

# **CITY AUDITOR'S OFFICE**



## **INTERNAL CONTROL REVIEW ACTIVITY REPORT DECEMBER 31, 2009**

**Report No. CAO 2900-0910-10**

**January 28, 2010**

**RADFORD K. SNELDING, CPA, CIA, CFE**

**CITY AUDITOR**

# INTERNAL CONTROL REVIEW ACTIVITY REPORT DECEMBER 31, 2009

**CAO 2900-0910-10**

## **BACKGROUND**

The City Auditor's Office has the responsibility to Evaluate, Enhance, Educate, and Enforce internal control issues that come to the Office's attention.

- **Evaluate** - The Office independently and objectively performs Internal Control Reviews to evaluate applicable internal controls through professional expertise and judgment.
- **Enhance** - After evaluation, the Office makes recommendations to enhance the adequacy and effectiveness of existing controls and further recommends additional controls as appropriate.
- **Educate** - Through the Internal Control Review Memorandums to management and the periodic Internal Control Review Activity Reports, the Office educates management and others of appropriate internal controls.
- **Enforce** - Enforcement is limited to supplying data to management to help them enforce the policies and procedures of the City.

The results of the Internal Control Reviews are reported in two steps:

- An Internal Control Review Memorandum is released to the appropriate levels of management and the Mayor and City Council. This Memorandum assists management in the timely correction of control deficiencies.
- Semiannually, a summary report is made of all findings and recommendations from the Internal Control Review Memorandums and released in a *formal Internal Control Review Activity Report*.

This report summarizes the Internal Control Review Memorandums issued since the last Internal Control Review Activity Report (June 30, 2009), including findings, recommendations, and management responses. The recommendations are included in the follow-up system for tracking purposes.

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**OBJECTIVES**

Our objectives in completing the *Internal Control Review Activity Report* are to:

- Review all activity for the period noted relative to internal control reviews;
- Document for tracking purposes findings and recommendations noted in Internal Control Review Memorandums; and
- Report to the public the results of activities of the City Auditor's Office.

The objectives of each of the Internal Control Reviews were to:

- Determine the adequacy of existing internal controls;
- Determine the reason(s) for any control failure;
- Recommend corrective action; and
- Report the results of our review.

**SCOPE AND METHODOLOGY**

The scope of the audit was limited to Internal Control Review Memorandums issued from June 30, 2009 through December 31, 2009.

The scope of our work on internal control was limited to the controls within the context of the objectives and the scope of each Internal Control Review.

Our audit methodology during each of the Internal Control Reviews included:

- Observing operations.
- Interviewing personnel.
- Reviewing records, reports, and other applicable documentation.

We conducted this performance audit in accordance with generally accepted government auditing standards except for the requirement for an external peer review every three years. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**INTERNAL CONTROL MEMORANDUMS ISSUED**

**1. ICR-051 - Internal Control Review: Municipal Court – ASED Fraud**

**Background**

On June 27, 2008 Detention and Enforcement (D&E) responded to a report of a theft by an ASED court clerk of \$462. The following information was gathered:

- ASED oversees a program where defendants can satisfy court fines through payments or community work hours.
- On June 25, 2008, a customer paid court fines of \$462 using a credit card.
- The court clerk who processed this transaction knowingly failed to write the corresponding case number on the credit card receipt.
- The court clerk subsequently stole \$462 in cash from the day's deposit.
- In order for the court clerk's deposit to balance in total at the end of the day, rather than identifying that this customer had paid off the fines by payment, the court clerk made it appear that the customer had worked off his fines by reducing the required work hours.
- The customer was unaware of the court clerk's actions.

D&E is proceeding with the District Attorney's office in the prosecution of the court clerk.

**Findings and Conclusions:**

The ASED court clerks collect payments and process court ordered work hours as a part of their daily tasks. ASED is currently using several disconnected systems for these tasks that do not allow for easy reconciliation of the different transaction types. With the use of these multiple systems, an opportunity currently exists for schemes such as this one to go undetected.

**Recommendation:**

The following recommendations are made:

1. Municipal Court management should conduct random surprise audits of each clerk's daily deposits.
2. Municipal Court management should request that work hours documentation be included with the daily cash receipts to account for all hours either being paid or reduced through the work program.
3. Municipal Court management should request that the CMS developer accelerate the completion of the module to correct the possible flaws in the current method of balancing daily deposits.

**Recommendation 1:**

Municipal Court management should conduct random surprise audits of each clerk's daily deposits.

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**Recommendation 2:**

Municipal Court management should request that work hours documentation be included with the daily cash receipts to account for all hours either being paid or reduced through the work program.

**Recommendation 3:**

Municipal Court management should request that the CMS developer accelerate the completion of the module to correct the possible flaws in the current method of balancing daily deposits.

**2. ICR-052 - Internal Control Review: Credit Card Fraud at Bryan Safekey**

**Background**

A Safekey employee who was a cashier at the Richard Bryan Elementary School Safekey site was arrested by Detention and Enforcement (D&E) for credit card fraud. This employee allegedly used personal credit card information of a Safekey customer to purchase pizza, pay cell phone and dental bills, and make various online purchases. The Safekey employee made a voluntary statement admitting to the fraudulent use of several Safekey customers' credit cards. D&E is pursuing prosecution of the suspect on violations of NRS #205.463 (identity theft) and NRS #205.690 (possession of credit card without owner's consent).

