACY M. SANDOVAL
DEPUTY CHIEF ADMINISTRATIVE OFFICER/
AUDITOR AND CONTROLLER

AUDITOR AND CONTROLLER
OFFICE OF AUDITS & ADVISORY SERVICES
5530 OVERLAND AVENUE, SUITE 330, SAN DIEGO, CA 92123-1261
Phone: (858) 495-5991

JUAN R. PEREZ
CHIEF OF AUDITS

May 31, 2017

TO: Dan McAllister, Treasurer/Tax Collector
Treasurer/Tax Collector

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: E-COMMERCE, CREDIT CARD PAYMENTS AUDIT

Enclosed is our report on the E-Commerce, Credit Card Payments Audit. We have reviewed your response to our recommendations and have attached them to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board of Supervisors Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. The Office of Audits & Advisory Services will contact you or your designee near the end of each quarter to request your response.

Also attached is an example of the quarterly report that is required until all actions have been implemented. To obtain an electronic copy of this template, please contact Christopher Ellis at (858) 694-2424.

If you have any questions, please contact me at (858) 495-5661.

JUAN R. PEREZ
Chief of Audits

AUD:CE:dp

Enclosure

c: Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor and Controller
Damien Quinn, Group Finance Director, Finance and General Government Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of the E-commerce, credit card and electronic check (eCheck) payment process. The objective of the audit was to evaluate the County of San Diego's (County) electronic payment risk exposure to verify whether controls are in place and operating effectively to ensure information security and conformance with best practices established by industry standards.

Background

At the time of the audit, 20 County departments were accepting payment by credit card through point of sale (POS) devices and/or through an online E-commerce portal.

Electronic payments made for County services are increasing on an annual basis. The Treasurer-Tax Collector (TTC) collects the largest amount of electronic payments of the County departments. In FY 2014-15, TTC collected $140,947,938 credit card and $786,712,640 eCheck payments. In FY 2015-16, they collected $157,444,132 credit card and $989,080,804 eCheck payments, a 12% and 25% increase respectively.

In September 2014, TTC requested assistance from the County Technology Office (CTO) in completing the annual self-assessment questionnaire (SAQ) required for conformance with payment card industry (PCI) standards. The CTO identified other departments accepting credit card payments for County services and assumed responsibility for the administration of the annual PCI assessment.

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor (ISA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

The SAQ is a validation tool for organizations that self-assess their PCI DSS conformance and are not required to submit a ROC. Completing a SAQ helps merchants evaluate their security practices and conformance with the required PCI DSS.

There are nine different versions of the SAQ. The version that each organization is required to complete depends on how they handle credit card data. The County is currently required to complete PCI SAQ

version A[1] and B[2] since credit card payments are being accepted through POS devices and E-commerce portals, but payment information is not stored.

As noted above, County departments are increasingly accepting eChecks as payment for services. Financial institutions created an organization called the National Automated Clearinghouse Association (NACHA) which manages the development, administration, and governance of the Automated Clearing House (ACH) network. NACHA developed a set of operating rules and guidelines that financial institutions, as well as organizations that accept eChecks must follow to ensure the movement of money and data is safe and secure. NACHA operating rules and guidelines include annual compliance audits.

In regards to regulatory requirements, California has Civil Codes that are a part of the 29 legal codes enacted by the California State Legislature, which together form the general statutory law of California. In particular, Section 1798.82 of the California Civil Code requires a person or business that conducts business in California to disclose a breach in the security of the data to a resident of California whose personal information was acquired by an unauthorized person. The Code also includes specific language, title, and format that must be used in the security breach notification.

Audit Scope & Limitations

The scope of the audit covered FY 2015-16 and included an evaluation of the County's electronic payment risk exposure to verify whether controls are in place and operating effectively to ensure data security and conformance with PCI DSS, NACHA, and California Civil Code requirements.

Four County departments were selected for review using a judgmental sampling approach based on the number and types of electronic payments accepted.

