mesa·az
CITY AUDITOR
mesaaz.gov

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

Date: April 5, 2012

To: Audit, Finance & Enterprise Committee

From: Jennifer Ruttman, City Auditor

Subject: Annual Credit Card Security Review

Pursuant to the Council-approved Audit Plan, the City Auditor's office has completed our Annual Credit Card Security Review. The final report is attached.

Please feel free to contact me if you have any questions.

480.644.3767 (tel)
480.644.2053 (fax)

mesa·az
CITY AUDITOR
mesaaz.gov

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

FINAL REPORT **CITY AUDITOR**

Report Date: April 5, 2012
Department: Citywide
Subject: Annual Credit Card Security Review

OBJECTIVES

Our annual credit card security review is an assessment of the City's efforts to protect customers' credit card information, as required by the Payment Card Industry's Data Security Standard (PCI DSS). This review focused on the credit card handling activities that take place outside of the City's IT infrastructure. There are 24 credit card acceptance sites across various departments citywide. We conducted this review to determine whether these departments:

1. Limit the creation of sensitive paper documents (e.g., receipts, payment authorization forms, etc.) and adequately secure existing documents.
2. Use only systems and vendors that have been approved by the Information Technology Department (ITD) or Accounting Services Division to process and store sensitive information.
3. Develop specific credit card handling procedures.
4. Ensure that individuals who handle credit card information are adequately screened and trained.

SCOPE & METHODOLOGY

To accomplish our objectives, we interviewed staff members, observed operations and processes, reviewed document inventories from the City's offsite storage vendor, and reviewed attendance records for the City's credit card handling training class.

BACKGROUND

As a merchant that accepts credit cards, Mesa is required to comply with the PCI DSS. Failure to comply with this standard could result in the credit card companies levying fines or prohibiting the City from accepting credit card payments.

Since most of the PCI DSS requirements center on information technology, ITD launched a project in 2006 to bring the City into compliance. ITD adopted the PCI Security Council's prioritized approach for ensuring compliance. They have implemented the most critical requirements for protecting the City's electronic credit card data, and are now focusing on the lower priority goals. Another key department involved with ensuring PCI DSS compliance is the Accounting Services Division, which manages the City's merchant accounts, continually develops Management Policy 212 – Credit Card Handling, and trains individuals on PCI DSS requirements and credit card handling procedures.

CONCLUSION & RECOMMENDATIONS

For the protection of the City and its customers, specific findings and recommendations are not detailed in this report. However, the following is a general summary of what we found.

Since our first review in 2008, most departments have implemented our recommendations. Further, those departments that had been continuously noncompliant in prior years have significantly improved. We made some additional recommendations this year, the goal of which was to ensure that departments maintain compliance moving forward. For example:

- Credit card terminal passwords (which limit access to credit card numbers or refunds) should be periodically checked and/or changed.
- Stored documents with credit card numbers should be redacted; and should be destroyed when they reach the end of their retention period (typically 3 years).
- Vendors that handle credit card information should be fully vetted for PCI DSS compliance before they are hired.

Specific recommendations were addressed to the respective departments, and have all been accepted and implemented. We will perform this review again in one year, to ensure their implementation has been successful and sustained.