# Orange County Transportation Authority
# Internal Audit Department



OCTA

# Payment Card Industry
# Data Security Standard Compliance

# Internal Audit Report No. 17-502

**January 4, 2017**



risk analysis
**ethical**
advisory / consulting
**objective**
financial / compliance / controls
**independent**
operational / functional / performance
**Internal Audit**

**Internal Audit Team:**    Gerry Dunning, Senior Internal Auditor, CIA, CISA, CFE
Janet Sutter, Executive Director, CIA

**Distributed to:**    Andrew Oftelie, Executive Director, Finance and Administration
Bill Mao, Chief Information Officer
Michael Bosche, Senior Information Services Security Analyst

**ORANGE COUNTY TRANSPORTATION AUTHORITY**
**INTERNAL AUDIT DEPARTMENT**
**Payment Card Industry (PCI)**
**Data Security Standard (DSS) Compliance**
**January 4, 2017**

## Table of Contents

## Conclusion

The Internal Audit Department (Internal Audit) has completed an audit of Payment Card Industry (PCI) Data Security Standard (DSS) compliance. The purpose of the audit was to assess the adequacy of controls, policies, and procedures to ensure compliance with PCI DSS and related payment card issuer standards.

Based on the audit, the Orange County Transportation Authority (OCTA) is not in compliance with standards and reporting requirements of the PCI DSS or related payment card issuer standards.

## Background

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 credit 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 the PCI DSS. Merchants and service providers not fully compliant with PCI DSS must document detailed action plans to remediate weaknesses and become compliant. In addition to the PCI DSS, American Express maintains an individual Data Security Operating Policy (DSOP), detailing requirements for merchants processing transactions at specified volume levels, and may request merchants to submit evidence of their compliance. Currently, only American Express requests OCTA to submit evidence of compliance with the PCI DSS and the American Express DSOP.

OCTA accepts credit cards for payment of bus passes and identification cards through the OCTA store, the OCTA website, and by phone, and for driver and vehicle permit fees to the Orange County Taxi Administration Program (OCTAP). Cofiroute, OCTA's third party vendor responsible for operation of the 91 Express Lanes, accepts credit cards for payment of toll and transponder fees. Based on the total volume of transactions processed, OCTA is classified as a level 2 merchant. This classification requires OCTA to conduct an annual self-assessment questionnaire (SAQ) and attestation of compliance (AOC), as well as quarterly network vulnerability scans. For any areas of non-compliance, OCTA must prepare and implement a remediation plan. The American Express DSOP requires OCTA to submit the SAQ and AOC, as well as quarterly network scans and any related remediation plans.

The DSS is divided into six sections and 12 subject areas, as follows:

- Build and Maintain a Secure Network and Systems

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

- Maintain a Vulnerability Management Program

  5. Protect all systems against malware and regularly update anti-virus software or programs
  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. Identify and authenticate access to system components
  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 for all personnel

Prior Audit Results

An audit of PCI DSS compliance issued July 6, 2011, found OCTA had not fully complied with PCI DSS requirements for attestation and submission of annual SAQ's and related action plans. Also, OCTA lacked evidence that network scans were performed as required.

## Objectives, Scope, and Methodology

The <u>objective</u> was to assess the adequacy of controls, policies, and procedures in place to ensure compliance with PCI DSS and payment card issuer standards. The <u>scope</u> included the period from January 2014 through September 2016. The <u>methodology</u> included review of SAQ's and related documentation for evidence of compliance and timely submission; review of quarterly network scans for compliance and timely submission; testing of selected assertions in the latest SAQ for accuracy; and interview and review of evidence of monitoring of Cofiroute USA's (Cofiroute) activities related to PCI DSS.

We conducted this performance audit 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 our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Audit Comments, Recommendations, and Management Responses

Conduct of Annual Self-Assessment Questionnaire and Attestation of Compliance

As identified in a prior audit, OCTA has not fully complied with PCI DSS requirements for timely completion of the annual SAQ and implementation of remediation plans.