- Department of Parks & Recreation (DPR)
- Planning & Development Services (PDS)
- Auditor and Controller/Office of Revenue & Recovery (ORR)
- Treasurer-Tax Collector (TTC)

The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236.

---

[1] SAQ version A applies to e-commerce or mail/telephone-order merchants that have fully outsourced all cardholder data to PCI DSS validated third-party service providers with no storage, processing or transmission of cardholder data on the merchant's systems.

[2] SAQ version B are e-commerce merchants who outsource all payment processing to PCI DSS validated third parties and who have a website(s) that doesn't directly receive cardholder data that can impact security of payment transactions. No electronic storage, processing or transmission of cardholder data on the merchants systems or premises occurs.

Methodology

OAAS performed the audit using the following methods:

- Interviewed County stakeholders.
- Reviewed PCI DSS Version 3.1 requirements.
- Reviewed NACHA Operating Rules and Guidelines.
- Reviewed County department policies and procedures regarding electronic payments, point of sale (POS) devices, E-commerce portals, disposal of credit cardholder information, etc.
- Reviewed service agreements between County departments and payment service providers.
- Identified, reviewed, and tested controls over electronic payments to ensure data security and conformance with PCI DSS and NACHA requirements including verifying:
  - Cardholder data is masked appropriately.
  - Cardholder data contained in hardcopy form is properly disposed of.
  - Monitoring and tracking of point of sale devices is in place.
  - Information security policies and payment service provider agreements are complete and up-to-date.
  - eCheck payment controls are in place.

AUDIT RESULTS

Summary

Within the scope of the audit, the adequacy of controls over electronic payments to ensure alignment with PCI DSS and NACHA eCheck requirements need improvement. Specific issues were identified in the areas related to the partial redirect of credit card payment information; monitoring and tracking of POS devices; eCheck monitoring and conformance; and lack of service agreements with payment service providers.

Finding I: **Accela Partial Redirect**

The Land Use and Environment Group (LUEG) has a known issue that was identified in the most recent annual PCI assessment performed in 2015. Credit card and eCheck payment information is entered on LUEG's Accela[3] E-commerce website that is hosted on County servers and then redirected to Hewlett Packard Convenience Pay[4] (HPCP)

[3] Accela is web-based E-commerce software for processing payments from County citizens for services provided. Accela includes land, asset, licensing and legislative management.

[4] HPCP is an electronic payment service that enables the County to accept electronic payments for services provided including tax collection and other fees.

system for payment processing. This is a partial redirect of payment information. When a full redirect is used, payment information entered on an E-commerce website is sent directly to the payment processor. This process eliminates the security risks associated with transmitting payment information across County servers.

LUEG has been working with Hewlett Packard Enterprise (HPE) since July 2014 to implement a full payment redirect in Accela. This project was put on hold until December 2015 due to an upgrade of the Accela system. In January 2016, HPCP was acquired by Fiserv, Inc., which is currently in the process of implementing a full redirect of credit card and eCheck payment information processed by HPCP.

The County is performing a full redirect on all other credit card payments based off our testing and research performed by the CTO, so it is only required to perform SAQ A and B to comply with PCI DSS. However, due to the timing of this issue with the Accela partial redirect of credit card information, the County is currently not in conformance with PCI DSS. If the County fails to meet applicable PCI DSS requirements, there may be potential fees or penalties. Additionally, the County's risk exposure of a security breach increases. Section 1798.82 of the California Civil Code requires a person or business that conducts business in California to disclose a breach in the security of the data to a resident of California whose personal information was acquired by an unauthorized person. Failure to do so could result in prosecution under California's Business and Professions Code 17200-17210 by the California Attorney General.

Recommendation: The LUEG executive office should continue to monitor the progress of the Fiserv full redirect project and confirm if a viable solution exists and can be implemented in a timely manner. If this is not the case, then a new payment service provider should be considered.

