mesa·az
CITY AUDITOR
mesaaz.gov

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

AUDIT REPORT

Date:	**July 22, 2021**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Lead Auditor:	**Dawn von Epp and Michelle Hutson, Sr Internal Auditors**

OBJECTIVE

Our annual credit card security review is an assessment of the City's operational efforts to protect customers' credit card information, as required by the Payment Card Industry's 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 credit card information are adequately screened and trained.
- When service providers are used to handle credit card information, 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 credit card handling activities at the City's credit card acceptance sites. Specific criteria and guidance for assessing compliance were provided by the PCI Security Standards Council's *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures v3.2.1*, May 2018. To accomplish our objectives, we interviewed staff members; and reviewed policies, procedures, document inventories, contract documents, and training records. Due to the impact of the Coronavirus Disease 2019 pandemic, we did not observe operations and processes as is part of our usual assessment. Additionally, 40 of the 44 sites that accept credit card payments were closed to the public and did not accept in-person credit card payments for either part of or for the entire fiscal year.

BACKGROUND & DISCUSSION

As a merchant that accepts credit cards, the City is required to comply with PCI DSS. Failure to do so could place our customers at risk for identity theft and could result in credit card companies levying fines or prohibiting the City from accepting credit card payments. To help ensure compliance citywide, the Accounting Services Division is responsible for maintaining Management Policy 212 Credit Card Handling (MP 212) and providing training for individuals on PCI DSS requirements and credit card handling procedures. They also manage the City's

merchant accounts. The Department of Innovation and Technology (DoIT) is responsible for ensuring the City's compliance with the IT-related requirements of PCI DSS, and for the annual submission of a Self-Assessment Questionnaire to our acquiring bank.

CONCLUSION

Prior Year Issues: Our 2020 report[1] included a few recommendations, all of which have been implemented, as briefly summarized in the following table:

Recommendation	Departments	Implemented
Staff should maintain an up-to-date list of POS devices, and use it when performing inspections.	PRCF	✓
Staff should conduct and document inspections of all point of sale devices to meet both PCI DSS and City requirements.	PRCF	✓
Staff should implement a control to ensure that new credit card handlers complete training within 3 months.	Arts & Culture Mesa Arts Center	✓
Staff should implement a control to ensure that all credit card handlers complete training within the required time frames.	PRCF	✓

New/Continuing Issues: Overall, management has attempted to implement better processes to ensure continued compliance, but awareness and compliance with PCI DSS requirements has not been consistent. Ensuring employees complete credit card training within PCI DSS timelines is a common recurring issue, often occurring within different departments year to year. The current issues are summarized below; and additional details are presented in the attached Issue and Action Plans (IAPs). Next year's review will include follow-up testing to verify that the departments have successfully resolved the issues.

SUMMARY OF OBSERVATIONS & RECOMMENDATIONS

1. **Observation:** Credit card training is not consistently being completed by credit card handlers within the required time frames.

   Recommendation: Library Services should implement controls to ensure that they comply with the training requirement.

2. **Observation:** Convention Center staff are sharing logins and passwords.

[1] The FY 2019 Annual Credit Card Security Review included a recommendation for the Convention Center to implement a secure process for receiving credit card information. The department implemented a plan to address the recommendation, but we have been unable to test the effectiveness since events have not been booked due to the pandemic. Once events are booked, we will verify the effectiveness of the department's action plan.

Recommendation: Ensure that a unique login and password is assigned to each user accessing any system that is used to process credit card transactions.

Issue and Action Plan #1

Issue #1: Credit card training is not consistently being completed within the required time frames.

Observation: Three credit card handlers at Library Services did not complete their annual credit card handling training this year while still processing credit card transactions.

Criteria: PCI DSS v3.2.1, Requirements and Security Assessment Procedures, Requirement 12.6.1: "*Educate personnel upon hire and at least annually.*"

Minimum Required Credit Card Handling Procedures, Merchant and Agent Responsibilities, Item #2: "*Agents shall receive training on Handling Procedures within three months of assignment to a position that requires Cardholder Data handling duties, and at least every year thereafter.*"

Comments: Without training, employees may unknowingly mishandle credit card data, putting customers at risk of credit card fraud. Although the number of employees that were not compliant was minimal, the process in the department does not appear to be working to ensure that all credit card handlers are taking required training timely.

Recommendation and Management's Action Plan:

Recommendation #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.

Action Plan #1-1: Written procedures will be changed to require new hires who handle cash and credit cards to be trained within 30 days of hire date instead of within their first 3 months. In addition, the formal "Information Services New Hire" checklist of items to completed within 30 days of hire will be updated to include the cash and credit card training. A spreadsheet tracking employee hire dates and training dates has been created. In addition to critical dates, it includes a column for supervisors to sign off once the new hire has been added to the monthly reminder spreadsheets that supervisors receive from Finance. All staff members who work the public service desks will also be required to complete the annual training in the month of September.

Individual or Position Responsible: Branch Operations Supervisor II at Main Library, Branch Operations Supervisor II at Red Mountain

Library, Branch Operations Supervisor I at Dobson Ranch Library, and Librarian II at Express Library (if re-opened).

Estimated Completion Date: September 30, 2021

Issue and Action Plan #2

Issue #2: Employees are sharing logins and passwords.

Observation: Parks, Recreation, and Community Facilities (PRCF) Convention Center staff were using a shared login and password when accessing the system used for exhibitor charges.

Criteria: MP 326 Information Security and Computer Usage Policy includes the following:

> Section II Security Posture: *"... Passwords and credentials used for access to City data and systems, will be strong, individually-owned, changed frequently, and always transmitted and stored encrypted, protected, and never disclosed to anyone."*
>
> Section IV Roles and Responsibility, City Staff:
> - *"Responsible for changing his/her passwords frequently;*
> - *Protect their passwords and shall never disclose to anyone, including family and other household members when work is being done at home;*
> - *May not use another's user ID and password. Exceptions must be approved by the Chief Information Officer or designee;"*

PCI DSS version 3.2.1 Requirements and Security Assessment Procedures, requirement # 8.1.1 states, *"Assign all users a unique ID before allowing them to access system components or cardholder data."*

Comments: While only a few people were using the same login, when this occurs, accountability of who accessed cardholder data, and why, is lost. Also, should inappropriate actions take place they cannot be traced to the specific responsible individual(s).

Recommendation and Management's Action Plan:

Recommendation #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.

Action Plan #2-1: Created separate log-ins for each user. The POYNT POS system plan was upgraded to include unlimited users. All Convention Center staff with system access now have separate accounts.

Individual or Position Responsible: Luis Ruiz, Interim Administrator – Commercial Facilities / Jose Ramirez – Events and Operations Supervisor

Estimated Completion Date: 6/29/2021