

AUDIT REPORT

CITY AUDITOR

Report Date:	May 10, 2018
Department:	Citywide
Subject:	Annual Credit Card Security Review
Lead Auditor:	Dawn von Epp, Sr. Internal Auditor

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 of PCI DSS, which apply to credit card handling activities at the City's 41 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 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 2017 report included one recommendation, which has been implemented. For additional information on that issue, please see the attached Appendix.

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. In those locations, we found issues in one or more of the following categories: training, device management, contract management, written procedures, and storage of cardholder data.

The issues found this year are summarized below; and additional details are presented in the attached Issue and Action Plans (IAPs). Some of the issues we found this year 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 the higher staff turnover in some areas tends to make consistency a challenge. Next year's review will include follow-up testing to verify that the departments have successfully resolved the issues.

SUMMARY of ISSUE & RECOMMENDATION

1. **Observation:** Staff at several locations with Point of Sale (POS) devices are not accurately recording and/or periodically inspecting those devices as required by PCI DSS.

Recommendations: Departments should create and maintain an up to date list of all card-reading devices and conduct periodic inspections.

2. **Observation:** Contracted service providers were not monitored for PCI DSS compliance in 2017. Also, 2 service provider agreements do not contain required language related to cardholder data security, and due diligence prior to engaging service providers was not always performed.

Recommendations: Provide refresher training for Purchasing staff. Establish controls to ensure due diligence occurs prior to engaging service providers and that service providers are monitored for PCI DSS compliance annually. Also, management should amend MP 200 – Purchasing Policy & Procedures and MP 356 – Delegation of Signature Authority and Agreement Approval Process, directing staff to contact Purchasing prior to contracting for a service involving credit card transactions or other access to cardholder data.

3. **Observation:** Credit card handling procedures were not developed for use by the Mesa Fire and Medical Department (MFMD) Honor Guard.

Recommendation: Prior to allowing departments to establish new credit card acceptance sites, Financial Services should ensure they have approved written procedures in place, as required by City policy. Also, MFMD should develop credit card handling procedures and submit them to Financial Services for approval.

4. **Observations:** The Convention Center occasionally stores card verification value (CVV) codes, a practice which is strictly prohibited by PCI DSS.

Recommendations: Management should ensure that the Convention Center does not store CVV codes for any reason. Also, any codes already on file should be destroyed.

Issue and Action Plan #1

Issue #1: Point of sale devices not consistently recorded and/or inspected.

Observation: The following departments did not maintain current lists of point of sale (POS) devices and/or did not perform required inspections: PRCF, Arts & Culture, Municipal Court, and MFMD (Honor Guard).

Criteria: "PCI DSS v3.2 Requirements and Security Assessment Procedures" includes following requirements (summarized):

- Requirement 9.9.1: *Maintain an up-to-date list of devices. The list should include make, model, location, and serial number (or other unique identifier).*
- Requirement 9.9.2: *Periodically inspect device surfaces to detect tampering or substitution.*

Comments: If POS devices are not recorded and inspected, tampering or substitution could go unnoticed, which would increase the potential impact of a breach.

Recommendations: The departments listed above should perform the following:

1-1. Staff should maintain an up-to-date list of POS devices, and use it when performing inspections.

1-2. Staff should conduct, and document, inspections of all card-reading devices (both swipe and chip/dip).

**Management
Responses:**

PRCF Response:

Action Plan for 1-1:

Create and verify up-to-date list of POS devices for use when performing inspections.

Individual or Position Responsible:

PRCF Sr Fiscal Analyst and Information Systems Coordinator

Estimated Completion Date: May 15, 2018 and ongoing

Action Plan for 1-2:

Staff will conduct and document inspections of all card-reading devices. This schedule will be quarterly for facilities that are open year-round. For seasonal Aquatics facilities, inspections will take

place at the beginning, mid-point and prior to the end of the season.