Finding II: **Monitoring and Tracking of Point of Sale (POS) Devices**

Of the four departments sampled, only three have POS devices. These three departments need improvement in the areas of:

- policies and procedures for inspecting POS devices for tampering or substitution.
- inspection of devices for tampering or substitution.
- keeping an accurate and up-to-date POS device list.
- upgrading to new POS device models with chip readers.

Audit results for the three departments tested include:

- None of the three departments have policies and procedures to check for device tampering or substitution

- Three departments have not inspected their POS devices for tampering or substitution
- Two of the three departments do not have a POS device list or the list is not accurate and up-to-date.
- Two of the three departments have older model POS devices that do not have a chip reader.

PCI DSS requirements 9.9, 9.9.1, 9.9.2 and 9.9.3 stipulate that an up-to-date POS device list is maintained, devices be inspected for tampering or substitution, staff be trained to detect and report attempted tampering or substitution, and policies and procedures be developed for each PCI requirement.

Additionally, October 1, 2015 was the deadline established by the major U.S. credit card issuers, MasterCard, Visa, Discover and American Express, for merchants to upgrade to new POS devices with chip readers. After this deadline, the liability for card-present fraud shifted to whichever party is the least EMV-compliant[5] in a fraudulent transaction.

POS devices should be periodically inspected for tampering or substitution to prevent criminals from stealing cardholder data. A criminal may try to add a "skimming" component to a POS device to capture payment card details before they enter the device so that the transaction will still be completed as normal.

Lastly, if a POS device list is not kept up-to-date or if devices are not periodically inspected, the risk that devices could be stolen or substituted and cardholder data compromised increases.

Recommendation:

1. The CTO should add procedures around inspecting POS devices for tampering or substitution to the PCI Attestation Process and Procedure Manual.
2. DPR, PDS, and ORR should inspect their POS devices for tampering or substitution on a periodic basis.
3. DPR and PDS should ensure they have a POS device list, and that it is accurate and up-to-date.
4. DPR and ORR should upgrade to newer POS devices that include chip readers.

Finding III:

eCheck Monitoring and Compliance

At the time of audit testing, three of the four departments sampled accepted eChecks as a payment method. Similar to credit card payments, if a customer wants to make a payment using an eCheck, they are re-directed to a third party payment provider where they will

[5] EMV stands for Europay, MasterCard and Visa and is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.

enter all of the payment information including Account Number, Routing Number, Name, etc.

NACHA operating rules and guidelines for financial institutions, as well as organizations that accept eChecks or their third party payment providers must be followed to ensure the movement of money and data is safe and secure. These operating rules and guidelines include required annual compliance audits.

Currently there is no centralized function at the County with ownership over monitoring eCheck payments for conformance with NACHA requirements. Departments sampled did not have an established process in place to verify their third party payment providers' compliance with NACHA, and assumed that the responsibility for monitoring of eCheck payments was entirely on the third party payment service providers.

If the County or its third party payment service providers fail to meet applicable NACHA requirements there are potential fees or penalties including losing the ability to accept eChecks as a payment for services as detailed in the NACHA Operating Rules and Guidelines Subpart 10.4.7.

Recommendation: The TTC, ORR, and LUEG should ensure that individuals at each department responsible for monitoring service agreements with the payment service providers obtain the annual ACH Rules Compliance Audit that is required of Third-Party Service Providers by the NACHA Operating Rules and Guidelines Part 8.1, and review to verify compliance.

Finding IV: **Lack of Service Agreement with HPCP/Fiserv**

Two of the departments sampled (PDS, ORR) did not have a service agreement with their payment service provider HPCP/Fiserv for credit card and eCheck payments.

Prior to January 2016, HPCP was part of HPE and payment services were provided to County departments via work requests in accordance with provisions of the IT & Telecommunications Service Agreement between the County and HPE. As of January 2016, the Convenience Pay Services (HPCP) business was acquired by Fiserv, Inc. Although an HPE contracts manager has stated that the agreement regarding Convenience Pay services between HPE and the County was retained in its entirety by HPE and was not transferred to Fiserv, he did not provide evidence to support that statement. He further stated that as the primary contracting party, HPE engages Fiserv to provide Convenience Pay services to the County on its behalf in a manner consistent with service delivery before the sale of HPCP.

