Express Memo

PCI Compliance (Virtual) Audit

2020-08
Report Date: 6/30/2020

Background

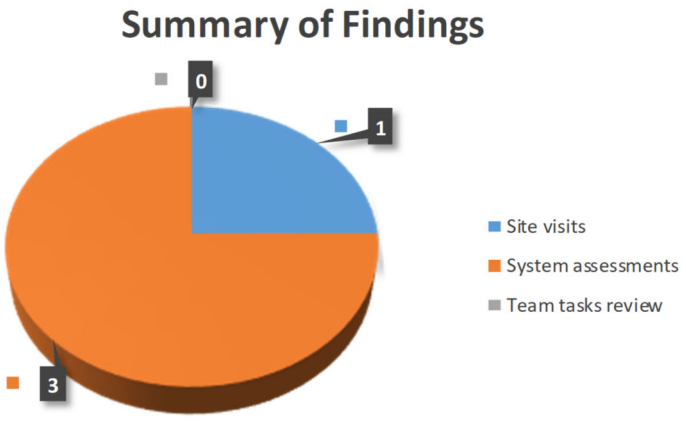
The City of Glendale accepts payment cards as a form of payment for fees, therefore City departments must adhere to the Payment Card Industry Data Security Standards (PCI DSS) requirements in order to protect customers' cardholder data. Failure to do so may result in significant fines and/or revocation or suspension of payment card processing privileges, increased liability from potential fraudulent charges, and damage to the City's reputation. The City of Glendale processed over 1.7 million payment card transactions in 2019, which makes the City a Level 2 merchant as defined by the PCI Security Standards Council (PCI SSC). To ensure compliance with the PCI DSS, the City hired an external Qualified Security Assessor (QSA) to perform an annual assessment and prepare and submit a formal Report on Compliance (ROC) for the City's required validation. In order to assess ongoing compliance with PCI DSS and help City departments be better prepared for the annual assessment, Internal Audit is tasked to perform periodic audits of the City's PCI Policy (APM 7-9) and all related departmental Payment Card Acceptance and Processing Procedures (Procedures).

Objective/Scope/Methodology

The objective of this audit is to determine the City's compliance with its PCI Policy and Procedures. The scope of this audit was based upon the PCI DSS in-scope requirements, as defined by the QSA. The detailed scope and methodology are shown in Appendix A.

Summary of Results

Based on our review, 4 of the 21 areas reviewed were determined to be non-compliant with the City's PCI Policy and Procedures. The table below provides a summary of the non-compliant areas noted based on locations, systems, and tasks. All non-compliant findings have been remediated. Detailed test results are shown on the next page.



By the Numbers

4	12	5
Sites that process card payments reviewed for compliance.	Systems that process card payments reviewed for compliance.	PCI Team assigned tasks reviewed for timely completion.

Detailed Results

The table below summarizes the controls and exceptions.

Test	Description	Areas Tested	Findings
1.	Determine if Procedures are being followed by departments through performing site visits.	4	1
2.	Determine if system controls (password policy, user accounts, critical patches) are in place to ensure cardholder data is safeguarded. This includes both testing the hosted system and obtaining compliance documentation from third party vendors that process card payments for the City.	12	3
3.	Determine if the tasks assigned to the PCI Team members are being completed in a timely manner following the Annual PCI Compliance Calendar within the City's PCI DSS Guide.	5	0
Total		**21**	**4**

Findings and Action Taken

The table below details the non-compliant areas noted, actions taken, and remediation status.

