

Internal Audit Department

O R A N G E C O U N T Y
 6th Largest County in the USA

Information Technology Audit: **TREASURER-TAX COLLECTOR CONTROLS OVER COMPLIANCE WITH PAYMENT CARD INDUSTRY DATA SECURITY STANDARD**

As of December 31, 2009

**Critical
 Impact
 Audit**

**THE COUNTY COLLECTS \$193
 MILLION ANNUALLY THROUGH
 CREDIT/DEBIT CARDS**

We audited the Treasurer-Tax Collector's (T-TC) governance policies/procedures (controls) to ensure Countywide compliance with the Payment Card Industry Data Security Standard (PCI DSS) Validation Requirements. We also selected a sample of five (5) departments to determine whether:

- PCI DSS validation documentation was submitted to the acquiring banks;
- Third party payment card processors and equipment complied with PCI DSS; and
- Third party agreements addressed PCI DSS compliance.

We found that the T-TC did not have a Countywide governance policy/procedure and there was no centralized oversight to ensure departments are submitting PCI DSS compliance validation documents (Self Assessment Questionnaire and Attestation) to the acquiring banks. This is a **Significant Issue**. For 4 of 5 departments reviewed, the departments did not submit the validation documentation to the acquiring banks for calendar year 2008. We were informed the acquiring bank did not specifically request the validation documentation from the County for 2008. Generally for the County's merchant level, compliance is dictated by the acquiring banks.

During our audit the T-TC developed a Countywide policy, which was completed and distributed after the end of our fieldwork. The new policy requires County departments to annually submit the PCI DSS compliance validation documents to the acquiring banks. Additionally, while the T-TC is not responsible for ensuring individual departments comply with PCI DSS, the T-TC has agreed to monitor and verify that each department submits their annual documentation to the acquiring banks. As of 6/30/10, we were informed by the T-TC that all County departments have submitted their validation documentation for calendar year 2009 to the primary acquiring bank (Wells Fargo Bank). As such, we consider this **Significant Issue** to be corrected. We also identified **eleven (11) Control Findings** to enhance existing controls, processes, and systems for payment card processing including the need for the T-TC's credit card readers to become PCI DSS compliant.

AUDIT No: 2946
REPORT DATE: OCTOBER 21, 2010

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

RISK BASED AUDITING

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



American Institute of Certified Public Accountants Award to Dr. Peter Hughes as 2010 Outstanding CPA of the Year for Local Government



2009 Association of Certified Fraud Examiners' Hubbard Award to Dr. Peter Hughes for the Most Outstanding Article - Ethics Pays



2008 Association of Local Government Auditors' Bronze Website Award



2005 Institute of Internal Auditors' Award to IAD for Recognition of Commitment to Professional Excellence, Quality, and Outreach

 ORANGE COUNTY BOARD OF SUPERVISORS'
Internal Audit Department

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**
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



OC Fraud Hotline (714) 834-3608



Transmittal Letter



Audit No. 2946 October 21, 2010

TO: Chriss W. Street
Treasurer-Tax Collector

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

SUBJECT: IT Audit: Treasurer-Tax Collector
Controls over Compliance with Payment
Card Industry Data Security Standard

We have completed an Information Technology Audit of Treasurer-Tax Collector - Controls over Compliance with Payment Card Industry Data Security Standard (PCI DSS). For the 12-month period ended December 31, 2009, County departments/agencies processed over **840,000** payment card transactions totaling approximately **\$193 million** (excluding the Clerk-Recorder). We performed this audit in accordance with our *FY 2009-10 Audit Plan and Risk Assessment* approved by the Audit Oversight Committee and the Board of Supervisors. Our final report is attached for your review.

Please note we have a structured and rigorous **Follow-Up Audit** process in response to recommendations and suggestions made by the Audit Oversight Committee (AOC) and the Board of Supervisors (BOS). As a matter of policy, our **first Follow-Up Audit** will begin at six months from the official release of the report. A copy of all our Follow-Up Audit reports is provided to the BOS as well as to all those individuals indicated on our standard routing distribution list.

The AOC and BOS expect that audit recommendations will typically be implemented within six months and often sooner for significant and higher risk issues. Our **second Follow-Up Audit** will begin at six months from the release of the first Follow-Up Audit report, by which time **all** audit recommendations are expected to be addressed and implemented.

At the request of the AOC, we are to bring to their attention any audit recommendations we find still not implemented or mitigated after the second Follow-Up Audit. The AOC requests that such open issues appear on the agenda at their next scheduled meeting for discussion.

We have attached a **Follow-Up Audit Report Form**. Your department should complete this template as our audit recommendations are implemented. When we perform our first Follow-Up Audit approximately six months from the date of this report, we will need to obtain the completed document to facilitate our review.

Letter from Dr. Peter Hughes, CPA



Each month I submit an **Audit Status Report** to the BOS where I detail any material and significant audit findings 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.

As always, the Internal Audit Department is available to partner with your staff so that they can successfully implement or mitigate difficult audit recommendations. Please feel free to call me should you wish to discuss any aspect of our audit report or recommendations.

Additionally, we will request your department complete a **Customer Survey** of Audit Services. You will receive the survey shortly after the distribution of our final report.

ATTACHMENTS

Other recipients of this report are listed on the **OC Internal Auditor's Report** on page 7.

Table of Contents



*Information Technology Audit:
Treasurer-Tax Collector
Controls over Compliance with
Payment Card Industry Data Security Standard (PCI DSS)
Audit No. 2946*

As of December 31, 2009

Transmittal Letter	i
OC Internal Auditor's Report	
OBJECTIVES	1
RESULTS	2
BACKGROUND	3
SCOPE	6
SCOPE EXCLUSIONS	6
DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT REPONSES	
<u>Audit Objective #1</u> – County PCI DSS Governance	
1. Finding No. – No Countywide Governance Policy and Procedure Regarding PCI DSS and the Validation Requirements (Significant Issue)	8
2. Finding No. 2 – No Countywide Governance Policy and Procedure Regarding Establishing Bank Accounts (Control Finding)	9
3. Finding No. 3 – No Countywide Governance Policy and Procedure Regarding Establishing Merchant Accounts (Control Finding)	9
4. Finding No. 4 – No Auditor-Controller Policy Regarding Payment Cards/Electronic Payments (Control Payment)	10
5. Finding No. 5 – T-TC Forms Do Not Address PCI DSS (Control Finding)	10
6. Finding No. 6 – Increasing PCI DSS Awareness (Control Finding)	11
<u>Audit Objective #2</u> – PCI DSS Validation Requirements	
7. Finding No. 7 – Departments Did Not Complete/Submit Self-Assessment Questionnaires to Acquiring Bank (Control Finding)	12
8. Finding No. 8 – Quarterly Network Security Scan for T-TC (Control Finding)	13
<u>Audit Objective #3</u> – Third Party Processors and Equipment Certified PCI DSS Compliant	
9. Finding No. 9 – T-TC’s Cashiering System Terminals/Payment Card Readers Are Not PCI DSS Compliant (Control Finding)	14
<u>Audit Objective #4</u> – Third Party Agreements	
10. Finding Nos. 10 and 11 – County Third Party Agreements Do Not Address PCI DSS Requirements (Two Control Findings)	15
11. Finding No. 12 – Third Party Processing Not Clear to User (Control Finding)	16

Table of Contents



TABLE OF CONTENTS (Continued)

Information Technology Audit:

Treasurer-Tax Collector

Controls over Compliance with

Payment Card Industry Data Security Standard (PCI DSS)

Audit No. 2946

ATTACHMENT A: Report Item Classifications	18
ATTACHMENT B: PCI Validation Requirements	19
ATTACHMENT C: County Payment Statistics (excludes Clerk-Recorder)	20
ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS	24
ATTACHMENT E: Treasurer-Tax Collector Responses	33
ATTACHMENT F: Auditor-Controller Response	36
ATTACHMENT G: County Procurement Office Response	37
ATTACHMENT H: OC Public Works Responses	38



Audit No. 2946

October 21, 2010

Audit Highlight

We audited the T-TC's governance policies and procedures (controls) to ensure Countywide compliance with Payment Card Industry Data Security Standard (PCI DSS) Validation Requirements. For the 12-month period ended December 31, 2009, County departments processed over **840,000** payment card transactions totaling about **\$193 million** (excluding the Clerk-Recorder).

We found the T-TC did not have a Countywide governance policy/procedure and there was no centralized oversight to ensure departments are submitting PCI DSS validation documentation to the acquiring banks. Generally for the County's merchant level, compliance is dictated by the acquiring banks.

We identified **one (1) Significant Issue** that has been subsequently corrected and **eleven (11) Control Findings** to enhance existing controls, processes and systems for payment card processing.

TO: Chriss Street
Treasurer-Tax Collector

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

SUBJECT: IT Audit: Treasurer-Tax Collector
Controls over Compliance with Payment Card Industry
Data Security Standard

OBJECTIVES

The Internal Audit Department conducted an Information Technology Audit of Treasurer-Tax Collector - Controls over Compliance with Payment Card Industry Data Security Standard (PCI DSS).