Without a written service agreement, the conditions and terms of service being provided may be undefined, including the County's rights, the service provider's compliance and performance responsibilities, penalties for not meeting commitments, liability for damages, etc.

PCI DSS requirement 12.8.2 states, "Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment."

Recommendation: The CTO, PDS and ORR should ensure that a service agreement between HPE and Fiserv, Inc. is established and signed off by the appropriate parties.

DEPARTMENTS' RESPONSE

County of San Diego

MIKEL HAAS
CHIEF INFORMATION OFFICER
(619) 531-5570

COUNTY TECHNOLOGY OFFICE
1600 PACIFIC HIGHWAY ROOM 308F, SAN DIEGO, CA 92101
www.sandiegocounty.gov/cto

SUSAN GREEN
ASSISTANT CHIEF INFORMATION OFFICER
(619) 515-4337

May 25, 2017

TO: Juan R. Perez, Chief of Audits
Office of Audits & Advisory Services

FROM: Mikel Haas, Chief Information Officer
County Technology Office (CTO)

CTO RESPONSE TO AUDIT RECOMMENDATIONS: IE-COMMERCE, CREDIT CARD PAYMENTS

Finding I: Monitoring and Tracking of Point of Sale (POS) Devices

OAAS Recommendation 1: The CTO should add procedures around inspecting POS devices for tampering or substitution to the PCI Attestation Process and Procedure Manual.

Action Plan: Agree. The CTO will add a POS tampering inspection section to the PCI Attestation Process and Procedure Manual.

Planned Completion Date: July 31, 2017

Contact Information for Implementation: Michael Teays, CISO

Finding IV: Lack of Service Agreement with HPCP/Fiserv

OAAS Recommendation 1: The CTO, PDS and ORR should ensure that a service agreement between HPE and Fiserv, Inc. is established and signed off by the appropriate parties.

Action Plan: Agree. DXC (formerly HPES) provided the CTO with a written statement that following the sale of HP Convenience Pay (HPCP) to Fiserv that DXC retained the HPCP service contract on behalf of the County and is providing PCI services in a manner fully consistent with the IT Outsourcing Agreement. Fiserv is listed on the PCISecurityStandards.org vendor PCI compliance website with a current expiration date of December 14, 2017. Additionally, the County has received the annual ACH audit report for Fiserv/Convenience Pay and no audit exceptions related to compliance with NACHA are reported.

Planned Completion Date: Completed

Contact Information for Implementation: Mike Teays, CISO

If you have any questions, please contact Mike Teays at (619) 316-5208.

MIKEL HAAS, Chief Information Officer
County Technology Office

CTO:MT:bm

County of San Diego

BRIAN ALBRIGHT
DIRECTOR
(858) 966-1301

DEPARTMENT OF PARKS AND RECREATION
5500 OVERLAND AVENUE, SUITE 410, SAN DIEGO, CA 92123
Administrative Office (858) 694-3030
www.sdparks.org

April 5, 2017

TO: Juan R. Perez
Chief of Audits

FROM: Brian Albright, Director
Department of Parks and Recreation

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: E-COMMERCE, CREDIT CARD PAYMENTS AUDIT

On behalf of the Department of Parks & Recreation (DPR), I thank the Office of Audits and Advisory Services for their professional work on this audit. The Department concurs with the findings and recommendations. Despite the observations noted, there has never been any tampering, substitution, or any issues reported. The vast majority of our DPR credit card business is conducted over the phone or on-line by customers. In response to the audit, DPR will take necessary actions to address the recommendations for improvement contained in the report.

Finding I: Accela Partial Redirect. Not applicable to DPR.

Finding II: Monitoring and Tracking of Point of Sale (POS) Devices.

OAAS Recommendations:

1. The CTO should add procedures around inspecting POS devices for tampering or substitution to the PCI Attestation Process and Procedure Manual.

