




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

Date: February 10, 2010

To: Audit and Finance Committee

From: Jennifer Ruttman, Interim City Auditor 

Subject: Credit Card Security Review

cc: Bryan Raines, Deputy City Manager
Jack Friedline, Deputy City Manager
Kari Kent, Deputy City Manager

Pursuant to the Council-approved audit plan the City Auditor's Office has completed this year's review of the City's compliance with the Payment Card Industry's Data Security Standard (PCI DSS). Our review focused primarily on day-to-day processing activities, with the purpose of assisting in the City's PCI DSS compliance efforts led by the Information Technology Department (ITD).

The final report is attached. In following with the PCI DSS requirements, we will perform this review on an annual basis.

We would like to thank each department's management and staff for their cooperation, professionalism, and assistance throughout the review process. If you have any questions please feel free to contact me at x3767 or Jason Taylor at x3635.

**City Auditor
Credit Card Security Review
Final Report
February 2010**

Scope and Objectives

The purpose of this review was to evaluate compliance with the Payment Card Industry's Data Security Standard (PCI DSS). This review focused on the credit card handling operations that take place outside of the City's IT infrastructure. There are 25 credit card acceptance sites across 11 departments citywide. We observed each of these departments' operations to determine whether they:

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

Background

As a merchant that accepts credit cards, Mesa is required to comply with the credit card security standard that has been established by the credit card industry. The PCI Security Standards Council was founded by the major payment card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc) to develop and manage a uniform set of security standards. The Security Council developed the PCI DSS, which was most recently updated in October 2008. The general requirements of the PCI DSS are as follows:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Failure to comply with the PCI DSS could result in the credit card brands levying fines or prohibiting the City from accepting credit card payments. The fines vary, depending on the merchant's size, the level of noncompliance, and the severity of related security breaches. They start at \$10,000 per month; and recent large scale, high profile breaches have drawn fines of several million dollars. Mesa processes a sizeable number of transactions (about 574,000 transactions totaling \$73.4 million in fiscal year 2009), but is still considered to be a small-to-medium sized merchant by PCI standards. Since most of the PCI DSS requirements center on information technology, ITD launched a project in 2006 to bring the City into compliance. The project was broken into several phases.

The first phases were considered to be most critical for protecting the City's electronic credit card data from a potential breach. The remaining phases are focused on other compliance issues, such as strengthening protection against internal breaches and developing various policies and procedures required by the PCI DSS. As of October 2009, ITD had finished its critical phases and begun work on the others.

Other key departments involved with ensuring PCI compliance include the Accounting Services Division and the City Auditor. Accounting Services manages the City's merchant accounts; continually develops Management Policy 212, *Credit Card Handling*; and trains individuals on the PCI DSS requirements and credit card handling procedures. Beginning last year, our office annually reviews the credit card handling operations that take place outside of the City's IT infrastructure.

Summary of Recommendations

Since last year's review, the departments that process credit cards have made a significant effort to implement our recommendations. This is especially commendable in light of the reduction in workforce that took place since that review. As a result of this effort, several risks have been successfully mitigated.

Most of the remaining recommendations should require little effort to implement. All departments have agreed to implement them, with some departments indicating that they did so immediately after the review. The general recommendations are as follows:

- 1. Continue eliminating unnecessary credit card information**—One of the tenets of the PCI DSS is that sensitive information should not be stored if it is not needed. To help minimize sensitive credit card information that needs to be protected, the Accounting Services Division has transitioned most departments' credit card terminals to models that do not display credit card numbers on merchant copy receipts.

However, most departments have receipts that were printed prior to this transition. Many of these receipts are beyond the 3 year retention period, and should be destroyed. Storing cardholder data that exceeds the retention period creates an unnecessary risk that the data could be stolen and used for fraudulent purposes.

- 2. Improve controls over remaining credit card information**—If merchants have a legitimate business need to retain sensitive credit card information (for example, to provide certain refunds), the PCI DSS requires that the merchants take various measures to protect that information. Some departments still need to improve this protection, as follows.

- **Restrict access to processing systems and reports**—Several credit card systems used by the City display sensitive information to users with a business need for the information. However, one department granted access to a few employees that do not need have a business need, and several other departments have not changed the access password from the vendor default, which could be easily guessed. Resolving these access problems will require minimal effort, provided the departments periodically review the access rights and change the passwords.
- **Implement access logging and inventory procedures**—Departments that have physically secured their sensitive credit card information onsite have generally implemented adequate

access logging and inventory procedures. However, the 4 departments storing information offsite have not. Without such controls, stolen or missing information could go unnoticed indefinitely.

- 3. Implement credit card training refreshers**—The Accounting Services Division has implemented an initial training class for individuals that handle credit cards for the City. However, the PCI DSS requires that those individuals receive refresher training and acknowledge understanding of the City’s Credit Card Handling policy (Management Policy 212) on an annual basis. The Accounting Services Division and ITD should continue their plans to implement an online application to meet these requirements.
- 4. Clarify responsibilities for managing service providers**—The City’s policies do not specify who should manage service providers that handle paper credit card documents. To ensure that credit card information remains secure when not in a merchant’s custody, the PCI DSS requires merchants to manage service providers, for example by thoroughly vetting providers before hire and requiring them to formally acknowledge responsibility for information. Most of the City’s service providers handle electronic information and are managed by ITD, in following with Management Policy 212, *Credit Card Handling*. However, two service providers currently handle paper documents. One of these providers was recently hired with significantly less due diligence than the other provider; and neither provider has formally acknowledged responsibility for credit card documents in its custody. Since the Accounting Services Division is responsible for developing Management Policy 212, it should determine which department is best suited to manage these service providers, and recommend the necessary changes to the Policy. This will help ensure consistent and thorough management of all service providers.
- 5. Develop department-specific procedures**—The one area that has not received adequate attention is the development of specific credit card handling procedures. The PCI DSS requires merchants to develop credit card security procedures to serve as “desk instructions” for employees. Failure to do so could result in employees not properly securing all sensitive information or resources, which could in turn lead to a breach. Accounting Services has communicated various security procedures in its Credit Card Handling class. However, each department should develop specific procedures that address its unique business environment.