FIRST FOLLOW-UP AUDIT

INFORMATION TECHNOLOGY AUDIT: TREASURER-TAX COLLECTOR'S CONTROLS OVER COMPLIANCE WITH PCI DSS

ORIGINAL AUDIT NO. 2946

AS OF JUNE 15, 2011

Our First Follow-Up Audit found that the Treasurer-Tax Collector, Auditor-Controller, OC Public Works, CEO/Procurement, and OC Community Resources fully implemented nine (9) recommendations and three (3) recommendations are in process from our original audit report dated October 21, 2010.

AUDIT NO: 1050-A
REPORT DATE: JULY 14, 2011

Director: Dr. Peter Hughes, Ph.D., CPA
Deputy Director: Eli Littner, CPA, CIA
Senior IT Audit Manager: Autumn McKinney, CPA, CIA, CISA
IT Audit Manager: Wilson Crider, CPA, CISA

Independence Objectivity Integrity

OC Internal Audit Department

ORANGE COUNTY BOARD OF SUPERVISORS'

GAO & IIA Peer Review Compliant - 2001, 2004, 2007, 2010

Providing Facts and Perspectives Countywide

RISK BASED AUDITING

Dr. Peter Hughes — **Ph.D., MBA, CPA, CCEP, CITP, CIA, CFE, CFF**
Director
Certified Compliance & Ethics Professional (CCEP)
Certified Information Technology Professional (CITP)
Certified Internal Auditor (CIA)
Certified Fraud Examiner (CFE)
Certified in Financial Forensics (CFF)
E-mail: peter.hughes@iad.ocgov.com

Eli Littner — **CPA, CIA, CFE, CFS, CISA**
Deputy Director
Certified Fraud Specialist (CFS)
Certified Information Systems Auditor (CISA)

Michael Goodwin — **CPA, CIA**
Senior Audit Manager

Alan Marcum — **MBA, CPA, CIA, CFE**
Senior Audit Manager

Autumn McKinney — **CPA, CIA, CISA, CGFM**
Senior Audit Manager
Certified Government Financial Manager (CGFM)

Hall of Finance & Records

12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

Phone: (714) 834-5475 Fax: (714) 834-2880

To access and view audit reports or obtain additional information about the OC Internal Audit Department, visit our website: www.ocgov.com/audit

Orange County's Internal Audit — Fraud Hot-Line — 24/7 Fraud Hotline

OC Fraud Hotline (714) 834-3608

Letter from Dr. Peter Hughes, CPA

Transmittal Letter

Audit No. 1050-A **July 14, 2011**

TO: Shari L. Freidenrich
Treasurer-Tax Collector

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: First Follow-Up Audit: Treasurer-Tax Collector's Controls over Compliance with PCI DSS, Original Audit No. 2946, Issued October 21, 2010

We have completed a First Follow-Up Audit of the Treasurer-Tax Collector's Controls over Compliance with Payment Card Industry Data Security Standard (PCI DSS). Our audit was limited to reviewing, as of June 15, 2011, actions taken to implement the **twelve (12) recommendations** from our original audit. We conducted this First Follow-Up Audit in accordance with the *FY 10-11 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and Board of Supervisors (BOS).

The results of our First Follow-Up Audit are discussed in the **OC Internal Auditor's Report** following this transmittal letter. Our First Follow-Up Audit found the Treasurer-Tax Collector, Auditor-Controller, OC Public Works, CEO/Procurement, and OC Community Resources **fully implemented nine (9) recommendations and three (3) recommendations are in process**.

Each month I submit an **Audit Status Report** to the BOS where I detail any critical and significant control weaknesses released in reports during the prior month and the implementation status of audit recommendations as disclosed by our Follow-Up Audits. Accordingly, the results of this audit will be included in a future status report to the BOS.

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 5.

Table of Contents

First Follow-Up Audit of Information Technology Audit: Treasurer-Tax Collector's Controls over Compliance with PCI DSS Audit No. 1050-A

As of June 15, 2011

OC Internal Auditor's Report

Audit No. 1050-A **July 14, 2011**

TO: Shari L. Freidenrich, Treasurer-Tax Collector

FROM: Dr. Peter Hughes, CPA, Director
Internal Audit Department

SUBJECT: First Follow-Up Audit: Treasurer-Tax Collector's Controls over Compliance with PCI DSS, Original Audit No. 2946, Issued October 21, 2010.

Scope of Review

We have completed a First Follow-Up Audit of the Treasurer-Tax Collector's Controls over Compliance with Payment Card Industry Data Security Standard (PCI DSS). Our audit was limited to reviewing actions taken as of June 15, 2011 to implement the **twelve (12) recommendations** made in our original audit report.

