OFFICE OF THE INTERNAL AUDITOR

Internal Audit Memorandum

CITIZENS PROPERTY INSURANCE CORPORATION

To: Jennifer Montero, Chief Financial Officer

From: Patrick Lynch, Internal Audit Manager

CC: Barry Gilway, President/CEO/Executive Director
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Mark Kagy, Acting Inspector General
Joe Martins, Chief of Internal Audit

Date: October 14, 2019

Subject: Targeted Accounts Payable Analytics

During 2018, Citizens implemented an integrated ERP solution (Oracle Fusion Cloud Service) named CenterPoint. CenterPoint, replaced independent applications previously used by Human Resources, Finance and Procurement to promote a strong financial operating environment.

During 2019, the Office of the Internal Auditor completed an audit of CenterPoint Financial and Procurement User Access which identified certain system limitations associated with the complexity of Oracle roles and permissions and the business need to create custom roles. This contributed to challenges in effectively managing user access and these conditions suggested the need to validate that vulnerabilities have not been exploited.

In response, the OIA scheduled this targeted review of Accounts Payable transactional data.

Objectives and Scope

The audit objective was to assess occupational fraud risks related to the vendor management, purchasing and accounts payable processes and identify potential misconduct related to payment transactions.

Leveraging data analytics, we evaluated all accounts payable disbursement transactions since the implementation of CenterPoint (January 2018) to March 31, 2019. This identified anomalies (or red flags) in the data that required detailed review to validate any potential misconduct.

Results

We considered occupational fraud risks common in the accounts payable process and developed 15 computer-aided audit techniques (“CAAT”) that were designed to identify unexpected or unexplained patterns in data that may represent potential misconduct. Results of our CAATs highlighted 11 anomalies (or red flags) in the data that required detailed review to validate any potential misconduct. The anomalies identified were categorized by us as onetime payment with no physical address, potential duplicates, and/or multiple payments on same day, among others.

Our review of all 11 anomalies found no instances of fraud, waste or abuse and we are of the opinion that the user access vulnerabilities previously identified have not had a significant impact on the validity of accounts payable transactions during the period of the review.