mesa·az
CITY AUDITOR
mesaaz.gov

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

AUDIT REPORT **CITY AUDITOR**

Report Date:	**August 29, 2019**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Assigned Auditors:	**Dawn von Epp and Karen Newman**

OBJECTIVES

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:

- City departments maintain and enforce 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 effectively implemented all corrective action plans developed in response to prior PCI DSS reviews.

SCOPE & METHODOLOGY

This review was focused on assessing compliance with the operational (non-IT) requirements[1] of PCI DSS, which apply to credit card handling activities at the City's 43 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*, April 2016. To accomplish our objectives, we interviewed staff members; observed operations and processes; and reviewed policies, procedures, document inventories, contract documents, and training records.

BACKGROUND

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

[1] Beginning with this year's review, we have decided to exclude PCI DSS Requirement 2.1 from our scope. This standard requires that factory default passwords be changed on Point-of-Sale devices before they are installed on the City's network. This is a technological requirement, as only IT staff would be expected to have the expertise necessary to ensure it is done. At this time, to the best of our knowledge, the City is unable to comply with this requirement, due to limitations imposed by the device vendor.

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 Information Technology Department (ITD) 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 2018 report included several recommendations, all of which have been implemented, as briefly summarized in the following table:

Recommendation	Departments	Implemented
Track and regularly inspect POS devices.	Arts & Culture Court MFMD PRCF	✓
Train Purchasing staff on PCI DSS requirements, establish controls for contracting with payment card service providers, and monitor providers annually.	Business Services	✓
Amend non-compliant contracts.	Arts & Culture MFMD	✓
Require new sites to have approved written procedures prior to operating.	Financial Services	✓
Develop procedures and submit for approval.	MFMD	✓
Do not store CVV codes for any reason.	PRCF	✓

New/Continuing Issues: While most City credit card handling operations remained PCI DSS compliant this year, we found a few locations which were not fully compliant. The current issues are summarized below; and additional details are presented in the attached Issue and Action Plans (IAPs). Some of the current issues have been identified in previous audits, although not necessarily in the same departments and/or in consecutive years. Overall, management has attempted to implement better processes to ensure continued compliance, but awareness and compliance with City policies has not been consistent. Next year's review will include follow-up testing to verify that the departments have successfully resolved the issues.

SUMMARY of ISSUES & RECOMMENDATIONS

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

   Recommendations: Financial Services should regularly remind departments that new credit card handlers must complete the training within their first 3 months. Library Services should implement a control to ensure that they comply with this requirement.

2. **Observation**: Cardholder data was not destroyed per the retention schedule.

   Recommendation: The Court should destroy all records containing cardholder data that exceeds retention schedules; and should implement a control to ensure that records are destroyed in accordance with the retention schedule in the future.

3. **Observation:** Cardholder data was being accepted via unsecured emails and faxes.

   Recommendation: The Convention Center should implement a secure process for receiving customer credit card information. Customers should be directed in the use of that process and informed that credit card numbers will not be accepted via email or fax.

4. **Observation:** Staff did not comply with PCI DSS and City requirements when engaging a payment processing service provider.

   Recommendation: City-contracted vendors should be used to process credit card payments. If the contracted vendors do not meet critical business needs, staff should consult with the Purchasing division to establish a new contract in which the vendor accepts responsibility for cardholder data.

Issue and Action Plan #1

Issue #1: Credit card training is not consistently being completed by new credit card handlers within the required time frame.

Observation: 3 of 14 new credit card handlers at Library Services did not complete credit card handling training within 3 months, as required by policy.

Criteria: PCI DSS v3.2, 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.

Recommendations and Management's Action Plans**:**

Recommendation #1-1: Financial Services should include a statement in their monthly credit card training emails, reminding departments that new credit card handlers must complete the training within 3 months of performing cardholder data handling duties.

Action Plan #1-1: Financial Services will include a statement in our monthly credit card training emails, reminding departments that new credit card handlers must complete the training within 3 months of performing the duties.

Individual or Position Responsible: Lester Smith, Sr Accountant

Estimated Completion Date: October 2019

Recommendation #1-2: Library Services should implement a control to ensure that new credit card handlers complete training within 3 months.

Action Plan #1-2: 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. 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 (Jenny Hoffman).

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.

Estimated Completion Date: September 30, 2019

Issue and Action Plan #2

Issue #2: Cardholder data was not destroyed after the retention period expired.

Observation: Municipal Court's FY 2015 records containing cardholder data were not destroyed per the retention schedule.

Criteria: PCI DSS v3.2, Requirements and Security Assessment Procedures:

- Requirement 3.1: *"Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures…"*
- Requirement 9.8: *"Destroy media when it is no longer needed for business or legal reasons…"*

AZ State Library, Archives and Public Records, General Records Retention Schedule for All Public Bodies, Schedule Number GS 1017–Financial Records, Item #10057, specifies a retention period of 3 years "*after fiscal year created or received*" for credit card records.

Comments: The retention schedule for FY 2015 records was satisfied as of July 2018; however, the Court had not destroyed them as of June 2019. The risk of unauthorized access to customers' cardholder data is increased when records are not destroyed in a timely manner.

Recommendations and Management's Action Plans**:**

Recommendation #2-1: Destroy all cardholder data that currently exceeds retention schedules.

Action Plan #2-1: To ensure that the correct destruction date is marked/labeled on every envelope that contains cardholder data/credit card tapes/information so that it is destroyed according to the retention schedule. Per Edna Ramon, Court Supervisor in Customer Service, after further review of the credit card tapes it was discovered that the envelopes in question were labeled with the incorrect destruction date. Edna Ramon and Rachel Thomas have reviewed all the envelopes to ensure that they are labeled correctly with the correct destruction date.