Background

The original audit reviewed the Treasurer-Tax Collector's controls over compliance with payment card industry data security standard. The primary objective of our audit was to:

1. **Determine Whether Treasurer-Tax Collector's Countywide Governance Policies and Procedures (Controls) Ensure Compliance with PCI DSS Validation Requirements:** Review the Treasurer-Tax Collector's Countywide governance policies and procedures regarding payment card processing to determine whether they are adequate to ensure compliance with PCI DSS Validation Requirements.

The secondary audit objectives were to perform the following for a sample of **five (5)** County departments including the Treasurer-Tax Collector:

2. **Determine Whether PCI DSS Validation Documentation Requirements Were Met:** Determine the County's merchant level for each payment card brand accepted by the sample departments. Then based on the merchant level, determine whether the sample departments submitted the appropriate PCI DSS validation documentation to the acquiring banks.

3. **Review County's Third Party Payment Card Processors and Equipment for Compliance:** Determine whether third party payment card processors and equipment used by the sample departments were certified PCI DSS compliant.

4. **Review Third Party Agreements for PCI DSS Compliance:** For the sample departments, review a sample of the third party agreements for payment card processors, operating management agreements, and cashiering systems/applications to determine whether they address PCI DSS compliance.

The original audit identified one (1) **significant issue** and eleven (11) **control findings**.

Results

Our First Follow-Up Audit indicated the Treasurer-Tax Collector, Auditor-Controller, OC Public Works, CEO/Procurement and OC Community Resources **fully implemented nine (9) recommendations and three (3) recommendations are in process.** We believe the remaining **three (3) recommendations** are still appropriate and further efforts should be made to fully implement them. Based on the Follow-Up Audit we conducted, the following is the implementation status of the twelve (12) original recommendations.

1. **No Countywide Governance Policy and Procedure Regarding PCI DSS and the Validation Requirements** **(Significant Issue)**
   Recommendation not required as corrective action has been taken by the Treasurer-Tax Collector to implement a Countywide policy.

   Current Status: **Fully Implemented** at time of original report issuance. Therefore, we consider this recommendation fully implemented.

2. **No Countywide Governance Policy and Procedure Regarding Establishing Bank Accounts** **(Control Finding)**
   We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of bank accounts.

   Current Status: **In Process.** The Treasurer-Tax Collector prepared a draft Countywide policy for the establishment and closure of bank accounts. The draft was completed on January 31, 2011 and is currently undergoing final review. Therefore, we consider this recommendation to be in process.

   Planned Action:
   The Treasurer-Tax Collector will finalize and issue the policy by October 3, 2011.

3. **No Countywide Governance Policy and Procedure Regarding Establishing Merchant Accounts** **(Control Finding)**
   We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of merchant accounts.

   Current Status: **In Process.** The Treasurer-Tax Collector prepared a draft Countywide policy for the establishment and closure of merchant accounts. The draft was completed on January 31, 2011 and is currently undergoing final review. Therefore, we consider this recommendation to be in process.

   Planned Action:
   The Treasurer-Tax Collector will finalize and issue the policy by October 3, 2011.

4. **No Auditor-Controller Policy Regarding Payment Cards/Electronic Payments (Control Finding)**
We recommend that the Auditor-Controller revise Accounting Manual No. C-4 - *Deposits* to address acceptance of payment cards.

Current Status: **In Process.** The Auditor-Controller is currently revising the policy to address acceptance of payment cards. Therefore, we consider this recommendation to be in process.

Planned Action:
The Auditor-Controller will finalize and issue the revised policy by September 30, 2011.

5. **Treasurer-Tax Collector Forms Do Not Address PCI DSS (Control Finding)**
We recommend that the Treasurer-Tax Collector update the Agency Worksheet and Cash Management Checklist for Setting up New Merchant Accounts to address PCI DSS validation requirements.

Current Status: **Fully Implemented.** The Treasurer-Tax Collector updated the Agency Worksheet and Cash Management Checklist for Setting Up New Merchant Accounts on April 19, 2011 to address PCI DSS validation requirements including referencing the County PCI DSS policy. Therefore, we consider this recommendation fully implemented.

6. **Increasing PCI DSS Awareness (Control Finding)**
Recommendation not required as corrective action has been taken by the Treasurer-Tax Collector to increase awareness of PCI DSS.

Current Status: **Fully Implemented** at time of original report issuance. Therefore, we consider this recommendation fully implemented.

7. **Departments Did Not Complete/Submit Self-Assessment Questionnaires to Acquiring Banks (Control Finding)**
We recommend that the Treasurer-Tax Collector annually monitor and verify that each County department accepting payment cards completes and submits the applicable PCI DSS Self Assessment Questionnaire to the acquiring banks.

Current Status: **Fully Implemented.** We reviewed the Treasurer-Tax Collector's monitoring of submissions for the 2010 filing period and noted that all departments submitted their Self Assessment Questionnaire (SAQ) and Attestation of Compliance to the merchant banks as required.

