mesa·az
CITY AUDITOR
mesaaz.gov

20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

AUDIT REPORT

Date:	**June 30, 2022**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Lead Auditor:	**Michelle Hute, Senior Internal Auditor**

OBJECTIVE

Our annual credit card security review is an assessment of the City's operational efforts to protect cardholder data, as required by the Payment Card Industry Data Security Standard (PCI DSS). Specifically, our objectives were to determine whether:

- The City maintains and enforces policies and procedures that meet PCI DSS requirements.
- Individuals who handle cardholder data are adequately screened and trained.
- When service providers are used to handle cardholder data, due diligence is performed prior to engaging them, written agreements include required language, and they are monitored annually for PCI DSS compliance.
- Management has implemented corrective action plans in response to prior PCI DSS reviews.

SCOPE & METHODOLOGY

This review was focused on assessing compliance with the operational (non-IT) requirements of PCI DSS, which apply to the City's credit card acceptance sites. Specific criteria and guidance for assessing compliance were provided by the PCI Security Standards Council's *PCI Data Security Standard Requirements and Security Assessment Procedures v3.2.1*, May 2018.

To accomplish our objectives, we:

- Interviewed staff members to ensure they are aware and knowledgeable of PCI DSS requirements and the City's security policies and procedures.
- Reviewed policies and procedures and observed credit card handling operations and processes to ensure they comply with PCI DSS requirements.
- Reviewed contracts and other documentation to ensure service providers are properly managed.
- Reviewed personnel files and training records to ensure cardhandlers are adequately screened and trained.

BACKGROUND & DISCUSSION

The PCI Data Security Standards are technical and operational requirements developed to protect cardholder data and sensitive authentication data. The standards are administered and managed by the PCI Security Standards Council, whose mission is to enhance payment account data security throughout the transaction process. It applies to all entities that store, process, or transmit cardholder data. This includes those entities that are involved in payment card processing, such as merchants, processors, acquirers, issuers, and service providers.

As a merchant that accepts credit cards as a method of payment, the City is required to comply with PCI DSS requirements. Failure to do so could place customers at risk for fraudulent activity and could result in credit card companies levying fines or prohibiting the City from accepting credit card payments. To help ensure compliance, the Accounting Services Division is responsible for maintaining Management Policy 212, *Credit Card Handling*, and providing training for individuals on PCI DSS requirements and the City's credit card handling policies and procedures. They are also responsible for managing the City's merchant accounts. The Department of Innovation and Technology is responsible for ensuring compliance with the IT-related requirements of PCI DSS as well as the annual submission of a Self-Assessment Questionnaire to the City's acquiring bank.

CONCLUSION

In our opinion, management has implemented policies and procedures to ensure continued compliance with PCI DSS requirements. However, awareness and compliance with some PCI DSS requirements has not always been consistent. Specifically, ensuring employees complete credit card handling training within PCI DSS timelines is a common recurring issue, often occurring within different departments year to year. Our current observations and recommendations are summarized below. For additional details, please see the attached Issue and Action Plans.

Our FY 2021 report included two recommendations, which have been implemented and are summarized in the following table:

Recommendation	Implemented
1-1: Library Services should implement a control to ensure that all credit card handlers complete training within the required time frames and that only individuals who have completed the training are processing credit card transactions.	✓
2-1: Ensure that a unique login and password is assigned to each user accessing any system that is used to process credit card transactions.	✓

SUMMARY OF OBSERVATIONS & RECOMMENDATIONS

1. **Observation:** Credit card handling training is not completed within the required timeframes.

   Recommendation: Development Services and Falcon Field should implement a control to ensure that they comply with PCI DSS training requirements.

2. **Observation:** Service providers' PCI DSS compliance status was not monitored.

   Recommendation: Business Services should enforce its written policies and procedures by performing its verification process on its list of service providers at least annually.

Issue and Action Plan #1

Issue #1: Credit card handling training is not completed within the required timeframes.

Observation:

One new credit card handler at Development Services and one new credit card handler at Falcon Field did not complete the credit card handling training within 90 days of beginning their credit card handling responsibilities.

Criteria:

According to PCI DSS v3.2.1, *Requirements and Security Assessment Procedures*, Requirement 12.6.1, the City should educate personnel upon hire and at least annually.

In addition, according to Management Policy 212, *Credit Card Handling*, all employees who handle credit card information must take the Credit Card Handling Training within 90 days of beginning of their credit card handling duties.

Comments:

Without proper training, employees may unknowingly mishandle cardholder data, putting customers at risk of credit card fraud.

Recommendations and Management's Action Plans:

Recommendation #1-1: Development Services should implement a control to ensure that all credit card handlers complete training within the required time frames and that only individuals who have completed the training are processing credit card transactions.

Action Plan #1-1: Ensuring the completion of credit card handler training for new staff has been added to the supervisor's training checklist and all new staff will complete the required training within 6 weeks of their start date.

Individual or Position Responsible: Heather Basford, Permits Supervisor

Estimated Completion Date: 5/31/2022

Recommendation #1-2: Falcon Field should implement a control to ensure that all credit card handlers complete training within the required time frames and that only individuals who have completed the training are processing credit card transactions.

Action Plan #1-2: In addition to the supervisor's new-hire check-list, the supervisor will ask the new hire to confirm with the Financial Coordinator the requirements for handling credit card transactions. This includes the requirement to complete the credit card training within 6 weeks of their start date. The Financial Coordinator will follow up with the supervisor the status of training for each employee who has financial responsibilities.

Individual or Position Responsible: Rick Welker, Financial Coordinator

Estimated Completion Date: 6/6/2022

Issue and Action Plan #2

Issue #2: Service providers' PCI DSS compliance status was not monitored.

Observation: Business Services is responsible for monitoring the PCI DSS compliance status for 11 service providers. However, for 7 of the 11 service providers, Business Services did not perform any follow-up monitoring procedures during the year to ensure that they continued to remain PCI DSS compliant.

Criteria: According to PCI DSS v3.2.1, *Requirements and Security Assessment Procedures*, Requirement 12.8.4, the City is required to maintain a program to monitor service providers' PCI DSS compliance status at least annually.

In addition, according to Business Services' *PCI DSS Compliance Guidelines*, the Business Services department is responsible for maintaining a program to monitor the City's service providers' PCI DSS compliance status. A designated compliance coordinator is responsible for collecting information, such as a certificate or signed statement of compliance, to ensure the service providers are PCI DSS compliant. This verification process should be conducted as least annually for each service provider on its list of providers.

Comments: Without an effective monitoring program in place, there is a risk that the City could overlook a service providers' PCI DSS compliance status. Specifically, if a service provider did not comply with PCI DSS requirements, there is an increased risk that cardholder data and other sensitive authentication data may not be protected.

Recommendation and Management's Action Plan:

Recommendation #2-1: To ensure the City's service providers are PCI DSS compliant, Business Services should enforce its written policies and procedures by performing its verification process on its list of service providers at least annually.

Action Plan #2-1: The Business Services staff member that handles this duty was assigned additional duties and projects and simply lost sight of this task. The tracking spreadsheet has been added to the department director's weekly exception reports as a back-up to ensure we stay on top of the verification process. We have caught up on all but one contract that is expiring at the end of June.

Individual or Position Responsible: Tom Lavell, Specialty Billing and Collections Administrator; Ed Quedens, Business Services Director

Estimated Completion Date: 6/30/2022