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 T-TC'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 T-TC:

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.



RESULTS

We identified **one (1) Significant Issue** that has been subsequently corrected and **eleven (11) Control Findings** resulting in **eleven (11) recommendations** to enhance controls, processes, and systems for payment card processing as discussed in the *Detailed Findings, Recommendations and Management Responses* section of this report. See *Attachment A* for a description of Report Item Classifications. Based upon our audit, we noted:

- **Objective #1 – County PCI DSS Governance:** *Determine whether Treasurer-Tax Collector's Countywide governance policies and procedures (controls) ensure compliance with PCI DSS validation requirements.*
- **Results:** We found that the Treasurer-Tax Collector did not have a Countywide governance policy/procedure and there was no centralized oversight to ensure departments are submitting PCI DSS compliance validation documents to the acquiring banks. This is considered to be a **Significant Issue**. We also identified **five (5) Control Findings** in this area. (See Findings Nos. 1-6).

Status of Significant Issue: The Treasurer-Tax Collector did not have a Countywide governance policy and procedure and there was no centralized oversight to ensure departments are submitting PCI DSS compliance validation documents (Self Assessment Questionnaire and included Attestation of Compliance) to the acquiring banks.

For 4 of 5 departments reviewed, the departments did not submit the validation documentation to the acquiring banks for calendar year 2008. These four (4) departments were considered level "4" merchants in 2008. The County's acquiring bank (Wells Fargo for Visa, MasterCard, and Discover payment cards) published requirements (Fall 2008) for level "4" merchants are: annual completion of the applicable Self-Assessment Questionnaire and included Attestation of Compliance. We were informed by the T-TC that the acquiring banks did not specifically request documentation from the County for 2008. Generally for the County's merchant level, compliance is dictated by the acquiring banks.

During our audit the T-TC was in the process of developing a Countywide policy, which was completed and distributed after the end of our fieldwork. See T-TC's policy in Attachment D. The policy, effective for calendar year 2009, requires County departments to annually submit the PCI DSS compliance validation documents to the acquiring banks. Additionally, while the T-TC is not responsible for ensuring individual departments comply with PCI DSS, the T-TC has agreed to monitor and verify that each department submits their annual documentation to the acquiring banks.

As of 6/30/10, we were informed by the T-TC that all County departments have submitted their PCI DSS validation documentation for the calendar year 2009 to the primary acquiring bank (Wells Fargo Bank). **As such, we consider this Significant Issue to be corrected.**



Secondary Audit Objectives:

➤ **Objective #2 – PCI DSS Validation Requirements:** *For the five (5) sample departments, determine whether PCI DSS validation documentation requirements were met.*

➤ **Results:** For 4 of 5 departments selected, we found that the departments did not submit validation documentation to the acquiring banks for calendar year 2008. However, we were informed by T-TC that the acquiring banks did not specifically request the documentation from the County for 2008. We identified **two (2) Control Findings** in this area. (See Finding Nos. 7-8).

➤ **Objective #3 – Third Party Processors and Equipment Certified PCI DSS Compliant:** *For the five (5) sample departments, determine whether third party payment card processors and equipment were certified PCI DSS compliant.*

➤ **Results:** For 4 of 5 departments selected, we found that the payment card vendors and equipment were certified PCI DSS compliant. However, the T-TC's card readers for their cashiering system were not PCI DSS compliant (1 of 5 departments). We identified **one (1) Control Finding** related to the T-TC's card readers. (See Finding No. 9).

➤ **Objective #4 – Third Party Agreements:** *For the five (5) 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*

➤ **Results:** We found several third party agreements that did not address PCI DSS compliance. We identified **three (3) Control Findings** for third party agreements not addressing PCI DSS compliance. (See Finding Nos. 10-12).

BACKGROUND

The Payment Card Industry Data Security Standard (PCI DSS) is a collaborative effort among several payment card brands (American Express, Discover, JCB, MasterCard, Visa) to achieve a common set of security standards for use by entities that process, store, or transport payment card data.

Each payment card brand has incorporated PCI DSS into technical requirements for compliance. However, each payment card brand has variations in their processes for determining compliance. Compliance is mandated by the individual payment card brands and is enforced by the Merchant Card Processors also known as acquiring banks. PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed or transmitted by the merchant (i.e., County) or third party service provider.

PCI DSS Requirements:

There are 12 requirements:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;



- Protect cardholder data;
- Encrypt transmission of cardholder data across open, public networks;
- Use and regularly update anti-virus software;
- Develop and maintain secure systems and applications;
- Restrict access to cardholder data by business need to know;
- Assign a unique ID to each person with computer access;
- Restrict physical access to cardholder data;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and
- Maintain a policy that addresses information security.

PCI DSS Validation Requirements:

The validation requirements for PCI DSS compliance depend on the merchant level. Merchants are segmented into four (4) levels based on the number and type of transactions processed per year, past compromising incidents, and identification by other payment card brands.

Validation requirements may include:

- (1) Completing and submitting the appropriate Self Assessment Questionnaire (SAQ A, B, C, or D) and included Attestation of Compliance.
- (2) Quarterly network security scanning performed by an Approved Scanning Vendor (ASV) and submitting the results to the acquiring bank.
- (3) Payment card operations audited by Qualified Security Assessor (QSA).

See Attachments B and D for more details on merchant levels, the SAQ validation types, and associated compliance validation requirements.

County Use of Payment Cards and Merchant Account Establishment:

The County departments accept the following payment card brands:

- Master Card, Visa, and Discover via merchant agreement with Wells Fargo Bank (acquiring bank).
- American Express via merchant agreement directly with American Express.

The T-TC manages the relationship with Wells Fargo Bank and American Express on behalf of the County. As such, the T-TC also manages the County's overall PCI DSS program.

Each County department may accept payment cards based on these agreements. For a County department to accept payment cards, they must first establish a merchant account (with separate merchant ID) by completing the Agency Worksheet for Setting up New Merchant Account and forwarding it to the T-TC. The T-TC then establishes a merchant account with Wells Fargo Bank or American Express on behalf of the department. The T-TC utilizes a Cash Management Checklist for Setting Up New Merchant Accounts to ensure the account is established properly.

The T-TC also offers general guidance to departments for accepting payment cards. This includes operating a terminal, the importance of using fraud prevention tools including the Card Verification Value (CVV) number and address verification, minimizing chargebacks, and the costs associated with accepting payment cards.



Countywide Payment Card Activity:

For the year ended December 31, 2009, the County accepted over **840,000** debit/credit card payments totaling approximately **\$193 million**. This does not include Superior Court activity or Clerk-Recorder activity. See Attachment C for details of County department payment card transactions.

“Card not present” transactions (online/phone transactions) accounted for approximately 17% of the transactions totaling \$148 million (mainly from T-TC operations). “Card not present” transactions have a lower transaction volume threshold when determining merchant level, resulting in greater PCI DSS compliance requirements.

Treasurer-Tax Collector Payment Card Activity:

The T-TC collects property tax payments in person (card reader) and via phone and the internet (card not present). Of the total \$193 million payments processed by County departments, the T-TC processed **15% of the transactions** totaling \$151 million or **79% of the total dollars**. All T-TC payment card transactions are processed by a third party payment processor (Official Payments Corporation).

County's Acquiring Bank Requirements:

Compliance with PCI DSS is mandated by the individual card brands and enforced by the acquiring banks.

- **Wells Fargo Bank (Visa, MasterCard, and Discover):** The County departments are considered level “4” merchants. Wells Fargo’s published requirements (Fall 2008) for level “4” merchants are: annual completion of applicable Self-Assessment Questionnaire and included Attestation of Compliance. Wells Fargo also strongly recommends quarterly network security scans by an Approved Scanning Vendor.
- **American Express:** Except for JWA, the County departments are considered level “3” merchants. According to the T-TC, American Express does not require level “3” merchants to submit the applicable Self-Assessment Questionnaire (SAQ) and included Attestation of Compliance annually. American Express does strongly recommend quarterly network security scans by an Approved Scanning Vendor.

JWA is considered a level “2” merchant for American Express. American Express requires level “2” merchants to submit: the applicable Annual Self-Assessment Questionnaire (SAQ), quarterly network security scans by an Approved Scanning Vendor, and annual signed “Attestation of Report Accuracy.” Based upon their credit card processing environment/configuration, JWA has sought and obtained annual waivers from American Express.

Cost of Non-Compliance:

The following information was obtained from the “PCI DSS Compliance Closing the Loop” Whitepaper written by the Open Text Connectivity Solutions Group 2009:

There are a number of costs associated with being non-compliant with PCI DSS. First, the organization would be exposed to fines and penalties. Since the beginning of 2009, Visa has started levying monthly fines of \$25,000 to non-compliant US merchants and \$5,000 to their Acquirers. Merchants may also have their merchant level changed to level 1 requiring annual audits and quarterly network security scans and their associated costs. In addition, payment card processing privileges may be terminated.



In addition to non-compliance fines, the PCI DSS allows the various payment card brands to fine a merchant for non-compliance with PCI for each incident. The fines can amount to \$500,000 per incident per card brand per compromise type (PCI includes both the PCI DSS and the PCI PIN requirements).