Individual or Position Responsible:

PRCF Sr Fiscal Analyst

Estimated Completion Date: May 31, 2018 and ongoing

Arts & Culture Response:

Action Plan for 1-1:

The Arts and Culture Department is implementing a spreadsheet with all the devices listed. The spreadsheet will have the location of the device, make, model, serial number, general condition (good, scratches etc.) the employee will then initial next to the device & date the form.

Individual or Position Responsible:

AZMNH – Sandra Williamson, i.d.e.a Museum – Jessica Kuenne

MAC – Lydia Mendoza & Kelly Farrow

Estimated Completion Date: July 1, 2018

Action Plan for 1-2:

The Arts and Culture Department will be performing inspections quarterly at each location on our card-readers and swipe devices. The inspections will be documented on a spreadsheet with the employee's signature and date of the inspection. If the employee notices anything suspicious they can notify our Fiscal Analyst, or they can also call the Fraud and Ethics hotline.

Individual or Position Responsible:

AZMNH – Sandra Williamson, i.d.e.a Museum – Jessica Kuenne

MAC – Lydia Mendoza & Kelly Farrow

Estimated Completion Date: July 1, 2018

Municipal Court Response:

Action Plan for 1-1:

Create log containing the serial numbers of POS Card Reader devices utilized at the Customer Service Windows. The log will contain the serial numbers for the devices, along with a place for court staff to indicate the date of the inspection and the name of the staff member who performed the inspection.

Individual or Position Responsible:

Court financial staff: Rosa Gracia, Dee Menchaca, Faviola Medrano, Cassey Butler and Loretta Daniels

Estimated Completion Date: January 22, 2018

Action Plan for 1-2:

Court financial staff will perform quarterly inspection of POS Card Reader devices utilized to process credit card transactions at the Customer Service Windows. The staff member will document on the POS Card Reader Log the date the inspection was completed and the staff members initials. The log will be kept in the financial room at the Mesa Municipal Court.

Individual or Position Responsible:

Court financial staff: Rosa Gracia, Dee Menchaca, Faviola Medrano, Cassey Butler and Loretta Daniels

Estimated Completion Date: April 16, 2018

MFMD Response:

Action Plan for 1-1:

Gail Coakley is maintaining an up-to-date list of POS devices that she will use when performing quarterly inspections. If new devices are purchased Gail will add them to the list and maintenance plan.

Individual or Position Responsible:

Gail Coakley, Sr. Program Assistant

Estimated Completion Date: April 1, 2018

Action Plan for 1-2:

Gail Coakley is maintaining an up-to-date list of POS devices that she will use when performing quarterly inspections. Inspections started on 4/1/18 at which time Gail conducted and documented inspections of all card-reading devices (currently one) and will do the same quarterly and log them. If more devices are purchased Gail will add them to the list and maintenance plan.

Individual or Position Responsible:

Gail Coakley, Sr. Program Assistant

Estimated Completion Date: April 1, 2018

Issue and Action Plan #2

Issue #2: Compliance with service provider requirements was inconsistent.

Observations:

With regard to contracts with external service providers:

- 2 written agreements do not contain necessary language related to the vendor's acknowledgement of responsibility for cardholder data security.
- Due diligence activities to ensure that contracted vendors have the ability to be PCI DSS compliant were only partially completed for 2 service providers, and were not completed for 2 other service providers.
- Annual monitoring of service providers for PCI DSS compliance did not occur in 2017.

Criteria:

"PCI DSS v3.2 Requirements and Security Assessment Procedures" requires the following, related to service providers:

- 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..."*
- Requirement 12.8.3: *"Ensure there is an established process for engaging service providers including proper due diligence prior to engagement."*
- Requirement 12.8.4: *"Maintain a program to monitor service providers' PCI DSS compliance status at least annually."*

Business Services "PCI DSS Compliance Policy" states:

"Specific language will be included in the solicitation documents generated by the City for services in which the respondent may store, process, or transmit customer cardholder data on behalf of the City or otherwise impact the security of the City's cardholder data environment as part of the proposed services. This language will include a statement that any applicable service provider must demonstrate their PCI DSS compliance prior to being awarded a contract with the City and must maintain their compliance throughout the term of the agreement."