OCTA continues to reflect non-compliant status with all 12 areas outlined by the PCI DSS. While remediation plans and dates are identified as required, comparison of the SAQ's year-over-year identified no progress toward achieving compliance and staff acknowledged that resources dedicated to implementing these plans are insufficient. Internal Audit noted that some remediation dates exceeded the 12 month limitation set by the American Express DSOP and that remediation dates listed in the prior years' SAQ were not achieved. In addition, the SAQ's have not been completed and submitted timely upon request of the payment card issuer, American Express.

Cofiroute staff also completes a SAQ for the purpose of providing input to OCTA for inclusion in the combined SAQ; however, OCTA staff does not obtain, evaluate, and/or periodically validate Cofiroute's information.

**Recommendation 1:**

Internal Audit recommends that management evaluate the necessary resources and controls to ensure full compliance with PCI DSS and develop a proposal to obtain compliance and/or provide a reasonable approach moving forward. In addition, management should implement oversight controls to assess the accuracy, timeliness, and sufficiency of Cofiroute's PCI DSS compliance information.

**Management Response:**

Management agrees with the recommendation to implement oversight controls to assess the accuracy, timeliness, and sufficiency of Cofiroute's PCI DSS information.  Since Cofiroute processes over 780,000 credit card transactions yearly, it has assigned two full-time staff members for PCI compliance activities.  OCTA management requires and expects Cofiroute to keep its customer credit card information secure and will implement yearly reviews to assess the accuracy, timeliness, and sufficiency of Cofiroute's PCI DSS information.

OCTA processes credit card information at a much smaller scale than Cofiroute.  The total quantity of credit card transactions processed by OCTA is approximately 10,000 on a yearly basis.  OCTA's Information Systems (IS) staff manages cybersecurity based on risk potential to our technology environment and the customers that are affected by its systems.  Staff acknowledges the importance of PCI compliance and has placed priority

and resources on cybersecurity. A full-time position has been reallocated within the IS Department to augment the staff focused exclusively on cybersecurity. The current goal of OCTA's cyber security activities is focused on securing the environment and OCTA's customer's information. These cybersecurity activities improve the overall PCI compliance level at OCTA.

Previously, staff had informally determined that the cost of becoming fully PCI compliant outweighed the incremental security benefits it would provide given the relatively few credit card transactions, the high PCI standards, and the cybersecurity efforts already in place at OCTA. However, management agrees to undertake a formal assessment to determine if it is advisable to become fully PCI compliant given the projected number of transactions, the cost to implement the recommendations, and the overall cyber security environment already employed at OCTA.

In addition, any new OCTA commerce functions requiring credit card information are being outsourced to third party channels. The implementation of OCTA's mobile ticketing application is an example in which customers buying OCTA mobile tickets do not have their credit card information pass through OCTA's networks.

In response to Internal Audit's recommendations, management will do the following:

1. Management will engage with a third party PCI Security Assessor to perform SAQs going forward.  This will provide objective third party expertise on OCTA's compliance efforts.
2. Management will assess the remediation items identified in the SAQ and address items that fall into existing security improvement efforts.
3. Management will perform a yearly assessment of Cofiroute's PCI DSS compliance information.
4. Management will undergo a review to determine if OCTA should take the steps necessary to become fully PCI compliant.
5. Management will continue to allocate and prioritize resources to cybersecurity risks while addressing PCI compliance concerns


## Quarterly Network Scans

As identified in the prior audit, OCTA does not complete and submit quarterly scans as required by PCI DSS and the American Express DSOP. Non-certified PCI DSS scans are generally performed on a monthly basis, and identify vulnerabilities in OCTA systems. Remediation efforts to address the identified weaknesses are not documented and implemented, as required. In addition, OCTA does not obtain, evaluate, or periodically validate Cofiroute's activities related to network scans and results of the scans performed by Cofiroute are not included in submissions to American Express.

**Recommendation 2:**

Internal Audit recommends that management implement procedures to ensure that quarterly network scans are performed and remediation efforts are identified and addressed accordingly. Management should also implement procedures for oversight and monitoring of Cofiroute's activities and incorporate their system scan results into submissions to American Express.

**Management Response:**

Management agrees with Internal Audit's recommendation and will implement procedures to ensure quarterly network scans are performed. Management will also identify items to be remediated and implement them based on risk and cost. Management will allocate resources to perform periodic assessments of Cofiroute's PCI DSS compliance information.