There are also indirect costs associated with a security breach of about \$90 to \$305 per record, such as costs of investigation, notification, response, and restitution.

SCOPE

Our audit was to determine whether the Countywide controls over compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements were sufficient as of December 31, 2009. Our scope included the following elements:

- We reviewed the T-TC governance policies and procedures (controls) to ensure Countywide compliance with the PCI DSS Validation Requirements.
- We also selected a sample of five (5) departments to determine whether:
 - PCI DSS validation documentation was submitted to the acquiring banks;
 - Third party payment card processors and equipment complied with PCI DSS; and
 - Third party agreements addressed PCI DSS.

Departments were selected based on either volume of payment card activity or “card not present” transactions. As a result, we selected the following five (5) departments:

1. Treasurer-Tax Collector
2. John Wayne Airport
3. OCCR/OC Animal Care
4. OCCR/OC Public Library
5. OC Public Works – only for GeoData Retrieval system and Green River Golf Course (under a management/operating agreement with OC Flood Control District.)

SCOPE EXCLUSIONS

Our audit did not include validating whether the County met individual PCI DSS requirements. Our audit did not include the other County departments not selected for review.

Management's Responsibilities for Internal Controls

In accordance with the Auditor-Controller's County Accounting Manual section S-2 - *Internal Control Systems*, “All County departments/agencies shall maintain effective internal control systems as an integral part of their management practices. This is because management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls. Control systems shall be continuously evaluated and weaknesses, when detected, must be promptly corrected.” The criteria for evaluating an entity's internal control structure is the Committee of Sponsoring Organizations (COSO) control framework. Our Internal Control Audit enhances and complements, but does not substitute for the Treasurer-Tax Collector's and the five sampled departments' continuing emphasis on control activities and self-assessment of control risks.



Inherent Limitations in Any System of Internal Control

Because of inherent limitations in any system of internal controls, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the Treasurer-Tax Collector's and the five sampled departments' controls, operating procedures, and compliance with payment card industry requirements.

Acknowledgement

We appreciate the courtesy extended to us by Treasurer-Tax Collector and the selected departments. If we can be of further assistance, please contact me directly; or Eli Littner, Deputy Director at 834-5899; or Autumn McKinney, Senior Audit Manager at 834-6106.

Attachments

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
Kim Hansen, Cash Manager, 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
Nicholas Chrisos, County Counsel
Satish Ajmani, Chief Information Officer
Tony Lucich, County Information Security Officer, CEO/Information Technology
Ronald C. Vienna, County Purchasing Agent, County Procurement Office
Alan L. Murphy, Director, John Wayne Airport
Steve Siemion, Deputy Airport Director, JWA/Finance and Administration
Lisa Kawashima, Manager, JWA/Accounting
Scott Suzuki, Manager, JWA/Quality Assurance & Compliance
Steve Franks, Director, OC Community Resources
Ryan Drabek, Director, OCCR/OC Animal Care
Kristine Watson, Chief of Customer Service, OCCR/OC Animal Care
Helen Fried, County Librarian, OCCR/OC Public Library
James Martin, Manager, OCCR/OC Public Library/Fiscal and Purchasing Services
Dave Sankey, Manager, OCCR/Budget and Financial Services
Clyde Gamboa, Manager, OCCR/Information Technology
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



Audit Objective #1 – County PCI DSS Governance

Our objective was to determine whether the Treasurer-Tax Collector's (T-TC) Countywide policies and procedures (controls) ensure compliance with PCI DSS validation requirements. Policies and procedures should address acceptance and processing of payment cards, establishment of merchant accounts, and monitoring departments' compliance with validation requirements.

Process and Control Strengths

Process and control strengths noted during the audit include:

- ✓ T-TC Provides Guidance to County Departments for Payment Card Processing: The T-TC offers general guidance for accepting payment cards. This includes operating a terminal, the importance of using fraud prevention tools including the CVV number and address verification, minimizing chargebacks, and the costs associated with accepting payment cards.
- ✓ Standardized Forms Used for Account Establishment: The T-TC establishes the merchant accounts for County departments based on their completion of a Standard Worksheet and Checklist.

The following are areas where processes and controls can be enhanced:

1. **Finding No. 1 – No Countywide Governance Policy and Procedure Regarding PCI DSS and the Validation Requirements (Significant Issue)**

The Treasurer-Tax Collector did not have a Countywide governance policy and procedure for PCI DSS. There was no centralized oversight to ensure County departments are submitting PCI DSS compliance validation documents (Self Assessment Questionnaire and included Attestation of Compliance) to the acquiring banks.

For 4 of 5 departments reviewed, the departments did not submit the validation documentation to the acquiring banks for calendar year 2008. We were informed the acquiring banks did not specifically request the validation documentation from the County for calendar year 2008 (except in one instance for JWA who obtained a waiver from American Express). Generally for the County's merchant level, compliance is dictated by the acquiring banks.

During our audit the T-TC was in the process of developing a Countywide policy, which was completed and distributed after the end of our fieldwork. The policy requires County departments to annually submit the PCI DSS compliance validation documents to the acquiring banks by April 30th, effective for calendar year 2009. Additionally, while the T-TC is not responsible for ensuring individual departments compliance with PCI DSS, the T-TC has agreed to monitor and verify that each department submits their annual documentation to the acquiring banks. As of June 30, 2010, we were informed by the T-TC that all County departments have submitted their validation documentation for calendar year 2009 to the primary acquiring bank (Wells Fargo Bank). **As such, we consider this Significant Issue to be corrected by the T-TC and no recommendation is needed.**

Recommendation No. 1: Not required as corrective action has been taken by the Treasurer-Tax Collector to implement a Countywide policy. See policy in Attachment D to this report.

Treasurer-Tax Collector Response: Not required.



2. Finding No. 2 – No Countywide Governance Policy and Procedure Regarding Establishing Bank Accounts (Control Finding)

The Treasurer-Tax Collector does not have a Countywide policy or formalized procedures for the establishment of bank accounts including the requirement that all County departments must open bank accounts through the T-TC.

Additionally, departments may not be aware that establishing Pay Pal accounts may be considered banking relationships. Without Countywide policy and guidance from the T-TC, a department could establish accounts outside the control of the County (e.g., Pay Pal accounts linked to personal bank accounts) exposing the County to loss of funds or fines and penalties if a breach were to occur. A risk is that Pay Pal accounts allow for debit cards to be issued for withdrawing monies.

Recommendation No. 2:

We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of bank accounts.

Treasurer-Tax Collector Response:

Concur. Treasurer-Tax Collector management will develop and distribute a Countywide governance policy for the establishment of bank accounts by January 31, 2011.

3. Finding No. 3 – No Countywide Governance Policy and Procedure Regarding Establishing Merchant Accounts (Control Finding)

The Treasurer-Tax Collector does not have a Countywide policy or formalized procedures for establishing merchant accounts. We were informed by the T-TC that departments can establish their own merchant accounts and are not required to go through the T-TC.

The T-TC has a merchant agreement with Wells Fargo Bank (for Visa, Master Card, and Discover) and the majority of departments utilize Wells Fargo Bank as their merchant bank (acquiring bank) for those payment cards. However, there are some exceptions:

- OCPW/Green River Golf Course: We were informed they were unable to utilize the Wells Fargo merchant agreement (because the industry specific software associated with their Point of Sale system was not certified by Wells Fargo Bank) and therefore, established a merchant agreement with Elavon – Electronic Transaction Systems. The T-TC informed us that it did verify that Green River Golf Course submitted their calendar year 2009 PCI DSS compliance validation documentation to the acquiring bank.
- Clerk-Recorder: We were informed the Clerk-Recorder has established a merchant agreement with an entity other than Wells Fargo. We did not audit the Clerk-Recorder as part of this audit. However, we were informed by the T-TC that it did not verify whether the Clerk-Recorder submitted their calendar year 2009 PCI DSS compliance validation documentation to the acquiring bank. The T-TC indicated they are willing to monitor submission of the annual compliance documentation once provided with details regarding the Clerk-Recorder's merchant agreement/acquiring bank.



The T-TC should develop a policy or formalized procedures for the establishment of merchant accounts including the requirement that County departments notify the T-TC when establishing a merchant account (acquiring bank) with someone other than Wells Fargo. This will allow the T-TC to monitor the departmental submissions of annual PCI DSS compliance validation documentation to the other acquiring banks.

Recommendation No. 3:

We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of merchant accounts.

Treasurer-Tax Collector Response:

Concur. Treasurer-Tax Collector management will develop and distribute a Countywide governance policy for the establishment of merchant accounts by January 31, 2011.

4. Finding No. 4 – No Auditor-Controller Policy Regarding Payment Cards/Electronic Payments (Control Finding)

The Auditor-Controller Accounting Manual No. C-4 - *Deposits* does not address payment cards/electronic payments. The policy was revised in 2001 (before PCI DSS) and only addresses cash and checks. The Auditor-Controller should have documented policies and procedures for accepting and handling electronic/payment card transactions including ensuring staff are adequately trained on the requirements. The policy should include a requirement that County departments must follow the T-TC's new policy for PCI DSS compliance and the validation requirements. Without appropriate policies, these transactions may not be processed properly exposing the County to liability and loss of funds.

