



*July 13, 2011*

**To:** Finance and Administration Committee  
**From:** Will Kempton, Chief Executive Officer  
**Subject:** Review of Payment Card Industry Data Security Standards Compliance

**Overview**

The Internal Audit Department of the Orange County Transportation Authority has completed a review of Payment Card Industry Data Security Standard Compliance. The review found that the Orange County Transportation Authority has not fully complied with Payment Card Industry Data Security Standard requirements and provided three recommendations. Management indicated that the recommendations will be implemented.

**Recommendation**

Direct staff to implement recommendations in the Review of Payment Card Industry Data Security Standards Compliance, Internal Audit Report No. 11-507. Recommendations included completion of the required annual self assessment questionnaire and related action plans, documentation of quarterly vulnerability scans, and creation of centralized accountability for compliance, which encompasses the operations of both the Orange County Transportation Authority and the 91 Express Lanes operations.

**Background**

The Orange County Transportation Authority (OCTA) Fiscal Year 2010-11 Internal Audit Department Internal Audit Plan included a review of Payment Card Industry (PCI) Data Security Standards (DSS) Compliance.

The PCI DSS is an information security standard defined by the PCI DSS Council, an independent counsel formed by American Express, Discover Financial Services, Japan Credit Bureau International, MasterCard Worldwide, and Visa Inc. The PCI DSS was created to help organizations that accept and process card payments to prevent fraud by specifying the framework for a secure payments environment.

Any organization that collects, processes, stores, or transmits credit card information is required to be in compliance with PCI DSS. Merchants and service providers not fully compliant with PCI DSS must document detailed action plans to remediate weaknesses and become compliant. While all merchants are expected to comply with the PCI DSS, merchants at defined transaction volumes have additional requirements for documenting compliance.

OCTA accepts credit cards as part of the 91 Express Lanes operations and customer service operations. The total volume of transactions is approximately 730,000 annually with toll road operations representing approximately 700,000 per year and customer service department transactions totaling approximately 30,000 per year.

### ***Discussion***

The Internal Audit Department (Internal Audit) found that OCTA has not complied with PCI DSS requirements for completion and attestation of an annual self assessment questionnaire (SAQ) and related action plans. The SAQ is used by merchants to self-identify their level of compliance with PCI DSS and to document plans for remediation of areas found to be non-compliant. Internal Audit found that separate SAQs for OCTA and 91 Express Lanes operations have been partially completed but have not been compiled, attested to, or submitted annually as required. Further, there was no evidence that action plans to address self-identified areas of non-compliance were developed and implemented. Internal Audit recommended management implement procedures to ensure an annual SAQ and related action plans are completed, attested to, and submitted as required. Management agreed to implement procedures as recommended.

Internal Audit found that, while management maintained evidence that vulnerability scans were performed as requested by American Express, there was no evidence that the scans were performed on a quarterly basis, as required by PCI DSS. Internal Audit recommended that management conduct these scans quarterly and retain documentation to evidence results of the scans and any remediation plans for areas of failure. Management indicated that actions have been taken to ensure documentation of quarterly scans and related action plans is retained in accordance with requirements.

Finally, Internal Audit recommended that responsibility and authority for compliance with PCI DSS be centralized in order to coordinate compliance and reporting. Management agreed and has designated OCTA's Chief Information Officer as the party to oversee compliance reporting for both OCTA and the 91 Express Lanes.

***Summary***

Based on this review, Internal Audit offered three recommendations and management indicated that the recommendations will be implemented.

***Attachment***

- A. Review of Payment Card Industry Data Security Standards Compliance, Internal Audit Report No. 11-507

**Approved by:**



Janet Sutter  
Executive Director, Internal Audit  
714-560-5591

# Orange County Transportation Authority Internal Audit Department



## Review of Payment Card Industry Data Security Standards Compliance

INTERNAL AUDIT REPORT NO. 11-507

July 6, 2011



**Internal Audit Team:**

Janet Sutter, CIA, Executive Director, Internal Audit  
Gerald Dunning, CIA, CISA, CFE, Senior Internal Auditor

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

<b>CONCLUSION .....</b>	<b>1</b>
<b>BACKGROUND .....</b>	<b>1</b>
<b>Objectives, Scope, and Methodology .....</b>	<b>2</b>
<b>Audit Comments, Recommendations and Management Responses .....</b>	<b>4</b>
Non Compliance with Requirements for Annual Self Assessment and Related Action Plans..	4
OCTA Lacked Evidence that Vulnerability Scans are Performed on a Quarterly Basis.....	4
OCTA Lacks Centralized Responsibility and Authority for PCI DSS Compliance .....	5

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

**CONCLUSION**

The Internal Audit Department (Internal Audit) of the Orange County Transportation Authority (OCTA) has completed a review of Payment Card Industry (PCI) Data Security Standard (DSS) Compliance. The purpose of the review was to determine the adequacy of controls in place to ensure that OCTA is in compliance with the PCI DSS compliance requirements.

