OC Board of Supervisors'

1st District	2nd District	3rd District	4th District	5th District
Janet Nguyen, Chair	John M.W. Moorlach	Bill Campbell, Vice Chair	Shawn Nelson	Patricia C. Bates

Internal Audit Department

ORANGE COUNTY

AUDIT HIGHLIGHT   OCTOBER 21, 2010

Information Technology Audit:
TREASURER-TAX COLLECTOR
CONTROLS OVER COMPLIANCE WITH
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD
Audit No. 2946

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

WHY IS THIS AUDIT CRITICALLY IMPORTANT?

The Payment Card Industry Data Security Standard (PCI DSS) is a collaborative effort among several card brands to achieve a common set of security standards for use by entities that process, store or transport payment card data. For the 12-month period ended December 31, 2009, County departments/agencies processed over **840,000 payment card transactions totaling $193 million** (excluding the Clerk-Recorder).

There are a number of costs associated with being non-compliant with PCI DSS as further described in the report.

WHAT THE AUDITORS FOUND?

We found that the Treasurer-Tax Collector did not have 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 a **Significant Issue**.

During our audit the Treasurer-Tax Collector (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 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. 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. The T-TC and applicable departments concurred with all findings and recommendations.