



**January 11, 2017**

**To:** Finance and Administration Committee

**From:** Darrell Johnson, Chief Executive Officer  
Janet Sutter, Executive Director  
Internal Audit Department

**Subject:** Payment Card Industry Data Security Standard Compliance,  
Internal Audit Report No. 17-502

### **Overview**

The Internal Audit Department has completed an audit of Payment Card Industry Data Security Standard compliance. Based on the audit, the Orange County Transportation Authority is not fully compliant with standards and reporting requirements of the Payment Card Industry Data Security Standard or related payment card issuer standards.

### **Recommendation**

Direct staff to implement two recommendations provided in Payment Card Industry Data Security Standard Compliance, Internal Audit Report No. 17-502.

### **Background**

The Payment Card Industry (PCI) Data Security Standard (DSS) was created to help organizations that accept and process credit card payments to prevent fraud by specifying the framework for a secure payment environment. Any organization that collects, processes, stores, or transmits credit card information is required to be in compliance with the PCI DSS. 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.

The Orange County Transportation Authority (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. Cofiroute USA (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.

### ***Discussion***

As identified in a prior audit, OCTA has not fully complied with PCI DSS and American Express DSOP requirements for timely completion of the annual SAQ and implementation of remediation plans. Cofiroute staff also completes a SAQ for the purpose of providing input to OCTA; however, OCTA staff does not obtain, evaluate, and/or periodically validate the information compiled by Cofiroute. Internal Audit recommended management evaluate the necessary resources and controls to ensure full compliance with PCI DSS and develop a proposal to achieve compliance and/or provide a reasonable approach moving forward. Management agreed and outlined actions for undertaking an assessment and evaluation of steps necessary to become fully compliant.

In addition, 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; however, remediation efforts to address 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. Internal Audit recommended management implement procedures to ensure that quarterly network scans are performed and remediation efforts are identified and addressed accordingly. Management agreed to perform quarterly scans and implement remediation actions based on risk and cost.

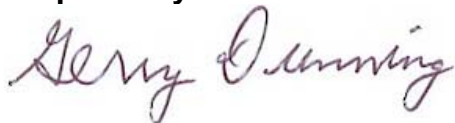
### ***Summary***

The Internal Audit Department has completed an audit of PCI DSS compliance.

***Attachment***

- A.      Payment Card Industry Data Security Standard Compliance, Internal  
          Audit Report No. 17-502

**Prepared by:**



Gerry Dunning  
Senior Internal Auditor, Internal Audit  
714-560-5875

**Approved by:**



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