The Treasurer-Tax Collector also updated its Countywide Payment Card Industry Data Security Standards Policy (February 2011) requiring all departments to submit their SAQ and Attestation of Compliance to the Treasurer-Tax Collector for tracking compliance, regardless of the merchant bank, and clarifying that non-Wells Fargo merchants/departments are responsible for submitting their appropriate banks.

Based on the above, we consider this recommendation fully implemented.

8. **Quarterly Network Security Scan for Treasurer-Tax Collector** **(Control Finding)**
We recommend that the Treasurer-Tax Collector determine whether they are considered a level "3" merchant by Wells Fargo and whether they need to begin having quarterly network security scans performed by an Approved Scanning Vendor.

Current Status: **Fully Implemented.** On August 13, 2010, the Treasurer-Tax Collector received confirmation from the Wells Fargo Bank Merchant Service Relationship Manager that a quarterly network security scan is not required. Therefore, we consider this recommendation fully implemented.

9. **T-TC's Cashiering System Terminals/Payment Card Readers Are Not PCI DSS Compliant** **(Control Finding)**
We recommend that the Treasurer-Tax Collector complete its project to replace the current cashiering system and payment card readers/terminals as soon as possible to limit the County's exposure.

Current Status: **Fully Implemented.** We confirmed the Treasurer-Tax Collector's newly implemented cashiering system (J-Point) is Payment Application-Data Security Standard (PA-DSS) certified by reviewing the listing of compliant software maintained by the PCI Security Standards Council. Therefore, we consider this recommendation fully implemented.

10. **County Third Party Agreements Do Not Address PCI DSS Requirements** **(Control Finding)**
We recommend that the County Procurement Office work with County Counsel to develop standard terms and conditions to address PCI DSS and PA DSS compliance for contracts with third party payment processors or for the purchase/lease of payment card equipment and systems/applications.

Current Status: **Fully Implemented.** The CEO/Procurement Office and County Counsel completed the new bid/contract language titled PCI-DSS Compliance during November 2010. The new County Term/Condition (#122) has been distributed to all County departments and is now available on the County Purchasing Intranet Website. Therefore, we consider this recommendation fully implemented.

11. **County Third Party Agreements Do Not Address PCI DSS Requirements** **(Control Finding)**
We recommend that the OCPW/Corporate Real Estate work with County Counsel to develop standard terms and conditions to address PCI DSS and PA DSS compliance in the operating/property management agreements.

Current Status: **Fully Implemented.** OCPW/Corporate Real Estate worked with County Counsel and developed standard terms and conditions that address PCI DSS and PA DSS compliance in the lease/real property agreements. The new terms and conditions are available on the County Intranet (Real Estate Portal). We reviewed the new standard terms and conditions which address PCI DSS and PA DSS compliance. Therefore, we consider this recommendation fully implemented.

12. Third Party Processing Not Clear to User (Control Finding)

We recommend that the Treasurer-Tax Collector, OC Public Works, and OC Community Resources modify their payment acceptance web sites to clearly state that they are being directed to a third party for payment processing.

Current Status: **Fully Implemented.** OC Community Resources modified their payment web site at the time of the original audit report. We verified that the Treasurer-Tax Collector and OC Public Works modified their web payment page to display a notification to the customer that payment processing will be performed by a third party vendor payment processing website. Therefore, we consider this recommendation fully implemented.

We appreciate the assistance extended by the Treasurer-Tax Collector, Auditor-Controller, OC Public Works/Corporate Real Estate, and CEO/Procurement Office during our Follow-Up Audit. If you have any questions, please contact me directly or Eli Littner, Deputy Director at 834-5899, or Autumn McKinney, Senior IT Audit Manager at 834-6106.

Distribution Pursuant to Audit Oversight Committee Procedure No. 1:

Members, Board of Supervisors
Members, Audit Oversight Committee
Thomas G. Mauk, County Executive Officer
Bob Franz, Deputy CEO, Chief Financial Officer
Alisa Drakodaidis, Deputy CEO, OC Infrastructure
Paul Gorman, Chief Assistant Treasurer-Tax Collector
Rosanne De Vera, Assistant Cash Manager, Treasurer-Tax Collector
David E. Sundstrom, Auditor-Controller
Shaun Skelly, Chief Deputy Auditor-Controller
Jan Grimes, Director, Auditor-Controller/Central Accounting Operations
Ronald C. Vienna, County Purchasing Agent, County Procurement Office
Jess Carbajal, Director, OC Public Works
Thomas Mason, Manager, OCPW/Corporate Real Estate
Alicia Campbell, Manager, OCPW/Special Services
Merrie Weinstock, Manager, OCPW/OC Engineering/Flood Control/Green River Golf Course
Foreperson, Grand Jury
Darlene J. Bloom, Clerk of the Board of Supervisors