Express Memo

PCI Compliance Audit

City of Glendale
Internal Audit

# 2022-01
Report Date: 09/28/2021

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. To ensure compliance with the PCI DSS, the City hired an external Qualified Security Assessor (QSA) to perform an annual assessment. Additionally, in order to assess ongoing compliance with PCI DSS and help City departments better prepare for the annual assessment, Internal Audit is tasked with performing periodic audits of the City's adherence to its PCI Policy (APM 7-9) and departmental Payment Card Acceptance and Processing Procedures (Procedures). The goal is to cover all in-scope sites, systems, and calendar tasks once per year prior to the QSA's annual assessment. This is the last of three audits scheduled for calendar year 2021.

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.

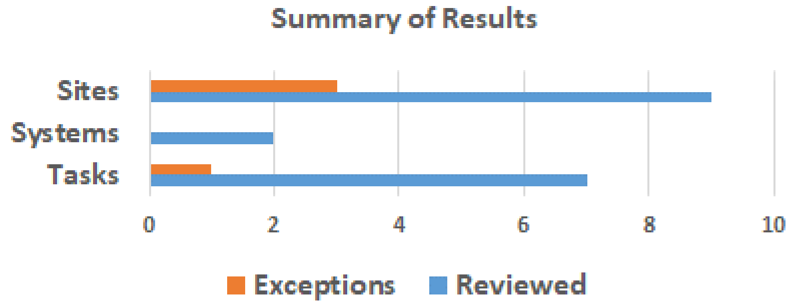
Summary of Results

As of August 31, 2021, there were a total of 53 in-scope sites/systems/tasks, 18 were reviewed in the current audit. The table below summarizes the audit for calendar year 2021.

Calendar Year 2021 Review Status

Column1	1st Audit	2nd Audit	Current Audit	Total
Sites	6	5	9	20
Systems	2	2	2	6
Tasks	14	6	7	27
Total	**22**	**13**	**18**	**53**

Based on a review of the 18 areas, three exceptions were noted during the site visits related to tamper seals and record keeping. There was also one task related exception with regards to Attestation of Compliance (AOC) management. All four exceptions were remediated.



Detailed Results

The table below summarizes the controls, number of areas tested, and exception(s).

Test	Description	Areas Tested	Exception(s)
1.	Determine if departmental Procedures are being followed through performing site visits.	9	3
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 utilize the City's merchant ID to process payments cards.	2	0
3.	Determine if the calendar tasks assigned to the PCI Team members are being completed in a timely manner per the City's PCI DSS Guide.	7	1
	Total	**18**	**4**

Exceptions and Actions Taken

The table below details the exception(s), action(s) taken, and remediation status.

	Exception(s)	Action(s) Taken
1.	Tamper seal checks on one payment card terminal and pin pad were not consistently performed at one site.	Tamper seal checks of the payment card terminal and pin pad have commenced at the required intervals. **Status: Remediated**
2.	One site had employees who were able to process payment cards without taking the requisite PCI training. In addition, when asked about the site's Procedures, a copy could not be provided nor was the location of the online copy known by staff.	All employees will be required to complete PCI training prior to processing payment cards. Staff was able to subsequently locate a physical copy of the site's Procedures and also found the location of the online copy. **Status: Remediated**
3.	One department, with three sites visited during the current audit, does not accept telephone payments. Nonetheless, the City Treasurer's Office (CTO) recommends that departments acknowledge the acceptance of telephone payments in their Procedures, in case they ever need to process refunds over the telephone.	The Procedures has now been updated to reflect telephone payments are accepted. **Status: Remediated**
4.	One calendar task item was related to ensuring current AOC documents from vendors are obtained. However, Internal Audit noted one vendor's AOC was expired.	The current AOC has been obtained from the vendor and future requests for AOCs will be made prior to the expiration date. **Status: Remediated**

Distribution List

For Action	For Information
• Rafi Manoukian, City Treasurer	• Audit Committee
• Guia Murray, Assistant City Treasurer	• City Council
	• Aram Adjemian, City Clerk
	• 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
	• Roubik Golanian, City Manager
	• Philip Lanzafame, Director of Community Development
	• Silvio Lanzas, Fire Chief
	• Carl Povilaitis, Police Chief
	• Gary Shaffer, Director of Library, Arts & Culture
	• John Takhtalian, Deputy City Manager
	• Mark Young, General Manager of Glendale Water & Power

Appendix A: Detailed Scope and Methodology

The City of Glendale is a Level 2 merchant as the City processes 1-6 million transactions annually. For calendar year 2020, the City processed over 525,000 payment card transactions, which is less than the 1 million lower limit threshold. However, Visa, one of the major payment card processing entities, does not recommend changes to a merchant's level based on reduced transaction volume in calendar year 2020 due to COVID-19. There are exceptions for significant store closures or bankruptcy, but those do not apply to the City. Since this reduced activity was likely attributable to COVID-19, the City's merchant bank has stated the City's merchant level will remain the same at Level 2.

To ensure compliance with the PCI DSS, the City hired an external QSA to perform an annual assessment and prepare and submit a formal Report on Compliance (ROC) for the City's required validation. A ROC is required for Level 1 merchant and is optional for a Level 2 merchant.

Scope

The scope of this audit covers the PCI DSS requirements, as defined by the QSA. The in-scope sites, systems, and tasks were based upon the listings maintained by the City Treasurer's Office (CTO).

Methodology

To gain an understanding of the PCI DSS requirements, Internal Audit shadowed the City's QSA during the 2020 annual PCI audit. Internal Audit also consulted with the QSA and/or 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. This may involve the following:
    - Obtaining updated device listings from CTO and ensure devices being used are reflected in the device listings.
    - Verifying that 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:
    - Collecting Attestation of Compliance documents.
    - Reviewing PCI compliance language in City contracts.
    - Performing system reviews.
- Review the City's PCI Policy (APM 7-9) and PCI DSS Guide to ensure knowledge and compliance of policies. This may involve the following:
    - Reviewing tasks noted in the Annual PCI Compliance Calendar and ensure they are being timely performed by assigned parties.
    - Interviewing PCI Team members to determine their knowledge and compliance with established roles.

Frequency

Internal Audit plans to test all in-scope sites, systems, and calendar tasks once per year through three separate quarterly audits. The next audit cycle will commence in 2022.