Comments: Although the "PCI DSS Compliance Policy" was implemented in the Business Services Department, we found that not all Purchasing Division staff were aware of the PCI DSS language that should be included in solicitation and contract documents.

Furthermore, since there is no citywide PCI DSS compliance policy, it is even less likely that other City staff would be aware of these PCI DSS requirements when contracts are established outside of Purchasing.

Recommendations: Business Services should:

- 2-1.** Provide refresher training for Purchasing staff regarding applicable PCI DSS requirements.
- 2-2.** Establish controls to ensure due diligence occurs prior to any department contracting for a service that may involve credit card transactions or any other access to cardholder data; and to ensure that PCI DSS compliance terms are included in all such contracts. To that end, we recommend adding language to Management Policies 200 – Purchasing Policy & Procedures (possibly Section VII) and 356 – Delegation of Signature Authority and Agreement Approval Process (possibly Section VI), directing staff to contact Purchasing prior to contracting for any service that may involve credit card transactions or any other access to cardholder data.
- 2-3.** Establish a control to ensure service providers are monitored for PCI DSS compliance annually.

Arts & Culture and MFMD should:

- 2-4.** Work with Purchasing to ensure that applicable contracts are amended to add required PCI DSS language.

Management Responses:

Business Services' Response:

Action Plan #2-1:

Purchasing with the help of Tom Lavell, will look to provide refresher training specialized for our Purchasing staff.

Individual or Position Responsible:

Procurement Administrator/Matt Bauer

Estimated Completion Date: June 30, 2018

Action Plan #2-2:

Management Policy 200 and 356 will be modified to direct departments to include PCI compliance terms when credit card information will be handled or stored by vendors.

Purchasing will add standardized PCI DSS compliance language to the Standard Terms and Conditions which are part of every solicitation published by Purchasing and are referenced on every Purchase Order.

Individual or Position Responsible:

Procurement Administrator/Matt Bauer

Estimated Completion Date: August 31, 2018

Action Plan #2-3:

A table has been developed in Purchasing's Contract Management System to identify procurements that may include elements subject to PCI DSS. Applicable procurements and subsequent contracts are compiled on another table that stores the date of the last PCI verification for that contract/vendor. Each applicable contract/vendor will be verified for compliance annually. The tables will be checked and updated on at least a weekly basis.

Individual or Position Responsible:

Business Services Administration/Contracts Administration/Tom LaVell

Estimated Completion Date: May 31, 2018

Arts and Culture's Response:

Action Plan #2-4:

In the Arts and Culture Department the Performing Arts Director is working with Purchasing to ensure that our third party operating application systems are following Payment Card Industry Data Security Standard (PCI DSS), we will ensure that their contracts are up to date with the language that our policy requires (policy 326 "Information Security & Computer Usage").

Individual or Position Responsible:

Randall Vogel

Estimated Completion Date: July 1, 2018

MFMD's Response:

Action Plan #2-4:

We have been in contact with Purchasing who was not familiar with PCI DSS language. They are working with the MAII in business services, who is more familiar with special contract language to see

if they can identify what is necessary and amend the Daisy Mountain billing contract.

Individual or Position Responsible:

Business Services, Purchasing (Brandy Andersen or Tom Lavell)

Estimated Completion Date: June 1, 2018

Issue and Action Plan #3

Issue #3: Departments do not have approved credit card handling procedures.

Observation: Credit card handling procedures were not created, approved, and implemented by the Mesa Fire and Medical Department (MFMD) Honor Guard when they began accepting credit card payments.