2. DPR, PDS, and ORR should inspect their POS devices for tampering or substitution on a periodic basis.

3. DPR and PDS should ensure they have a POS device list, and that it is accurate and up-to-date.

4. DPR and ORR should upgrade to newer POS devices that include chip readers.

Action Plans:

1. Not applicable to DPR.

2. DPR will develop a procedure that each device be inspected for tampering or substitution regularly to prevent criminals from stealing cardholder's data and to mitigate

the potential risk of cardholder's data being compromised. As an additional control, each site should record the date of inspection at each site's "Logbook".

3. DPR will update the POS device list and will develop a process for Site Supervisors to report each device identification number that are in their possession quarterly. This process detects if devices were stolen or substituted.

4. DPR is currently in the solicitation process for the replacement of the existing reservation system and related payment processor/credit card terminals. During FY17/18, it is anticipated to award the contract to a new Provider and a payment processor that provide chip reader terminals for all locations accepting credit cards. In the interim, upgrading to newer POS devices that include chip readers would require a new payment processor other than Element. This process would basically take as long as our new reservation system which DPR has already initiated with the Department of Purchasing and Contracting to procure a system that complies with the PCI DSS requirements.

Planned Completion Date: Action Plans #2 and #3 - May 15, 2017; Action Plan #4 - DPR expects that this action plan will be finalized in the next 18 months, at which time DPR will reaffirm compliance with the audit requirement.

Contact Information for Implementation: Sean O'Neill, Information Technology Analyst

Finding III: eCheck Monitoring and Compliance. Not applicable to DPR.

Finding IV: Lack of Service Agreement with HPCP/Fiserv. Not applicable to DPR.

If you have any questions, please contact me at (858) 966-1301.

BRIAN ALBRIGHT
Director

BA:jl

County of San Diego

MARK WARDLAW
DIRECTOR

PLANNING & DEVELOPMENT SERVICES
5510 OVERLAND AVENUE, SUITE 310, SAN DIEGO, CA 92123
(858) 694-2962 • Fax (858) 694-2555
www.sdcounty.ca.gov/pds

April 17, 2017

TO: Juan R. Perez
Chief of Audits

FROM: Mark Wardlaw, Director
Planning & Development Services

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: E-COMMERCE, CREDIT CARD PAYMENTS

On behalf of Planning & Development Services (PDS), thank you to the Office of Audits and Advisory Services for their professional work on this audit. The department concurs with the findings and recommendations and will take necessary actions to address them.

Finding I: Accela Partial Redirect

OAAS Recommendation: The LUEG Executive Office should continue to monitor the progress of the Fiserv full redirect project and confirm if a viable solution exists and can be implemented in a timely manner. If this is not the case, then a new payment service provider should be considered.

Action Plan: Planning & Development Services (PDS) will continue to work with the LUEG Executive Office to confirm a viable solution exists and commits to implementing the solution in a timely manner. PDS will make user acceptance testing of the partial redirect solution a priority when the solution is ready for review and testing.

Planned Completion Date: December 31, 2017

Contact Information for Implementation: Stephanie Nicholas, Group Program Manager

Finding II: Monitoring and Tracking of Point of Sale (POS) Devices

OAAS Recommendation 1: The County Technology Office (CTO) should add procedures around inspecting Point of Sale (POS) devices for tampering or substitution to the Payment Card Industry (PCI) Attestation Process and Procedure Manual.

Action Plan: PDS will integrate any CTO procedures regarding inspecting POS devices for tampering or substitution added to the PCI Attestation Process and Procedure Manual to supplement internal procedures to ensure PCI Standard compliance.

obtain the annual ACH Rules Compliance Audit that is required of Third-Party Service Providers by the NACHA Operating Rules and Guidelines Part 8.1, and review to verify compliance.

Action Plan: PDS and LUEG Executive Office have requested from CTO that the County's IT outsourcer, DXC, provide the documentation of both 1) the service agreement(s) with the payment service provider and 2) the annual ACH Rules Compliance Audit that is required by Third-Party Service Providers to ensure compliance with the National Automated Clearing House Association (NACHA) Operating Rules and Guidelines Part 8.1.