Recommendation No. 4

We recommend that the Auditor-Controller revise Accounting Manual No. C-4 - *Deposits* to address acceptance of payment cards.

Auditor-Controller Response:

We concur with the Internal Audit Department's Recommendation No. 4. The Auditor-Controller Accounting Manual No. C-4 – *Deposits* will be updated by October 15, 2010 to address payment/electronic cards.

5. Finding No. 5 – T-TC Forms Do Not Address PCI DSS (Control Finding)

The T-TC uses two standardized forms when establishing merchant accounts for County departments:

- Agency Worksheet for Setting up New Merchant Account - completed by County Departments.
- Cash Management Checklist for Setting Up New Merchant Accounts - completed by the T-TC.



These forms do not address PCI DSS compliance. The Agency Worksheet should include reference to PCI DSS requirements so the departments are aware of the requirements prior to establishing the account. The Cash Management Checklist should include steps to require the applicable Self Assessment Questionnaire (SAQ) be completed by the County department; this will help ensure the department is fully aware of the responsibilities and will be able to comply with the PCI DSS requirements.

Recommendation No. 5

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.

Treasurer-Tax Collector Response:

Concur. Both worksheets have been updated. When supplying potential new merchants with the Agency Worksheet, the TTC will also provide the Orange County Payment Card Industry Data Security Standard policy, a document on Getting Started and a cover letter.

6. Finding No. 6 – Increasing PCI DSS Awareness (Control Finding)

Quarterly, the T-TC receives payment card acceptance information from Wells Fargo Bank. This information is currently not being forwarded to the County departments that accept payment cards. By forwarding this information, it would raise awareness of PCI DSS requirements for County departments as well as promote compliance with the standard. In addition, the Wells Fargo newsletters may include information about additional services (some are no charge to the County) for complying with PCI DSS.

After our fieldwork was completed, the T-TC implemented procedures to periodically distribute information relating to PCI DSS, including the Wells Fargo newsletters, to the County departments. The T-TC provided an example of an informational email sent to the County departments on May 24, 2010. **As such, we consider this Control Finding to be corrected by the T-TC and no recommendation is needed.**

Recommendation No. 6: Not required as correction action has been taken.

Treasurer-Tax Collector Response: Not required.

Audit Objective #2 – PCI DSS Validation Requirements

Our objective for the five (5) selected departments was to determine whether the County met PCI DSS validation requirements. Our audit included determining the County's merchant level for each card brand accepted and verifying the validation requirements were met.



Process and Control Strengths

Process and control strengths noted during the audit include:

- ✓ T-TC Provides Guidance to County Departments for Payment Card Processing: The T-TC offers general guidance for accepting payment cards. This includes operating a terminal, the importance of using fraud prevention tools including the CVV number and address verification, minimizing chargebacks, and the costs associated with accepting payment cards.

The following are areas where processes and controls can be enhanced:

7. Finding No. 7 – Departments Did Not Complete/Submit Self-Assessment Questionnaires to Acquiring Bank (Control Finding)

Completion of the Self-Assessment Questionnaire (SAQ) is required to certify PCI DSS compliance. Non-compliance may result in fines or penalties including the revocation of payment card acceptance.

For calendar year 2008:

- Three of the five sampled departments (T-TC, OC Animal Care, and OCPW specifically for Geodata and Green River Golf Course) did not complete the applicable PCI DSS Self Assessment Questionnaire.
- One of the five sampled departments (OC Public Library) completed the applicable PCI DSS Self Assessment Questionnaire, but did not submit it to the acquiring bank.
- One of the five sampled departments (JWA) did not complete the applicable PCI DSS Self Assessment Questionnaire (SAQ). As noted below, JWA indicated the acquiring banks did not request the PCI DSS SAQ from JWA for 2008. Additionally, as JWA does not process payment card transactions through the County's data network or any internet service provider, JWA sought and received annual waivers from American Express for the quarterly network scanning and PCI DSS SAQ requirements.

Compliance with PCI DSS is enforced by the acquiring banks. According to the T-TC, the acquiring banks did not specifically request documentation from the County for calendar year 2008.

For calendar year 2009, the T-TC's new policy requires the County departments to complete and submit the PCI DSS Self Assessment Questionnaire to the acquiring banks.

Recommendation No. 7

We recommend that the T-TC 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.



Treasurer-Tax Collector Response:

Concur. The Orange County Payment Card Industry Data Security Standard policy has been amended to require the TTC to monitor and verify submissions to Wells Fargo Bank and all other acquiring banks. Below is the updated statement from the policy.

****Important Note:**

For locations that use Wells Fargo Bank as their merchant bank - SAQ's and an Attestation of Compliance must be submitted to Wells Fargo Merchant Services at the address below by April 30th of each year.

For locations that use a merchant bank other than Wells Fargo Bank - SAQ's and an Attestation of Compliance must be submitted to the Cash Management Division of the Orange County Treasurer's Office by April 30th of each year.

Compliance will be verified and monitored by the Treasurer's Office. Failure to comply could result in the closure of your merchant account.

8. Finding No. 8 – Quarterly Network Security Scan for T-TC (Control Finding)

For level "4" merchants, Wells Fargo strongly recommends quarterly network security assessments. For levels "1" through "3" merchants, Wells Fargo requires quarterly network security scans performed by an Approved Scanning Vendor (ASV).

For calendar year 2009, the T-TC processed 20,597 web (e-commerce) Visa payment card transactions. The threshold for Merchant level "3" for Visa and MasterCard transactions is 20,000 to 1,000,000 e-commerce transactions. As such, the T-TC may be considered a level "3" merchant. If so, Wells Fargo (acquiring bank) may require the T-TC to have quarterly network security scans performed by an Approved Scanning Vendor.

On April 2, 2010, we attended a meeting with T-TC and CEO/Information Technology (CEO/IT) staff. The T-TC initiated the meeting to determine whether they could utilize an existing Request For Proposal (RFP) that CEO/IT was preparing for security assessment vendors. The T-TC and CEO/IT also planned to research whether other County departments may be interested in participating in quarterly network security scans.

Recommendation No. 8

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.

Treasurer-Tax Collector Response:

Concur. TTC has received confirmation from Wells Fargo Bank that they are not required to have a quarterly network security scan. The only requirement is completing Self Assessment Questionnaire A – for merchants with no electronic storage, processing, or transmission of Cardholder Data on an annual basis.



Audit Objective #3 – Third Party Processors and Equipment Certified PCI DSS Compliant

Our objective for the five (5) selected departments was to determine whether third party payment card processors and equipment were certified PCI DSS compliant.

Process and Control Strengths

Process and control strengths noted during the audit include:

- ✓ Third Party Compliance: Payment card payment processors used by the selected County departments were certified PCI DSS compliant by MasterCard/Visa.
- ✓ Equipment Compliance: Payment card readers used by the selected County departments were certified PCI DSS compliant by MasterCard/Visa, except for the T-TC's payment card readers/cashiering system terminals.

The following are areas where processes and controls can be enhanced:

9. Finding No. 9 – T-TC's Cashiering System Terminals/Payment Card Readers Are Not PCI DSS Compliant (Control Finding)

The T-TC informed us that its cashiering system terminals/payment card readers were not PCI DSS compliant. The T-TC was aware of this issue prior to our audit and issued a Request for Proposal on April 15, 2009. The winning bidder was Salepoint. They plan to replace their cashiering system terminals/payment card readers by September 2010. The T-TC should be PCI DSS compliant to prevent exposure to fines/penalties from payment card brands, negative publicity, and civil penalties.

Recommendation No. 9

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.

Treasurer-Tax Collector Response:

Concur. The new cashiering system installation went live on September 14, 2010.

Audit Objective #4 – Third Party Agreements

Our objective for the five (5) selected departments was to 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 following is where processes and controls could be improved to enhance payment card processing and PCI DSS compliance:



10. Finding Nos. 10 and 11 – County Third Party Agreements Do Not Address PCI DSS Requirements (Two Control Findings)

We reviewed a sample of the third party agreements as listed below:

Third Party Payment Card Vendors:

- Authorize.NET – used by T-TC and OC Animal Care
- Pay Pal, Inc. – used by OCPW/Geodata and OC Public Library

Information System Agreements:

- Sirsi (point of sale cashiering system) and Envisionware (e-commerce gateway) – used by OC Public Library

Operating/Property Management Agreements:

- OCPW/Green River Golf Course
- JWA/Parking Concepts, Inc.

The above contracts/agreements did not mention or address PCI DSS compliance. Some of these contracts/agreements are older (before PCI DSS). However, some contracts/agreements were developed more recently (2008 and 2009).

Currently, the County does not have standard/approved contract language available to the County departments addressing PCI DSS or Payment Application (PA) DSS in these types of third party agreements. Effective July 1, 2010, Visa requires all payment applications to be PA DSS certified.

