

AUDIT REPORT

CITY AUDITOR

Report Date:	February 27, 2017
Department:	Citywide
Subject:	Annual Credit Card Security Review
Lead Auditor:	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.
- 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 32 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, 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 training 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 the PCI DSS.

In April 2016, the PCI DSS was updated to Version 3.2, which provided additional clarification and guidance on the requirements.

CONCLUSION

Prior Year Issues:

Our 2016 report included specific recommendations, which were necessary to ensure continued compliance with PCI DSS requirements. One of the action plans has been implemented, but one was still in progress at the time of this follow-up review. Additional information regarding the status of prior year action plans is presented in the attached Appendix.

New/Continuing Issues:

Overall, we found that City credit card handling operations are PCI DSS compliant. However, we found one issue that continues to warrant management's attention. The issue is summarized below; and additional details are presented in the attached Issue and Action Plan (IAP). Next year's review will include follow-up testing to verify that the department has successfully resolved the issue.

SUMMARY of ISSUE & RECOMMENDATION

Written procedures at the Municipal Court do not meet PCI DSS v3.2 requirements related to POS terminals, card swipe/dip devices, and access to Primary Account Numbers (PANs). We are recommending that the Court revise their procedures to include all requirements; and submit them to Accounting Services for approval, as required by Management Policy 212.

Issue and Action Plan

Issue #1: Procedures Do Not Meet PCI DSS Requirements

Observation: Departmental procedures at the Municipal Court as of January 2017 do not meet PCI DSS v3.2 requirements.

Criteria: "PCI DSS v3.2 Requirements and Security Assessment Procedures" requires that the following directives be contained within procedures (summarized):

- Requirement 3.3.a: A list of roles that need access to displays of more than the first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access.
- Requirements 9.9 & 9.9.2: 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.

Comments: PCI DSS v3.1 includes requirements related to procedures and training content for locations that utilize Point of Sale (POS) terminals and/or card swipe/dip devices to gather cardholder data during sales transactions. The requirements state that procedures must include a list of roles that need access to displays of full Primary Account Numbers along with the business need for such access.

Accounting Services provided these requirements to all applicable departments in 2015, and requested that they update their procedures accordingly.

During our 2016 PCI DSS review, we found that the Municipal Court had not yet updated their procedures; and, as of January 2017, they still had not done so.

Recommendation: 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:

- 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.

**Management
Response:**

Action Plan:

The Mesa Municipal Court plans on creating procedures and an inspection log on how to inspect the Point of Sale (POS) terminal.

The Mesa Municipal Court's Credit Card Handling Procedures will be updated to include a list of the roles and the business needs for issuing court ordered bond refunds processed by the Mesa Police Department (MPD). The only time the full credit card number access is utilized is with credit card bonds that were processed through the MPD.





Individual or Position Responsible:

Court Supervisor Edna Ramon is the cash custodian for the Mesa Municipal Court. Positions authorized to perform the inspection and maintain documentation are as follows:

- Court Supervisors assigned to the Customer Service Division
- Lead Court Specialists assigned to the Customer Service Division
- Court Financial Team members assigned to the Customer Service Div.

Estimated Completion Date: March 9, 2017

APPENDIX / ACTION PLAN IMPLEMENTATION STATUS REPORT

 = Implemented  = In Progress  = Not Implemented		
2016 Recommendations & Responses		Implementation Status
CAP #1: Non-compliance with credit card training requirements.		
Recommendation: 1-1. Departments with employees who handle credit cards should implement a reliable process to ensure they maintain compliance with the training requirements of Management Policy 212. 1-2. Accounting Services should track compliance with credit card training requirements and should implement a reliable process to ensure employees and supervisors are notified when they are due for annual training.	Implemented The majority of Credit Card Handlers are now current with training and Departments have implemented reliable processes to ensure they maintain compliance with the training requirements. Additionally, Accounting Services now tracks training requirements compliance and notifies employees and supervisors when they are due for annual training.	
CAP #2: Procedures and training materials require updates.		
Recommendation: 2-1. Library Services and Municipal Court should incorporate the new POS terminal and card swipe/dip device requirements into their procedures and should submit the updated procedures to the Accounting Services Division for approval, as required by Management Policy 212. 2-2. Municipal Court should include in their procedures a list of roles that need access to displays of full Primary Account Numbers (PANs) along with the business need for such access. The PAN masking requirements should also be included.	In Progress Library Services has updated their policies and procedures to include the necessary requirements. However, the Municipal Court still needs to include the new POS terminal and card swipe/dip device requirements; and also needs to include a list of roles that need access to displays of full Primary Account Numbers (PANs) along with the business need for such access.	