Based on the review, OCTA has not fully complied with PCI DSS requirements for attestation and submission of an annual self assessment questionnaire (SAQ) and action plan. OCTA could not provide evidence that action plans have been developed and implemented for those areas where SAQ's indicated non-compliance with PCI DSS. OCTA also lacked evidence that vulnerability scans are performed on a quarterly basis. Weaknesses in compliance and related documentation have resulted in part from a lack of centralized accountability for compliance, which encompasses the operations of both OCTA customer service and the 91 Express Lanes.

**BACKGROUND**

The Orange County Transportation Authority Fiscal Year 2010-11 Internal Audit Department Internal Audit Plan included a review of PCI DSS Compliance.

The PCI DSS is an information security standard defined by the PCI DSS Council, an independent counsel formed by American Express, Discover Financial Services, Japan Credit Bureau International, MasterCard Worldwide, and Visa Inc. The PCI DSS was created to help organizations that accept and process card payments to prevent fraud by specifying the framework for a secure payments environment.

Any organization that collects, processes, stores, or transmits credit card information is required to be in compliance with PCI DSS. Merchants and service providers not fully compliant with PCI DSS must document detailed action plans to remediate weaknesses and become compliant. While all merchants are expected to comply with PCI DSS, merchants at defined transaction volumes have additional requirements for documenting compliance.

OCTA accepts credit cards as part of 91 Express Lanes operations and customer service operations. The total volume of transactions is approximately 730,000 annually with 91 Express Lanes operations representing approximately 700,000 per year and customer service department transactions totaling approximately 30,000 per year. As such, OCTA is classified in the merchant level 2 category by American Express. This classification requires that OCTA conduct and submit an annual self-assessment questionnaire and attestation as well as quarterly vulnerability scans. OCTA must also provide a remediation plan (action plan) to address any areas of non-compliance identified in the self-assessment or the vulnerability scans.

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

The DSS is divided into six main sections and 12 subject areas.

- Build and Maintain a Secure Network  
Requirement 1: Install and maintain a firewall configuration to protect data.  
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect Cardholder Data  
Requirement 3: Protect stored cardholder data.  
Requirement 4: Encrypt transmission of cardholder data across open, public networks.
- Maintain a Vulnerability Management Program  
Requirement 5: Use and regularly update antivirus software.  
Requirement 6: Develop and maintain secure systems and applications.
- Implement Strong Access Control Measures  
Requirement 7: Restrict access to cardholder data by business need to know.  
Requirement 8: Assign a unique ID to each person with computer access.  
Requirement 9: Restrict physical access to cardholder data.
- Regularly Monitor and Test Networks  
Requirement 10: Track and monitor all access to network resources and cardholder data.  
Requirement 11: Regularly test security systems and processes.
- Maintain a Policy That Addresses Information Security  
Requirement 12: Maintain a policy that addresses information security.

According to staff, American Express is the only card brand that has contacted OCTA requesting submission of the required compliance validation and quarterly vulnerability scans. The first request was sent to Cofiroute USA, LLC in February 2009.

## **Objectives, Scope, and Methodology**

The objective of this review was to determine whether OCTA has policies and procedures in place to ensure compliance with PCI DSS requirements. The scope of the review included the policies and procedures that were in place as of December 31, 2010. The review methodology included, but was not limited to, the following:

- Review of PCI DSS at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- Review of OCTA related Data Security Policies & Procedures
- Review of Telvent, OCTA-91 Express Lanes PCI Credit Card Data Flow and Data Protection Documentation, version 1.1 August 28, 2009, for the 91 Express Lanes
- Review of Agreement No. C-9-0201 between OCTA and Bank of America for credit card clearinghouse services

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

- Review of Agreement No. C-5-0300 and Amendments 1 through 5 between OCTA and Cofiroute USA, LLC. for management and operational services for the 91 Express Lanes
- Review of Agreement No. C-8-1379 between OCTA and Sirit Corporation for hardware, software, and other services required to upgrade the 91 Express Lanes Electronic Toll and Traffic Management System
- Review Purchase Order A17591 between OCTA and Telvent to provide maintenance and support of the 91 Express Lanes Tollpro back office software system
- Review PCI DSS requirements of American Express, Discover Financial Services, MasterCard Worldwide, and Visa, Inc.
- Review of Draft OCTA PCI DSS Self Assessment,
- Interview of OCTA Senior Security Analyst, OCTA General Manager for Toll Roads, OCTA IS Project Manager for Toll Roads, and OCTA Senior External Affairs Administrator for Pass Sales

This review was conducted in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions based on audit objectives. Internal Audit believes that the evidence obtained provides a reasonable basis for our findings and conclusions.