JWA recently included language similar to the below in its recent draft Request For Proposal for a new parking lot/cashiering system application:

- The vendor provided payment application must be tested and approved by the PCI SSC (Security Standards Council) for new deployments.
- The vendor-provided payment application must be validated by a PA QSA (Payment Application Qualified Security Assessor) recognized by the PCI SSC.
- The vendor's application software shall conform to PCI DSS.
- PCI DSS and/or PA DSS certification shall be included in the proposer's bid response.

Third party agreements should address PCI DSS compliance to ensure the County is performing its due diligence as well as limit the County's exposure to fines/penalties from payment card brands, negative publicity, and civil penalties. There should be standard contract language developed and made available to the County departments.

For the operating/property management agreements, consideration should be given to PCI DSS and PA DSS compliance that is reasonably under the control of the operator versus under the control of the County.

**Recommendation No. 10:**

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.

County Procurement Office Response:

Concur. The CEO/Procurement Office is meeting with County Counsel to develop these standard terms and conditions. This process will be completed by October 31, 2010.

Recommendation No. 11:

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.

OC Public Works Response:

We concur; Corporate Real Estate will work with County Counsel to develop standard terms and conditions. The estimated date of completion is December 6, 2010.

11. Finding No. 12 – Third Party Processing Not Clear to User (Control Finding)

We reviewed the County's payment card websites for:

- Treasurer-Tax Collector - Property Tax website
- OC Public Works - Geodata Retrieval system
- OCCR/OC Animal Care - Chameleon system
- OCCR/OC Library - Sirsi system

We noted that it is not clear to the public that the user is being redirected to a third party for transaction processing. As a matter of transparency, the public should be made aware of who is processing their transaction. By alerting the public of the third party (such as a pop-up window), the County may limit its exposure in the event of a security breach.

Recommendation No. 12

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.

Treasurer-Tax Collector Response:

Concur. The Treasurer-Tax Collector web site has been modified with the statement below. It appears on each page where a tax payer has the opportunity to make a payment.

Clicking "Pay by Checking/Savings Account" or "Pay by Credit Card" will take you to a third party vendor payment processing website.



OC Public Works Response:

We concur; this recommendation has been implemented and is now operational.

OC Community Resources Response:

Not required. See auditor note below.

Internal Audit Note:

During the draft report process, OCCR updated its online payment card applications (Chameleon and Sirsi) to notify users that their payments are being processed by a third party. We validated that adequate corrective action was taken. **As such, we consider this recommendation for OCCR to be implemented. No further action is required for OCCR.**



ATTACHMENT A: Report Item Classifications

For purposes of reporting our audit observations and recommendations, we will classify audit report items into three distinct categories:

Material Weaknesses:

Audit findings or a combination of Significant Issues that can result in financial liability and exposure to a department/agency and/or to the County as a whole. Management is expected to address "Material Weaknesses" brought to their attention immediately.

Significant Issues:

Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of processes or internal controls. Significant Issues will generally require management's prompt corrective actions.

Control Findings:

Audit findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process of six months, but no later than twelve months.

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT B: PCI Validation Requirements

PCI Level	Visa, MasterCard and Discover Network	American Express	PCI DSS Compliance Validation Requirements
1	<ul style="list-style-type: none"> Over 6 million Visa or MasterCard transactions per year Businesses that experienced a data compromise Businesses meeting the Level 1 criteria of another payment card brand 	<ul style="list-style-type: none"> Over 2.5 million American Express transactions per year Businesses that experienced a data compromise 	<ul style="list-style-type: none"> Annual onsite review by a Qualified Security Assessor Quarterly network security scan by an Approved Scanning Vendor Annual submission of a compliant "PCI Report On Compliance" Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only
2	<ul style="list-style-type: none"> 1 million to 6 million Visa or MasterCard transactions per year Businesses meeting the Level 2 criteria of another payment card brand 	<ul style="list-style-type: none"> 50,000 to 2.5 million American Express transactions per year 	<ul style="list-style-type: none"> Annual Self Assessment Questionnaire must be submitted to Wells Fargo Merchant Services Quarterly network security scan by an Approved Scanning Vendor Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only Annual signed "Attestation of Report Accuracy"
3	<ul style="list-style-type: none"> 20,000 to 1 million e-commerce Visa or MasterCard transactions per year Businesses meeting the Level 3 criteria of another payment card brand. 	<ul style="list-style-type: none"> All other businesses 	<ul style="list-style-type: none"> Annual Self Assessment Questionnaire must be submitted to Wells Fargo Merchant Services Quarterly network security scan by an Approved Scanning Vendor Annual signed "Attestation of Report Accuracy"
4	<ul style="list-style-type: none"> All other businesses 	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> Annual Self Assessment Questionnaire Quarterly network security scan by an Approved Scanning Vendor strongly recommended

Source: Wells Fargo Merchant Intelligence Bulletin - Fall 2008

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT C: County Payment Statistics (excludes Clerk-Recorder)

January 1 -
December 31, 2009

MID	Location	Card Type	# of Transactions	Sales
226015002992	HCA - EMS	MasterCard	822	\$ 31,774.08
		Visa	1,397	\$ 54,004.00
		American Express	25	\$ 1,037.00
		Discover	9	\$ 345.00
226015003990	HCA - ENVIRONMENTAL HEALTH	MasterCard	317	\$ 162,554.87
		Visa	577	\$ 280,629.06
226015108997	HCA - EH/ACCOUNTING	MasterCard	282	\$ 220,969.55
		Visa	497	\$ 362,871.86
		American Express	357	\$ 220,621.74
		Discover	34	\$ 18,775.90
226015004998	HCA - 17th STREET	MasterCard	1,282	\$ 141,653.25
		Visa	1,998	\$ 213,183.50
		American Express	594	\$ 76,947.75
		Discover	133	\$ 12,888.00
226015005995	ANIMAL CARE SERVICES	MasterCard	6,043	\$ 626,369.68
		Visa	8,956	\$ 968,824.74
		American Express	1,282	\$ 152,293.37
		Discover	441	\$ 49,762.42
226210816998	ANIMAL CARE SRV WEB LICN <i>online</i>	MasterCard	3,125	\$ 138,638.00
		Visa	4,357	\$ 192,940.93
		American Express	808	\$ 32,857.50
		Discover	298	\$ 12,563.00
226015006993	OC CEMETERY DISTRICT ANAHEIM CEMETERY EL TORO MEMORIAL PARK SANTA ANA CEMETERY	MasterCard	200	\$ 295,367.81
		Visa	262	\$ 460,853.20
		Discover	29	\$ 46,537.70
226015010995	REGISTRAR OF VOTERS	MasterCard	18	\$ 7,132.85
		Visa	34	\$ 12,496.61
226015010995	CNG SALES	MasterCard	-	\$ -
		Visa	-	\$ -
226015021992	VINTAGE MARINA	MasterCard	1,153	\$ 175,833.81
		Visa	1,764	\$ 260,408.81
		American Express	533	\$ 108,255.86
		Discover	45	\$ 6,778.63
226015023998	DANA POINT MARINA INN	MasterCard	2,801	\$ 614,830.50
		Visa	5,268	\$ 1,224,981.07

Source: Treasurer-Tax Collector

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT C: County Payment Statistics (continued)

January 1 -
December 31, 2009

MID	Location	Card Type	# of Transactions	Sales
226015024996	EAST BASIN MARINA	MasterCard	1,026	\$ 251,353.49
		Visa	1,402	\$ 307,258.39
		American Express	3	\$ 974.00
226015127997	DANA WEST MARINA	MasterCard	35	\$ 16,784.68
		Visa	43	\$ 23,239.15
226015167993	DANA POINT PARKING	MasterCard	3,583	\$ 11,492.00
		Visa	6,352	\$ 20,522.05
481160140994	OC PUBLIC WORKS	MasterCard	849	\$ 428,506.16
		Visa	1,280	\$ 696,964.80
		American Express	704	\$ 605,532.14
481201745991	OCPW - GEODATA <i>online</i>	MasterCard	1,203	\$ 15,015.95
		Visa	2,284	\$ 26,481.40
008010156951	GREEN RIVER	MasterCard	12,767	\$ 623,956.75
		Visa	21,209	\$ 1,048,528.91
		American Express	5,536	\$ 304,371.43
226015165997	OC CIVIC CENTER PARKING	n/a	-	\$ -
226015153993	JWA <i>parking lot - PCI</i>	MasterCard	123,850	\$ 6,796,950.51
		Visa	193,326	\$ 10,460,086.88
		American Express	200,660	\$ 11,220,494.88
		Discover	5,342	\$ 300,125.08
226015155998	OC PUBLIC LIBRARY <i>online</i>	MasterCard	5,239	\$ 64,827.85
		Visa	7,470	\$ 94,578.17
		American Express	917	\$ 13,053.09
		Discover	189	\$ 2,545.22
226108900995	ORANGE COUNTY COLLECTION	MasterCard	364	\$ 91,825.89
		Visa	586	\$ 144,553.73
		Discover	22	\$ 4,919.05
226015164990	UNITED WAY GOLF	MasterCard	7	\$ 171.00
		Visa	13	\$ 1,220.00
226015166995	OC PARKS-PARKING	MasterCard	24,011	\$ 77,461.00
		Visa	43,886	\$ 142,114.25
		American Express	14	\$ 44.00