	Findings	Action Taken
1.	Full cardholder data was retained by staff after the underlying transactions were processed. Additionally, telephone payments were accepted, which was not consistent with the Department's Procedures.	Staff destroyed all applicable documents that contained full cardholder data and updated their Procedures to reflect telephone payments. **Status: Remediated**
2.	The Attestation of Compliance (AOC) on file for a third party merchant was completed using an outdated version of the form.	The correct version of the AOC was obtained. **Status: Remediated**
3.	One system had two active accounts belonging to users that no longer required access. Additionally, the automatic lockout feature for incorrect log on attempts was not enabled.	The accounts of the two inactive users were disabled and the automatic lockout feature was enabled. **Status: Remediated**
4.	One system did not have a mechanism in place for City staff to identify available system patches and to ensure that they are applied timely.	The department revised its Patch Management Policy and Procedure to assure proactive system patch update checking on a regular basis. **Status: Remediated**

Distribution List

For Action	For Information
• Rafi Manoukian, City Treasurer	• Audit Committee
• Guia Murray, Assistant City Treasurer	• City Council
	• Yasmin K. Beers, City Manager
	• Roubik Golanian, Assistant City Manager
	• Aram Adjemian, City Clerk
	• Elena Bolbolian, Director of Innovation, Performance, & Audit
	• Jason Bradford, Chief Information Officer
	• Onnig Bulanikian, Director of Community Services & Parks
	• Matthew Doyle, Director of Human Resources
	• Yazdan Emrani, Director of Public Works
	• Michele Flynn, Director of Finance
	• Michael J. Garcia, City Attorney
	• Philip Lanzafame, Director of Community Development
	• Silvio Lanzas, Fire Chief
	• Carl Povilaitis, Police Chief
	• Gary Shaffer, Director of Library, Arts & Culture
	• Stephen Zurn, General Manager of Glendale Water & Power

Appendix A: Detailed Scope and Methodology

Scope

The scope of this audit covers the PCI DSS requirements, as defined by the QSA. The in-scope site locations and systems were based upon the listings maintained by the City Treasurer's Office (CTO). If these listings are not complete, there could be departments processing payment cards and/or utilizing the services of third parties to process payments cards, that were not tested.

For the current quarter, Internal Audit selected the following locations, systems and tasks to test:

- 4 sites visits. The remaining 16 sites were closed due to COVID-19.
- 12 third party systems based on the listing provided by CTO at the start of the audit.
- 5 PCI Team assigned tasks that were due for completion from January-April 2020 as outlined in the Annual PCI Compliance Calendar within the City's PCI DSS Guide.

Methodology

As a Level 2 merchant, the City can either self-assess by an Internal Security Assessor (internal employee who is formally trained and PCI SSC certified) or hire an external QSA to conduct the assessment and issue a formal Report on Compliance (ROC) for the City's required annual PCI DSS validation. According to CTO, since Level 2 involves a higher level of scrutiny, the City decided to hire an external QSA, who is certified by the PCI SSC to validate an entity's adherence to PCI DSS.

To gain an understanding of the PCI DSS requirements, Internal Audit shadowed the City's QSA during the 2019 annual PCI audit. Internal Audit also consulted with the QSA and other PCI Team members as needed throughout the audit. Based upon this understanding, the following procedures were developed:

- Review updated Procedures and interview staff to ensure knowledge and compliance of policies and perform the following:
    - Obtain updated device listings from CTO and ensure devices being used are reflected in the device listings.
    - Determine if employees who handle payment card information have taken the necessary PCI training.
- Perform system assessments to ensure third parties have safeguards in place to protect cardholder data. This may involve the following:
    - Collect Attestation of Compliance documents.
    - Review PCI compliance language in City contracts.
    - Perform system reviews.
- Review the City's PCI Policy (APM 7-9) and PCI DSS Guide to ensure:
    - Tasks noted in the Annual PCI Compliance Calendar are being timely performed by assigned parties.
    - Interview PCI Team to determine knowledge and compliance with established roles.

For the current quarter, Internal Audit performed the audit steps virtually in order to maintain social distancing, due to COVID-19. In addition, the QSA provided assistance in performing system assessments.

Frequency

Internal Audit plans to test a portion of the in-scope PCI Compliance requirements quarterly. The goal is to cover all applicable locations, third parties, and calendar tasks once per year. The next audit is scheduled to take place in August 2020.