If the CTO is unable to obtain the annual ACH Rules Compliance Audit from the Contractor, PDS and LUEG Executive Office will encourage CTO to document non-compliance with the Contractor and evaluate whether or not eChecks will continue to be accepted.

Planned Completion Date: December 31, 2017

Contact Information for Implementation: David Lindsay, LUEG Group Program IT Manager

Finding IV: Lack of Service Agreement with HPCP/Fiserv

OAAS Recommendation: The CTO, PDS and ORR should ensure that a service agreement between HPE and Fiserv, Inc. is established and signed off by the appropriate parties.

Action Plan: PDS and LUEG Executive Office will request from CTO that the service agreement between HPE and Fiserv, Inc. is documented and signed off by the appropriate parties.

Planned Completion Date: July 31, 2017

Contact Information for Implementation: County Technology Office

If you have any questions, please contact me at (858) 694-2962.

Sincerely,

MARK WARDLAW
Director

RECEIVED

APR 21 2017

OFFICE OF AUDITS & ADVISORY SERVICES

County of San Diego

TRACY M. SANDOVAL
DEPUTY CHIEF ADMINISTRATIVE OFFICER/
AUDITOR AND CONTROLLER

AUDITOR AND CONTROLLER
OFFICE OF REVENUE AND RECOVERY
POST OFFICE BOX 121909, SAN DIEGO, CA 92112-1909
(619) 515-6200

SEAN S. SANDER
REVENUE AND RECOVERY DIRECTOR

April 14, 2017

TO: Juan R. Perez, Chief of Audits
Office of Audits and Advisory Services

FROM: Sean S. Sander, Director
Office of Revenue and Recovery

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: E-COMMERCE, CREDIT CARD PAYMENTS AUDIT

Finding I: Accela Partial Redirect

OAAS Recommendation: The LUEG executive office should continue to monitor the progress of the Fiserv full redirect project and confirm if a viable solution exists and can be implemented in a timely manner. If this is not the case, then a new payment service provider should be considered.

Action Plan: N/A

Planned Completion Date: N/A

Contact Information for Implementation: N/A

Finding II: Monitoring and Tracking of Point of Sale (POS) Devices

OAAS Recommendation:

1. The CTO should add procedures around inspecting POS devices for tampering or substitution to the PCI Attestation Process and Procedure Manual.

2. DPR, PDS, and ORR should inspect their POS devices for tampering or substitution on a periodic basis.

3. DPR, and PDS should ensure they have a POS device list, and that it is accurate and up-to-date.

4. DPR and ORR should upgrade to newer POS devices that include chip readers.

Action Plan:

1. N/A

2. ORR POS devices are located in areas secure from the public. ORR will establish and implement procedures to inspect our POS devices (for tampering and/or substitution) to align with the CTO procedures developed and recommended as described in recommendation 1 (Finding II).

3. N/A

4. ORR is in the process of upgrading the Cashiering software and hardware. It is anticipated that this will be completed in one year. The POS devices included in the new system will contain chip readers and access controls. ORR currently leases the POS devices through Wells Fargo Merchant Services. Two branch locations currently have POS devices with a chip reader--as it was necessary to replace those machines for maintenance. If other current models need replacement (prior to the Cashiering Upgrade), those machines will be replaced with the chip reader models as well. ORR's historical experience with credit/debit card charge backs including those pertaining to fraud has been nominal. There is also negligible risk of financial loss as any fraudulent payment received will be reversed from a debtor's account.

Planned Completion Date: **2).** Within 90 days of receiving procedures from the CTO; 4). 06/30/2018

Contact Information for Implementation: Brenda Jaeger-Das (858) 637-5828

Finding III: eCheck Monitoring and Compliance

OAAS Recommendation: The TTC, ORR, and LUEG should ensure that individuals at each department responsible for monitoring service agreements with the payment service providers obtain the annual ACH Rules Compliance Audit that is required of Third-Party Service Providers by the NACHA Operating Rules and Guidelines Part 8.1, and review to verify compliance.