Source: Treasurer-Tax Collector

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT C: County Payment Statistics (continued)

January 1 -
December 31, 2009

MID	Location	Card Type	# of Transactions	Sales
226015172993	OC PARKS-PERMITS	n/a	-	\$ -
226015173991	OC DIST ATTORNEY WJ	MasterCard	62	\$ 3,869.20
		Visa	102	\$ 7,001.20
		Discover	7	\$ 525.00
226015174999	OC DIST ATTORNEY NJ	MasterCard	127	\$ 8,943.07
		Visa	267	\$ 19,400.97
		American Express	14	\$ 975.77
		Discover	10	\$ 750.00
226015175996	OC DIST ATTORNEY CJ	MasterCard	98	\$ 6,118.04
		Visa	195	\$ 13,096.08
		American Express	17	\$ 925.13
		Discover	3	\$ 225.00
226015176994	OC DIST ATTORNEY HJ	MasterCard	99	\$ 6,679.35
		ATM	2	\$ 150.00
		Visa	165	\$ 11,354.86
		Discover	3	\$ 225.00
226015177992	OC DIST ATTN Y RECEPTION	MasterCard	29	\$ 1,474.37
		Visa	51	\$ 2,790.04
		American Express	9	\$ 723.91
226015169999	PROBATION DEPT	MasterCard	1,063	\$ 129,474.65
		Visa	1,605	\$ 184,627.88
226015170997	PROBATION DEPT FEES <i>Fees to Official Payments</i>	MasterCard	1,063	\$ 5,315.00
		Visa	1,605	\$ 8,025.00
226015185995	OC PUBLIC LAW LIBRARY	n/a	-	\$ -
481200224998	OC TAX COLLECTOR - Web <i>Web</i>	MasterCard	13,205	\$ 31,066,406.99
		Visa	20,597	\$ 43,026,063.27
		American Express	12,490	\$ 40,632,577.94
		Discover	2,105	\$ 4,402,278.39
481206349997	OC TAX COLLECTOR - Web Fees <i>Web - Fees to Official Payments</i>	MasterCard	13,205	\$ 776,622.24
		Visa	20,597	\$ 1,075,654.51
		American Express	12,490	\$ 1,015,816.53
		Discover	2,105	\$ 110,057.16
226015110993	OC TAX COLLECTOR - IVR <i>IVR</i>	MasterCard	3,772	\$ 7,111,021.65
		Visa	5,523	\$ 9,886,930.57
		American Express	2,474	\$ 6,706,549.14

Source: Treasurer-Tax Collector

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT C: County Payment Statistics (continued)

January 1 -
December 31, 2009

MID	Location	Card Type	# of Transactions	Sales
		Discover	553	\$ 968,599.89
481160141992	OC TAX COLLECTOR - IVR FEES <i>IVR - Fees to Official Payments</i>	MasterCard	3,772	\$ 177,776.18
		Visa	5,523	\$ 247,174.20
		American Express	2,474	\$ 167,664.17
		Discover	553	\$ 24,215.19
226015162994	OC TAX CASHIERING	MasterCard	648	\$ 1,220,835.58
		Visa	922	\$ 1,508,478.17
		Discover	199	\$ 449,481.86
		American Express	242	\$ 525,473.83
226015163992	OC TAX CASHIERING FEES <i>Fees to Official Payments</i>	MasterCard	648	\$ 30,521.05
		Visa	922	\$ 37,712.24
		Discover	199	\$ 11,237.07
		American Express	242	\$ 13,156.96
County Totals			841,969	\$ 192,586,908.25
T-TC			125,460	\$ 151,192,304.78
			15%	79%
Online (including OC Tax Web and IVR)			147,328	147,988,909
			17%	77%

Source: Treasurer-Tax Collector



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS



OFFICE OF THE TREASURER-TAX COLLECTOR

HALL OF FINANCE & RECORDS
11 CIVIC CENTER PLAZA, SUITE G76
POST OFFICE BOX 4515
SANTA ANA, CA 92702
www.ttc.ocgov.com

CHRIS W. STREET
TREASURER-TAX COLLECTOR
PAUL C. GORMAN, CPA., CFP
CHIEF ASSISTANT TREASURER-TAX COLLECTOR
JENNIFER BURKHART, CPA
ASSISTANT TREASURER-TAX COLLECTOR
ROBIN RUSSELL
ASSISTANT TREASURER-TAX COLLECTOR
ADMINISTRATOR

January 19, 2010

Action Required: PCI DSS Compliance Validation Policy

Please review the attached policy regarding compliance with the Payment Card Industry Data Security Standard (PCI DSS). This policy applies to all agencies within the County of Orange that process credit card transactions (merchants). **Each location that accepts credit cards must complete the PCI DSS Validation Requirements by April 30 of each year beginning this year, 2010.**

To provide a brief background, PCI DSS requires merchants and third party vendors who store or transmit cardholder data on behalf of the merchant to adhere to PCI DSS. These standards are intended to assist in fraud prevention by protecting cardholder data. Failure to comply with PCI Data Security Standards can result in losing the ability to process card payments. Card associations may also impose hefty fines as a result of non-compliance or breach in cardholder information. Failure to comply with these standards may also result in a violation of federal or state law.

Attached to this email are the following documents:

- ❖ PCI Compliance Policy – contains the County policy, provides a background on PCI DSS as well as links to various resources to further explain PCI DSS and provide all the tools necessary to complete the validation.
- ❖ Getting Started – use this document as a guide to begin validating PCI DSS.
- ❖ Location Data – provides each location's transaction volume by card type for calendar year 2009. In addition, the Treasurer's office has made an attempt to determine the appropriate PCI level and which Self Assessment Questionnaire (SAQ) each location must complete; **however, this is based on the assumption that no cardholder data is being stored as well as our knowledge of each location's transaction types. Each location must evaluate their processing methods. It is the responsibility of each location to ultimately determine the correct SAQ to complete.**

While PCI DSS compliance is the responsibility of each merchant, the overall program is managed by the County Treasurer. For questions regarding this policy or for further information and documentation, please feel free to contact me. Thank you.

Sincerely,

Rosanne De Vera
Assistant Cash Manager
Treasurer Tax Collector
email rdevera@ttc.ocgov.com
phone 714-834-4170 | fax 714-834-2192



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

County of Orange Payment Card Industry Data Security Standards Policy

I. Policy

This policy is not intended to replace Payment Card Industry Data Security Standards (PCI DSS). Agencies that accept credit card transactions should use this as a guide to ensure compliance with PCI DSS. Revisions to the PCI DSS could occur at any time. The next revision of PCI DSS is expected to be effective September 2010. For the latest in PCI DSS information please visit the PCI website at: www.pcisecuritystandards.org.

A. Overview

In order to protect cardholder information and maintain compliance with the Payment Card Industry Data Security Standards (PCI DSS), any agency (merchant) within the County of Orange (County) that processes credit card transactions must comply with PCI Data Security Standards by completing the PCI DSS Compliance Validation Requirements. On an annual basis, around January or February, merchants should review credit card transaction activity for the previous calendar year. PCI DSS Compliance Validation Requirements must be completed by April 30 of each year based on the activity from the previous year.

The PCI Security Standards Council (PCI SSC) (founded by the five major card associations: Visa, MasterCard, American Express, Discover, JCB) established a set of rules that require merchants and third party vendors who store or transmit cardholder data on behalf of the merchant to adhere to PCI Data Security Standards. These standards are intended to assist in fraud prevention by protecting cardholder data.

Failure to comply with PCI Data Security Standards can result in losing the ability to process card payments. Card associations may also impose hefty fines as a result of non-compliance or breach in cardholder information. Failure to comply with these standards may also result in a violation of federal or state law.

Included in this document, you will find a glossary and links to various resources to further explain PCI DSS. While PCI DSS compliance is the responsibility of each merchant, the overall program is managed by the County Treasurer. Please contact the Treasurer's Cash Management division for further information and documentation, if needed.

B. The PCI Data Security Standards

There are twelve fundamental requirements that make up the core of PCI Data Security Standards. Not all requirements apply to every merchant. For locations that use stand-alone dial-up terminals with no cardholder data being transmitted to internal systems or via the Internet, the top five requirements are: 3, 4, 7, 9, and 12 – listed below. For all other locations such as those that handle card-not-present transactions, have payment application systems connected to the Internet, store any portion of cardholder data electronically, or use wireless local area networks (WLAN) each requirement must be met.

Build and Maintain a Secure Network

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



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
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

II. PCI Compliance Validation Requirements

A. PCI Levels

Merchants are classified into one of the four PCI DSS levels based on card transaction volume over a 12-month period. Each level has defined compliance requirements. There are two compliance guidelines – one for MasterCard and Visa transactions and one for American Express transactions. For MasterCard and Visa transactions, use the highest volume of the two to determine your PCI DSS level. The table below will help to determine your PCI level and what the validation requirements are for that level.

