CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR

Audit of Information Technology Services Department
& Finance Department

Payment Card Industry Security

Project No. AU21-019

December 2, 2021

Kevin W. Barthold, CPA, CIA, CISA
City Auditor

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an audit of the Information Technology Systems Department (ITSD) and Finance Department, specifically the Payment Card Industry (PCI) Security. The audit objectives, conclusions, and recommendations follow:

Determine if the City is compliant with PCI Data Security Standards for credit card transaction processing.

The ITSD and Finance Departments have controls in place to ensure the City is compliant with PCI Security Standards.

We determined that the PCI Security Plan is periodically reviewed and addresses all areas of the PCI requirements related to IT security. Additionally, reporting by the City is accurate and timely which include Self-Assessment Questionnaires and quarterly vulnerability scans. Furthermore, all equipment used for credit card transactions within the City are PCI compliant and appropriate payment card acceptance training is in place.

ITSD and Finance managements' acknowledgment of audit results is in Appendix B on page 6.

Table of Contents

Background

The Payment Card Industry Data Security Standards (PCI DSS) is a set of standards for safely handling sensitive payment cardholder information. It was developed by the PCI Security Standards Council, founded by the five global payment brands: American Express, Discover Financial Services, JCB International, Mastercard Worldwide, and Visa Inc.

PCI DSS standards are designed to help secure credit card information that is stored, processed, or transmitted by merchants. Where the City processes Visa, Mastercard, American Express, and Discover credit card payments, the City must adhere to PCI DSS standards and technical requirements.

PCI compliance applies to all City departments that use credit card payment systems to process, store, and/or transmit credit card payment data. The City's requirement as a merchant depends on the type of payment systems, or third-party vendor product/services implemented and the number of payment card transactions processed through the acquiring bank, Chase, who processes payment card transactions on the City's behalf. The City has 138 active Pin Transaction Devices (PTS) in addition to web-based point of sale systems.

Each brand of credit card merchant has its own requirements for reporting compliance with PCI DSS version 3.2. The City's merchant levels and requirements are described in the table below.

Card Type	**Transaction Volume Calendar Year 2020** (Jan 2020–Dec 2020)	**Merchant Level**	**Merchant Level Requirements**
Mastercard	321,197	Level 3	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV
Visa	705,362	Level 3	Annual Self-Assessment Questionnaire and Quarterly Network Scan by ASV
American Express	78,647	Level 2	Quarterly Network Scan
Discover	13,737	Level 3	Quarterly Network Scan by ASV **AND** one of the following: -Annual onsite review by QSA-PCI DSS Assessment -Annual Self-Assessment
Total	**1,118,943**		

To fulfill all reporting requirements, ITSD, specifically IT Security, supports the Finance Department in the process of assessing PCI compliance, and assist the user departments in the process of self-assessment as well as with other technical issues related to PCI compliance. IT Security establishes a timeline that outlines

when specific Self-Assessment Questionnaires will be completed in quarterly segments throughout the year. In addition, quarterly security scans are performed by an Approved Scanning Vendor with the results accompanying the self-assessments submitted for each specific quarter.

There are potential penalties for failure to report compliance status in a timely manner as well as for experiencing a breach while not in compliance. A breach of cardholder information can lead to reputational damage, lawsuits, substantial fines, and being banned from accepting payment cards.

Audit Scope and Methodology

The audit scope was from January 2020 through March 2021.

To establish our test criteria, we reviewed Administrative Directive 7.3a Data Security, Payment Card Industry Data Security Standards version 3.2, and the City's Agreement with Chase Paymentech.

We interviewed ITSD and Finance staff and reviewed department policies and procedures to gain an understanding of the controls related to PCI Security.

As part of our testing procedures, we examined the following areas:

- Transaction counts reported by the City
- Inventory of all methods of payment card acceptance
- Staff training
- PCI Compliance Plan
- Self-Assessment Questionnaires
- Quarterly vulnerability scans
- Reporting to Chase Bank

We relied on system generated reports from SAP which stores credit card data. We relied on the accuracy of the credit card data rather than evaluating the system's general and application controls. We do not believe that the absence of testing general and application controls had an effect on the results of our audit.

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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

The ITSD and Finance Departments have controls in place to ensure the City is compliance with PCI Security Standards.

We determined that the PCI Security Plan is periodically reviewed and addresses all areas of the PCI requirements related to IT security. Additionally, reporting by the City is accurate and timely which include Self-Assessment Questionnaires and quarterly vulnerability scans. Vulnerability scans are performed by an approved scanning vendor and items requiring remediation are coordinated with ITSD staff and business owner. Furthermore, all equipment used for payment card transactions within the City are PCI compliant and appropriate payment card acceptance training is in place.

Appendix A – Staff Acknowledgement

Gabe Trevino, CISA, Audit Manager
Daniel Kuntzelman, CIA, CISA, Auditor in Charge

Appendix B – Management Acknowledgement

CITY OF SAN ANTONIO
SAN ANTONIO TEXAS 78283-3966

November 18, 2021

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
San Antonio, Texas

RE: Management's Acknowledgement of its Review of Payment Card Industry Security Audit

Finance Department and Information Technology Services Department management has reviewed the audit report and provided its comments to the auditors. As there are no recommendations for management, no management responses are required.

Finance and Information Technology Services Department:

☒ Fully Agrees

☐ Does Not Agree (provide detailed comments)

Sincerely,

Troy Elliott
Deputy Chief Financial Officer
Finance

11/19/2021
Date

R. Craig Hopkins Jr.
Craig Hopkins
Chief Information Officer
ITSD

19 Nov 2021
Date

Ben Gorzell
Chief Financial Officer
City Manager's Office

11/23/2021
Date