Action Plan: ORR will obtain and review a copy of the annual audit for compliance with PCI and NACHA guidelines (annually).

Planned Completion Date: Annually upon completion of Compliance Audit

Contact Information for Implementation: Brenda Jaeger-Das (858) 637-5828

Finding IV: Lack of Service Agreement with HPCP/Fiserv

OAAS Recommendation: The CTO, PDS and ORR should ensure that a service agreement between HPE and Fiserv, Inc. is established and signed off by the appropriate parties.

Action Plan: ORR will work with the CTO to ensure that a contract/service agreement is in place between HPE and their subcontractor, Fiserv.

Planned Completion Date: As determined by CTO.

Contact Information for Implementation: Brenda Jaeger-Das (858) 637-5828

If you have any questions, please contact Brenda Jaeger-Das, Manager of the Office of Revenue and Recovery, Fiscal Division at (858) 637-5828.

SEAN S. SANDER, Director
Office of Revenue and Recovery

FIS:BJD:lc

TREASURER-TAX COLLECTOR
COUNTY OF SAN DIEGO

COUNTY ADMINISTRATION CENTER • 1600 PACIFIC HIGHWAY, ROOM 152
SAN DIEGO, CALIFORNIA 92101-2477 • (619) 531-4743 • FAX (619) 446-8222

web site: http://www.sdttc.com

THOMAS PAOLICELLI
Chief Deputy Treasurer

March 30, 2017

TO: Juan R. Perez
Chief of Audits

FROM: Thomas Paolicelli, Chief Deputy Treasurer

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: E-COMMERCE, CREDIT CARD PAYMENTS AUDIT

Finding III: eCheck Monitoring and Compliance

OAAS Recommendation: The TTC, ORR, and LUEG should ensure that individuals at each department responsible to monitoring service agreements with the payment service providers obtain the annual ACH Rules Compliance Audit that is required of third-party service providers by the NACHA Operating Rules and Guidelines Part 8.1, and review to verify compliance.

Action Plan: The Treasurer-Tax Collector (TTC) department agrees with the audit recommendations. Heartland does not share their ACH Rules Compliance Audit. However, they are willing to share their attestation letter. The following steps have been implemented to address the finding:

1. On an annual basis, TTC will request a copy of the contractor's NACHA Operating Rules Compliance Attestation letter and follow-up with them on any significant compliance issues.

Planned Completion Date: Completed. Action plan has been implemented. Contractor provided the NACHA Operating Rules Compliance Attestation dated February 17, 2017.

Contact Information for Implementation: Israel Garza, Manager Treasury Accounting

If you have any questions, please contact me at (619) 531-5686.

Thomas Paolicelli
Chief Deputy Treasurer

TP:dg

Date

TO: Juan Perez
Chief of Audits

FROM: Department Head's Name, Title
Department

QUARTERLY STATUS UPDATE: INSERT TITLE OF THE AUDIT

Pursuant to Board of Supervisors Policy B-44, below is the quarterly status update of outstanding recommendations included in the audit report.

Finding I: Insert Audit's Finding Title

OAAS Recommendation: Insert Audit's Recommendation from the audit report.

Action Plan: Insert the Department's response from the audit report.

Action Plan Update: If your action plan has changed, include why they have changed and describe the alternative actions you are taking. If your action plan has not changed, put NA.

The current status is:

☐ Implemented ☐ In Progress ☐ Pending-Not Started

Original Planned Completion Date: Insert date from audit report

Completion Date Reported Last Quarter: If applicable, insert date from most recent quarterly update status.

Current Planned Completion Date (If different from last quarter, include reason for the change): Insert estimated date of implementation with an explanation if the plan completion date is different from the original planned completion date.

Contact Information for Implementation: Insert Contact Name and Title

If you have any questions, please contact me at phone number (xxx) xxx-xxxx.

Department Head's Name
Title

XX:xx