Individual or Position Responsible: Edna Ramon, Court Supervisor over Financial in Customer Service and Rachel Thomas, Lead Court Specialist over Financial in Customer Service.

Estimated Completion Date: As soon as Edna and Rachel reviewed the envelopes and realized that there were errors regarding the destruction dates, they relabeled the envelopes with the correct destruction dates. The relabeling was completed on Monday, 8/12/2019. ASDD, the Court's vendor for destruction of

documents/etc., is scheduled to be on site on September 9, 2019 to destroy the credit card tapes/information ready for destruction.

Recommendation #2-2: Implement a control to ensure that future cardholder data is destroyed when the retention schedule is satisfied.

Action Plan #2-2: To update the Court's Excel spreadsheet to include the information to track when the next retention period has expired to coordinate the destruction of the credit card tapes/information with the Administrative staff at the Court. With the exception of the mislabeling of the destruction dates on the envelopes containing the credit card tapes/information mentioned above, this process has been in place all along and the Court has maintained the schedule for the destruction of financial documents. The Court will continue to ensure that this tracking is in place and that the destruction occurs.

Individual or Position Responsible: Edna Ramon, Court Supervisor over Financial in Customer Service and Rachel Thomas, Lead Court Specialist over Financial in Customer Service.

Estimated Completion Date: ASDD, the Court's vendor for destruction of documents/etc., is scheduled to be on site on September 9, 2019 to destroy the credit card tapes/information ready for destruction.

Issue and Action Plan #3

Issue #3: Cardholder data was being accepted via unsecured emails and faxes.

Observation: Convention Center customers transmitted full credit card numbers to staff via fax or email; and staff did not completely and permanently delete emails containing cardholder data.

Criteria: Financial Services, Minimum Required Credit Card Handling Procedures, Cardholder, Item #12: *"Agents shall not send Cardholder Data unencrypted via email. An Information Technology Department approved encryption methods shall be used for any Cardholder Data that must be sent via email. City customers shall not be requested to supply Cardholder Data by email as a normal business practice. If any Cardholder Data is received by email, it shall be immediately transferred to an approved Processing System and purged from the City's email system."*

MP 326 Supplement, ITD Security Standard, Section 3.7.1: "*Use strong cryptography and security protocols to safeguard confidential data during transmission over private and public networks."*

Comments: When cardholder data is transmitted via unsecured email and fax, it exposes customers to an increased risk of credit card fraud.

Recommendations and Management's Action Plans**:**

Recommendation #3-1: Convention Center management should implement a secure process for receiving credit card information from customers. Customers should be directed in the use of that process and informed that credit card numbers will not be accepted via email or fax.

Action Plan #3-1: Current Action Plan: Written correspondence to clients has been revised to eliminate an area to provide credit card information. Forms that are sent to clients now include the statement "Credit card payments are only accepted in person or over the phone" and include instructions on who to call to process the payments.
Future Action Plan: The Convention Center will be initiating efforts to implement an online payment portal to accept credit card payments.

Individual or Position Responsible: PRCF Venue Operations Supervisor, TBD, and Parks, Recreation and Commercial Facilities Administrator, Dyan Seaburg.

Estimated Completion Date: Current Action Plan 08/09/2019; Future Action Plan 01/01/2020 with assistance from ITD.

Recommendation #3-2: Convention Center staff should be directed to completely purge any email which contains a full credit card number.

Action Plan #3-2: Convention Center staff has been notified that credit card information should not be transmitted via email, and if received via email , it is to be completely purged. Staff was reminded: the email should be deleted, and then should be deleted from their "deleted email" folder immediately and will be included in written processes and procedures.

Individual or Position Responsible: PRCF Venue Operations Supervisor, TBD, and Parks, Recreation and Commercial Facilities Administrator, Dyan Seaburg.

Estimated Completion Date: Completed 08/09/2019

Issue and Action Plan #4

Issue #4: Staff did not comply with PCI DSS and City requirements when engaging a payment processing service provider.

Observations:

City staff accepted a payment processing service provider's terms and conditions, which included a disclaimer of responsibility for the security of cardholder data.

Criteria:

PCI DSS v3.2, Requirements and Security Assessment Procedures, Requirement 12.8.2: "*Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer…"*

MP 212 Credit Card Handling, Section III. Policy Statement: "*…Only approved Credit Card Processing Systems shall be used for City credit card payments."*

MP 326 Supplement, Compliance Requirement Standard, Section 3.8 Outsourcing: "*Information security requirements shall be specified in contracts with third-party IT service providers, payment processors, and/or component providers.*"

Comments:

When the City allows a vendor to process credit card payments without accepting responsibility for the security of that data, the City is at an increased risk of loss in the event of a breach.

The Purchasing division has a process in place to annually verify the PCI DSS compliance status of all contracted payment processing service providers. However, Purchasing staff was unaware that this provider was being used, because there was no City contract in place.

Recommendation and Management's Action Plan**:**

Recommendation #4-1: Staff should use City-contracted providers to process credit card payments. If the contracted providers do not meet critical business needs, staff should consult with the Purchasing division to establish a new contract in which the provider accepts responsibility for cardholder data.

Action Plan #4-1: This activity is being transferred from PIO to PRCF. PRCF will work with ITD to implement the use of the ActiveNet Point of Sale module at the ice rink.

Individual or Position Responsible: Oscar Venegas, PRCF Special Events Coordinator and Tammy Davenport, PRCF Sr. Fiscal Analyst.

Estimated Completion Date: 11/30/2019