**Findings and Conclusions:**

Safekey uses a form known as the *City of Las Vegas Safekey Manual Credit Card Authorization Form* to manually record customer credit card information (i.e., type of card, credit card number, and amount charged, card security code, expiration date, printed name on card) and to obtain the customer's signature. A pencil tracing of the credit card is made on this form. Safekey cashiers at sites with laptops input the credit card number into the Class System.

The manual forms are submitted weekly to the Safekey administration offices where the Safekey supervisors process the credit card charges on credit card machines. The manual credit card form is retained at the Safekey administration offices. Personal information on the manual credit card form is not currently redacted after processing the transaction.

While it is challenging to protect the City and customers against the acts of dishonest employees, the security and safeguards over credit card processing must continually be evaluated to minimize the risk of this type of fraud and deter employees from misusing the personal information they obtain in the course of their duties.

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**Recommendations:**

Safekey management should implement the following measures to improve the security over credit card payments:

1. After processing the credit card payments, personal information on manual credit card forms should be redacted (i.e., the security code, the expiration date, and all but the last four digits of the credit card number).
2. Personal information on manual credit card forms currently being stored should be redacted (i.e., the security code, the expiration date, and all but the last four digits of the credit card number).
3. Safekey employees should sign a confidentiality agreement indicating they will safeguard all personal data obtained in the course of their duties.
4. Credit card documentation should always be stored in a secure location.
5. The adequacy of the security over personal information contained in the Class electronic files should be evaluated.
6. Increased automation should be used in processing credit card payments and personal credit card information should no longer be recorded on manual forms. The credit card information stored electronically should be protected with access controls and encryption.

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**MANAGEMENT RESPONSES  
TO  
INTERNAL CONTROL REVIEW ACTIVITY REPORT**

**1. ICR-051 - Internal Control Review: Municipal Court – ASED Fraud**

**Recommendation 1:**

Municipal Court management should conduct random surprise audits of each clerk's daily deposits.

**Management Response**

In September 2008, the accounting unit implemented a random/targeted audit program. All administrative errors, omissions, as well as any cash discrepancies are tracked and reported to ASED management. The unit went back to the beginning of the fiscal year and the goal is to complete roughly one every two working days or 150 audits per year. Additionally, we have added this to our internal performance plus measures and we are on track to meeting our goal for this fiscal year. All documentation is currently filed in the Budget Analyst's office at Municipal Court. This is an additional but necessary task that has been added to the amount and complexity of the unit's responsibilities.

**Estimated Date of Completion:** Completed

**Recommendation 2:**

Municipal Court management should request that work hours documentation be included with the daily cash receipts to account for all hours either being paid or reduced through the work program.

**Management Response**

In September 2008, the accounting unit changed the daily deposit form to include "work program hours worked" and started to collect all work program timesheets. An automated report was created to track total work hours rung by clerk and that report is reconciled to the work program timesheets by the accounting unit daily. All administrative errors, timesheet omissions, as well as any cash calculation discrepancies are tracked and reported to ASED management on a daily basis. All documentation is currently filed in the Budget Analyst's office at Municipal Court. This is an additional but necessary task that has been added to the amount and complexity of the unit's responsibilities.

**Estimated Date of Completion:** Completed

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**Recommendation 3:**

Municipal Court management should request that the CMS developer accelerate the completion of the module to correct the possible flaws in the current method of balancing daily deposits.

**Management Response**

IT management met with the CMS developer and they have established a timeline of which we are scheduled to train court staff in April 2009. We are expected to implement the new CMS in August 2009.

**Estimated Date of Completion:** August 2009

**2. ICR-052 - Internal Control Review: Credit Card Fraud at Bryan Safekey**

**Recommendation 1:** After processing the credit card payments, personal information on manual credit card forms should be redacted (i.e., the security code, the expiration date, and all but the last four digits of the credit card number).

**Management Response:**

Management will redact all personal information on manual credit cards forms processed in our program.

**Estimated Date of Completion:** January 5, 2009

**Recommendation 2:** Personal information on manual credit card forms currently being stored should be redacted (i.e., the security code, the expiration date, and all but the last four digits of the credit card number).

**Management Response:**

Management will have staff redact all existing manual credit card forms that are currently being stored.

**Estimated Date of Completion:** January 5, 2009

**Recommendation 3:** Safekey employees should sign a confidentiality agreement indicating they will safeguard all personal data obtained in the course of their duties.

**Management Response:**

Management will have all current and future Safekey staff members sign a confidentiality agreement form stating that they will safeguard all personal data obtained.

**Estimated Date of Completion:** January 5, 2009

**INTERNAL CONTROL REVIEW  
ACTIVITY REPORT  
DECEMBER 31, 2009  
CAO 2900-0910-10  
January 28, 2010**

**Recommendation 4:** Credit card documentation should always be stored in a secure location.

**Management Response:**

Management will take steps to make sure that all credit card documents are stored in a safe locked location.

**Estimated Date of Completion:** January 5, 2009

**Recommendation 5:** The adequacy of the security over personal information contained in the Class electronic files should be evaluated.

**Management Response:**

Management will have periodic meetings with the Class systems administrator to evaluate the adequacy of the security of information in the system.

**Estimated Date of Completion:** January 5, 2009

**Recommendation 6:** Increased automation should be used in processing credit card payments and personal credit card information should no longer be recorded on manual forms. The credit card information stored electronically should be protected with access controls and encryption.

**Management Response:**

Management plans to purchase electronic credit card machines that will encrypt the card information thus making it safer to use our program.

**Estimated Date of Completion:** January 5, 2009