Please note: For the County of Orange, PCI DSS compliance requirements are determined at the location level. Each location within the County of Orange that accepts credit cards is responsible for their own PCI DSS compliance. If you have questions regarding your PCI DSS level, please contact the Cash Management division of the Treasurer's Office. If you have questions regarding PCI DSS compliance, please contact our Wells Fargo Merchant Services representative, Katie Woodall at (301) 745-7002 or you may email her at Katie.Woodall@WellsFargoMerchantServicesLLC.com.

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

PCI Level	Visa and MasterCard	American Express	PCI DSS Compliance Validation Requirements
1	<ul style="list-style-type: none"> Over 6 million Visa or MasterCard transactions per year Businesses that experienced a data compromise Businesses meeting the Level 1 criteria of another payment card brand 	<ul style="list-style-type: none"> Over 2.5 million American Express transactions per year Businesses that experienced a data compromise 	<ul style="list-style-type: none"> Annual onsite review by a qualified Security Assessor Quarterly network security scan by an Approved Scanning Vendor Annual submission of a compliant "PCI Report On Compliance" Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only
2	<ul style="list-style-type: none"> 1 million to 6 million Visa or MasterCard transactions per year Businesses meeting the Level 2 criteria of another payment card brand 	<ul style="list-style-type: none"> 50,000 to 2.5 million American Express transactions per year 	<ul style="list-style-type: none"> Annual Self Assessment Questionnaire Quarterly network security scan by an Approved Scanning Vendor Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only Annual signed "Attestation of Report Accuracy"
3	<ul style="list-style-type: none"> 20,000 to 1 million e-commerce Visa or MasterCard transactions per year 	<ul style="list-style-type: none"> N/A 	<ul style="list-style-type: none"> Annual Self Assessment Questionnaire Quarterly network security scan by an Approved Scanning Vendor Annual signed "Attestation of Report Accuracy"
4	<ul style="list-style-type: none"> All other businesses 	<ul style="list-style-type: none"> All other businesses This is considered Level 3 for American Express but compares to V/MC Level 4 requirements 	<ul style="list-style-type: none"> Annual Self Assessment Questionnaire Quarterly network security scan by an Approved Scanning Vendor strongly recommended



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

B. Self Assessment Questionnaires (SAQ)

The SAQ is a document intended to assist merchants in self-evaluating their compliance with the PCI DSS. There are five SAQ validation categories, shown briefly in the table below and described in more detail in the Self Assessment Questionnaire Instruction Guide. Use the table to gauge which SAQ applies to your location, then review the detailed descriptions to ensure you meet all the requirements for that SAQ. Current copies of each SAQ as well as the Instruction Guide are available on the PCI SSC Website: https://www.pcisecuritystandards.org/saq/instructions_dss.shtml

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. <i>This would never apply to face-to-face merchants</i>	A
2	Imprint-only merchants with no cardholder data storage	U
3	Stand-alone dial-up terminal merchants, no cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no cardholder data storage	C
5	All other merchants (not included in descriptions for SAQs A-C above) and all service providers defined by a payment brand as eligible to complete an SAQ	D

****Important Note: SAQ's and an Attestation of Compliance must be submitted to Wells Fargo Merchant Services at the address below by April 30th of each year. Compliance will be verified and monitored by the Treasurer's Office. Failure to comply could result in the closure of your merchant account.**

Wells Fargo Merchant Services
Attention: Katie Woodal
P.O. Box 6600
Hagerstown, MD 21740

C. Approved Scanning Vendors (ASV)

Depending on your PCI DSS level, quarterly network security scans may be required by an ASV. ASVs are organizations that validate adherence to certain PCI DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers. A list of ASVs certified by PCI SSC can be found at: https://www.pcisecuritystandards.org/pdfs/asv_report.html

To assist in measuring your data security risk and to help you start the process of validating your PCI DSS compliance, Wells Fargo has made arrangements to have access to Trustwave's Risk Profiler at no additional cost. To do so please visit www.wellsfargo.riskprofiler.net and click on "Start Risk Profiler" and enter enrollment code: PCIWELLS

III. Third Party Processors

It is the merchant's responsibility to ensure that all applications hosted and/or furnished by a third party processor that receives or processes cardholder data to accept credit card payments comply with PCI Data Security Standards. Contracts with third party processors should require that the vendor be PCI compliant for the entire duration of the contract. In addition, you should request a certificate of compliance annually from your third party processor.



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

IV. Software - Payment Application Data Security Standards (PA-DSS)

The PA-DSS certification is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI Security Standards Council. Validated applications are listed at:

www.pcisecuritystandards.org/security_standards/pa_dss.shtml.

There are fourteen requirements to protecting Payment Application transactions:

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data
2. Provide secure password features
3. Protect stored cardholder data
4. Log application activity
5. Develop secure applications
6. Protect wireless transmission
7. Test applications to address vulnerabilities
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote software updates
11. Facilitate secure remote access to applications
12. Encrypt sensitive traffic over public networks
13. Encrypt all non-console administrative access
14. Maintain instructional documentation and training programs for customers, resellers, and integrators

*Note: California state law requires that cardholder expiration dates be masked on **both** the merchant and customer receipts. This is not a PCI DSS requirement; however, it is equally important (California Civil Code § 1747.09).

V. Hardware – Payment Card Devices

Any device used to swipe cards must encrypt the data at the point of capture.

Any pin pad device must comply with the PCI personal identification number (PIN) entry device (PED) security requirements. (PCI PED)

VI. Resources

For current information regarding PCI DSS, please visit the **PCI Security Standards Council's website at:**

<https://www.pcisecuritystandards.org/>

For current version of a **PCI Quick Reference Guide**, please visit the link below:

https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

For current version of the **Self Assessment Questionnaires (SAQ) Instructions and Guidelines** document and the **Navigating PCI DSS** document, please visit the link below:

https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#navigating

For current versions of the **SAQ** documents, please visit the link below:

https://www.pcisecuritystandards.org/saq/instructions_dss.shtml

For current versions of the **Prioritized Approach to Pursue PCI DSS Compliance** and the associated **Release Notes and Instructions**, please visit the link below:

<https://www.pcisecuritystandards.org/education/prioritized.shtml>



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

For current list of **Approved Scanning Vendors (ASV)**, please visit the link below:

https://www.pcisecuritystandards.org/gsa_asv/find_one.shtml

For current list of **Payment Application Data Security Standards (PA DSS)** certified vendors, please visit the link below:

https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Additional Resources:

Visa Business Guide to Data Security

https://usa.visa.com/merchants/risk_management/data_security_demo/popup.html

MasterCard PCI 360

<http://www.ijan.ibeam.com/events/mast001/24008/>

Wells Fargo Bank – Merchant Compliance

<https://www.wellsfargo.com/biz/merchant/service/manage/risk/security>



ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS (continued)

VII. Glossary

Application – Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications

Cardholder – Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Cardholder Data – At a minimum, cardholder data contains the full primary account number (PAN) or full magnetic stripe data. Cardholder data may also appear in the form of the full primary account number plus any of the following:

- Cardholder name
- Expiration date
- Service Code

Card Validation Code or Value – Refers to either: (1) magnetic-stripe data or (2) printed security features:

(1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV or CSC pending on payment card brand. The following list provides the terms for each card brand:

- **CAV** – Card Authentication Value (JCB payment cards)
- **CVC** – Card Validation Code (MasterCard payment cards)
- **CVV** – Card Verification Value (Visa and Discover payment cards)
- **CSC** – Card Security Code (American Express)

(2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit un-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following provides an overview:

- **CID** – Card Identification Number (American Express and Discover payment cards)
- **CAV2** – Card Authentication Value 2 (JCB payment cards)
- **CVC2** – Card Validation Code 2 (MasterCard payment cards)
- **CVV2** – Card Verification Value 2 (Visa payment cards)

Headquarter – a parent number assigned to one or more merchant IDs as a way to group similar operating locations.

Location – Refers to each County of Orange agency that processes card transactions assigned with their own unique headquarter.

Magnetic-Stripe Data – Also referred to as "track data". Data encoded in the magnetic stripe or chip used for authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.

Masking – Method of concealing a segment of data when displayed. Masking is used when there is no business requirement to view the entire PAN.

Merchant – any location that processes credit card payments.

Merchant Identification (MID) – A number assigned to each merchant identifying each merchant.




ATTACHMENT D: Treasurer-Tax Collector Policy for Orange County PCI DSS
(continued)

PAN – Acronym for "primary account number" and also referred to as "account number." The PAN is the account number printed on the front of a payment card.