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

## **Audit Comments, Recommendations and Management Responses**

### **Non-Compliance with Requirements for Annual Self Assessment and Related Action Plans**

OCTA has not fully complied with PCI DSS requirements for completion and attestation of an annual Self Assessment Questionnaire (SAQ) of equipment, systems, and networks. The purpose of the SAQ is to assist organizations in self-evaluating compliance with the PCI DSS. Separate SAQ's have been partially completed by OCTA staff, Cofiroute USA, LLC staff, and Telvant staff for various systems, equipment, and networks; but a single SAQ for all OCTA transactions is not prepared.

In addition, where a SAQ indicates areas of non-compliance with the PCI DSS, OCTA is required to complete action plans indicating management's plans to remediate the issue and the date of expected completion; not to exceed twelve months from the date of the action plan. None of the SAQ's include signed attestations or are submitted as required. In addition, OCTA could not provide evidence that action plans have been developed and implemented for those areas where SAQ's indicated non-compliance with PCI DSS minimum security requirements.

**Recommendation 1:** Internal Audit recommends management implement procedures to ensure an annual SAQ for all OCTA transactions is prepared and related action plans are developed, attested to, and submitted as required. Further, management should ensure documentation is on file to evidence action plans have been developed and implemented when required.

**Management Response:** Management concurs with the recommendations to implement procedures for ensuring SAQ's and related action plans are completed, attested to, and submitted as required. The procedures will outline, document, and serve as evidence of the action plans and implemented controls.

A review of the most recent SAQ's will be conducted to identify and document items that require further action or remediation. Action plans will be developed and retained in an up to date log/repository to be maintained and managed by OCTA's Senior Information Systems Security Analyst.

### **OCTA Lacked Evidence that Vulnerability Scans are Performed on a Quarterly Basis**

According to PCI DSS, OCTA is required to perform quarterly network vulnerability scans; however, OCTA did not maintain evidence that these scans are performed on a quarterly basis.

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

While there is evidence that scans are performed and submitted when requested by American Express, it appears the requests are not received quarterly and OCTA Information Systems personnel have not maintained documentation to evidence that scans have performed on a quarterly basis.

**Recommendation 2:** Internal Audit recommends management implement procedures to ensure vulnerability scans are performed on a quarterly basis and documentation of results and any required remediation efforts is retained.

**Management Response:** Management will modify the existing quarterly vulnerability scan procedures to ensure results of vulnerability scans and any required remediation efforts are documented and maintained.

The vulnerability scans are performed by a certified vendor (McAfee) on a quarterly basis. Information Systems Security has locked the most recent and subsequent scan results for a two year retention schedule from the date of generation, in accordance with PCI requirements.

**OCTA Lacks Centralized Responsibility and Authority for PCI DSS Compliance**

OCTA lacks a centralized function with authority and responsibility for ensuring that OCTA is in compliance with PCI DSS requirements. Annual self assessments and quarterly scans should be consolidated and a single person assigned the authority and responsibility for certifying and submitting the results along with any required remediation plans.

Currently, the Senior Security Analyst in OCTA's Information Systems Department is assigned responsibility for ensuring PCI DSS compliance for OCTA's bus pass sales and the OCTA store. The General Manager of Toll Roads is responsible for ensuring PCI DSS compliance for toll road operations.

**Recommendation 3:** Internal Audit recommends that responsibility and authority for compliance with PCI DSS be centralized in order to coordinate compliance and reporting.

**Management Response:** Management acknowledges the need for the responsibility and authority for compliance with PCI DSS to be centralized in order to coordinate compliance reporting.

OCTA's Chief Information Officer (CIO) will be the designated party to oversee compliance reporting for both OCTA and the 91 Express Lanes. Individual SAQ's will be compiled, attested to, and submitted by the CIO. Meetings will be scheduled with the

**ORANGE COUNTY TRANSPORTATION AUTHORITY  
INTERNAL AUDIT DEPARTMENT  
Review of Payment Card Industry  
Data Security Standards Compliance  
July 6, 2011**

appropriate groups and management representatives to formally implement the plan prior to any future PCI DSS reporting.