Criteria: "PCI DSS v3.2 Requirements and Security Assessment Procedures" requires the following related to operational procedures:

- Requirement #9.9 Testing Procedure: *"Examine documented policies and procedures to verify they include maintaining a list of devices, periodically inspecting devices to look for tampering or substitution, and training personnel to be aware of suspicious behavior and to report tampering or substitution of devices."*
- Requirement #9.10: *"Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties."*

Management Policy 212 – Credit Card Handling, states:

"... Each Department and Division that accepts payments by credit card, or otherwise processes Cardholder Data, shall have an approved Credit Card Handling Procedure that incorporates all necessary Payment Card Industry Data Security Standard (PCI DSS) requirements..."

Comments: MFMD staff reported that they were not aware that departmental credit card handling procedures were required.

Recommendation:

- 3-1.** Prior to allowing departments to establish new credit card acceptance sites, Financial Services should ensure they have approved written procedures in place, as required by City policy.
- 3-2.** MFMD should develop credit card handling procedures which include all relevant PCI DSS requirements, and submit them to Financial Services for approval.

**Management
Response:**

Financial Services' Response:

Action Plan #3-1:

1. Finance Dept. will revise MP212 to require approved Credit Card Handling Procedures as a pre-requisite to establishing a new credit card acceptance site
2. Finance Dept. will enhance current monthly notification to departments of their credit card handler's training statuses to now also include current status of department's Credit Card Handling Procedures compliance.

Individual or Position Responsible:

Mary Rota – Assistant Finance Director

Estimated Completion Date: December 31, 2018

MFMD's Response:

Action Plan #3-2:

Ella Eichinger, Financial Specialist for MFMD developed credit card handling procedures and submitted them to Financial Services for approval on March 6th, 2018.

Individual or Position Responsible:

Ella Eichinger, Financial Specialist

Estimated Completion Date: April 3, 2018

Issue and Action Plan #4

Issue #4: Card verification codes were stored after authorization.

Observations: The Convention Center was storing card verification value (CVV) codes after deposit transactions were authorized, for use when processing the final transaction after the scheduled event took place.

Criteria: "PCI DSS v3.2 Requirements and Security Assessment Procedures" requires the following, related to CVV codes:

Requirement 3.2.2: *"Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization."*

Comments: Although CVV codes were only stored for cards that require the code to be entered each time the card is used, PCI DSS prohibits this practice, because the codes can be used to execute fraudulent card-not-present transactions. Non-compliance with this requirement places the both City and its customers at risk.

Recommendation: **4-1.** Management should ensure that the Convention Center does not store CVV codes for any reason. Also, any codes already on file should be destroyed.

Management Response:

Action Plan #4-1:




Staff has been informed and has confirmed understanding as to not store CVV codes for any reason. Current files have been either destroyed or permanently and completely redacted. Statement will be added to departmental Credit Card Handling procedures to the fact that the CVV codes are not to be stored for any purpose.

Individual or Position Responsible:

PRCF (Convention Center) Venue Operations Supervisor

Estimated Completion Date: May 15, 2018

APPENDIX / ACTION PLAN IMPLEMENTATION STATUS REPORT

 = Implemented  = In Progress  = Not Implemented		
2016 Recommendations & Responses		Implementation Status
CAP #1: Procedures do not meet PCI DSS requirements.		
Recommendation: 1-1. The Municipal Court should incorporate the following PCI DSS requirements into their procedures and should submit the revised procedures to Accounting Services for approval, as required by Management Policy 212: <ul style="list-style-type: none"> • Maintain an up-to-date list of devices and periodically inspect device surfaces to detect tampering or substitution. The procedures should include the steps for inspecting devices and the frequency of inspections. • Maintain an up-to-date list of roles that need access to displays of full Primary Account Numbers (PANs), along with the business need for such access. 	Implemented The Municipal Court's <i>Credit Card Handling Procedures</i> were updated on 5/22/17 and contain the requirements as recommended. The revised procedures were submitted to Accounting Services, where they were approved.	