ATTACHMENT E: Treasurer-Tax Collector Responses



OFFICE OF THE TREASURER-TAX COLLECTOR

HALL OF FINANCE & RECORDS
11 CIVIC CENTER PLAZA, SUITE G76
POST OFFICE BOX 4515
SANTA ANA, CA 92702
www.ttc.ocgov.com

October 8, 2010

CHRISS W. STREET
TREASURER-TAX COLLECTOR

PAUL C. GORMAN, C.P.A., C.T.P., CPEM
CHIEF ASSISTANT TREASURER-TAX COLLECTOR

JENNIFER BURKHART, CFA
ASSISTANT TREASURER-TAX COLLECTOR

ROBIN RUSSELL
ASSISTANT TREASURER-TAX COLLECTOR
ADMINISTRATION

Dr. Peter Hughes
Director, Internal Audit
County of Orange
12 Civic Center Plaza, Room 232
Santa Ana, CA 92701

RECEIVED
INTERNAL AUDIT DEPARTMENT
OCT 12 PM 2:22

Dear Dr Hughes:

Pursuant to Audit Oversight Committee Administrative Procedure No. 1, we have prepared our response to the Draft Report on Treasurer-Tax Collector Controls over Compliance with Payment Card Industry Data Security Standard Validation Requirements as of December 31, 2009. The recommendation numbers used in your report reference our response.

Recommendation No. 2:
We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of bank accounts.

Treasurer-Tax Collector Management Response:
Concur. Treasurer-Tax Collector management will develop and distribute a Countywide governance policy for the establishment of bank accounts by January 31, 2011.

Recommendation No. 3:
We recommend that the Treasurer-Tax Collector develop and distribute a Countywide governance policy for the establishment of merchant accounts.

Treasurer-Tax Collector Management Response:
Concur. Treasurer-Tax Collector management will develop and distribute a Countywide governance policy for the establishment of merchant accounts by January 31, 2011.

Recommendation No. 5
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.

Treasurer-Tax Collector Management Response:
Concur. Both worksheets have been updated. When supplying potential new merchants with the Agency Worksheet, the TTC will also provide the Orange County Payment Card Industry Data Security Standard policy, a document on Getting Started and a cover letter.

Page 1 of 3



ATTACHMENT E: Treasurer-Tax Collector Responses (continued)

Dr. Peter Hughes
October 8, 2010

Recommendation No. 7

We recommend that the T-TC 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.

Treasurer-Tax Collector Management Response:

Concur. The Orange County Payment Card Industry Data Security Standard policy has been amended to require the TTC to monitor and verify submissions to Wells Fargo Bank and all other acquiring banks. Below is the updated statement from the policy.

****Important Note:**

For locations that use Wells Fargo Bank as their merchant bank - SAQ's and an Attestation of Compliance must be submitted to Wells Fargo Merchant Services at the address below by April 30th of each year.

For locations that use a merchant bank other than Wells Fargo Bank - SAQ's and an Attestation of Compliance must be submitted to the Cash Management Division of the Orange County Treasurer's Office by April 30th of each year.

Compliance will be verified and monitored by the Treasurer's Office. Failure to comply could result in the closure of your merchant account.

Recommendation No. 8

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.

Treasurer-Tax Collector Management Response:

Concur. TTC has received confirmation from Wells Fargo Bank that they are not required to have a quarterly network security scan. The only requirement is completing Self Assessment Questionnaire A – for merchants with no electronic storage, processing, or transmission of Cardholder Data on an annual basis.

Recommendation No. 9

We recommend that the Treasurer-Tax Collector complete its project to replace the current cashing system and payment card readers/terminals as soon as possible to limit the County's exposure.

Treasurer-Tax Collector Management Response:

Concur. The new cashing system installation went live on September 14, 2010.

Recommendation No. 12

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.



ATTACHMENT E: Treasurer-Tax Collector Responses (continued)

Dr. Peter Hughes
October 8, 2010

Treasurer-Tax Collector Management Response:

Concur. The Treasurer-Tax Collector web site has been modified with the statement below. It appears on each page where a tax payer has the opportunity to make a payment.

Clicking "Pay by Checking/Savings Account" or "Pay by Credit Card" will take you to a third party vendor payment processing website.

If you have additional questions or follow-up comments; please contact me at 834-2288.

Very truly yours,

A handwritten signature in cursive script that reads "Paul C. Gorman".

Paul C. Gorman
Chief Assistant Treasurer-Tax Collector

DETAILED FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES



ATTACHMENT F: Auditor-Controller Response



DAVID E. SUNDSTROM, CPA
AUDITOR-CONTROLLER

AUDITOR-CONTROLLER COUNTY OF ORANGE

HALL OF FINANCE AND RECORDS
12 CIVIC CENTER PLAZA, ROOM 200
POST OFFICE BOX 567
SANTA ANA, CALIFORNIA 92702-0567
(714) 834-2450 FAX: (714) 834-2569
www.ac.ocgov.com

RECEIVED
INTERNAL AUDIT DEPARTMENT

2010 OCT 13 AM 10:41

SHAUN M. SKELLY
CHIEF DEPUTY
AUDITOR-CONTROLLER

JAN E. GRIMES
DIRECTOR
CENTRAL ACCOUNTING OPERATIONS

WILLIAM A. CASTRO
DIRECTOR
SATELLITE ACCOUNTING OPERATIONS

PHILLIP T. DAIGNEAU
DIRECTOR
INFORMATION TECHNOLOGY

October 5, 2010

TO: Peter Hughes Director
Internal Audit Department

SUBJECT: Response to IT Audit: Treasurer-Tax Collector Controls over
Compliance with Payment Card Industry Data Security Standards

The following is our response to the recommendation contained in the IT Audit: Treasurer-Tax Collector Controls over Compliance with Payment Card Industry Data Security Standards, Audit No. 2946.

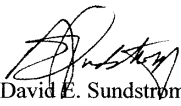
Recommendation No. 4

We recommend that the Auditor-Controller revise Accounting Manual No. C-4 *Deposits* to address acceptance of payment cards.

Auditor-Controller Response:

We concur with the Internal Audit Department's Recommendation No. 4. The Auditor-Controller Accounting Manual No. C-4 – *Deposits* will be updated by October 15, 2010 to address payment/electronic cards.

Thank you for the opportunity to respond to the draft report. Please contact Jan Grimes at 834-2470 if you have any questions on our response.


David E. Sundstrom
Auditor-Controller

/lr

cc: Autumn McKinney, Senior IT Audit Manager, Internal Audit Department
Shaun Skelly, Chief Deputy Auditor-Controller
Jan Grimes, Director, Auditor-Controller Central Accounting Operations




ATTACHMENT G: County Procurement Office Response



County Executive Office
Memorandum

September 01, 2010

To: Dr. Peter Hughes, Director, Internal Audit Department
From: Ronald C. Vienna, County Purchasing Agent 
Subject: Response to Draft Audit Report 2946

This memorandum provides my response to item 10 of the Draft Audit Report #2946.

Recommendation No. 10:

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.

County Procurement Office Response:

Concur. The CEO/Procurement Office is meeting with County Counsel to develop these standard terms and conditions. This process will be completed by October 31, 2010.

If you have any questions in regards to this information, please contact Ron Vienna at (714) 834-6889 or via email at ron.vienna@ocgov.com.

cc: Robert J. Franz, Chief Financial Officer

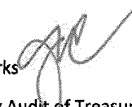


ATTACHMENT H: OC Public Works Responses



Jess A. Carbajal, Director
300 N. Flower Street
Santa Ana, CA
P.O. Box 4048
Santa Ana, CA 92702-4048
Telephone: (714) 854-2300
Fax: (714) 834-5158

Memorandum

DATE: August 31, 2010
TO: Peter Hughes, Ph.D., CPA, Director
Internal Audit Department
FROM: Jess A. Carbajal, Director, OC Public Works 
SUBJECT: Draft Report on Information Technology Audit of Treasurer-Tax Collector, Audit 2946

I am pleased to provide OC Public Works' response to the Internal Audit Department's Draft Report on the Information Technology Audit of Treasurer-Tax Collector – Controls over Payment Card Industry Data Security Standard. Our responses to recommendations No. 11 and 12 have been reviewed and approved by the County Executive Office.

Recommendation No. 11:

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.

OC Public Works Response:

We concur; Corporate Real Estate will work with County Counsel to develop standard terms and conditions. The estimated date of completion is December 6, 2010.

Recommendation No. 12:

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.

OC Public Works Response:

We concur; this recommendation has been implemented and is now operational.

Should you have any questions regarding OC Public Works' responses to the Internal Audit Department's recommendations, or require additional information on these items, please contact Larry Stansifer, Manager, OC Public Works/Administrative Services at (714) 834-3051.

Attachment

c: Alisa Drakodaidis, Deputy CEO, OC Infrastructure
Carlos Bustamante, Director, OC Public Works/Administrative Services
Mary Fitzgerald, Manager, OC Public Works/Administrative Services/Accounting Services
Bill Castro, Director, Auditor-Controller Satellite Accounting Operations
Tony Bernard, Manager, OC Public Works/ Administrative Services/Purchasing
Eli Littner, Deputy Director, Internal Audit Department
Mike Goodwin, Sr. Audit Manager, Internal Audit Department
Fred Neroni, Manager, OC Public Works/Administrative Services/Information Technology Services
Joseph Edwards, Manager, OC Public Works/OC Facilities and Real Estate
Tom Mason, Manager, OC Public Works/OC Facilities and Real Estate/Corporate Real Estate