CITY AUDITOR'S OFFICE

AUDIT OF OFFICE OF STRATEGIC SERVICES

CUSTOMER CARE CENTER
FINANCIAL OPERATIONS

Report SS001-2122-02

March 23, 2022

RADFORD K. SNELDING, CPA, CIA, CFE

CITY AUDITOR

TABLE OF CONTENTS

AUDIT OF OFFICE OF STRATEGIC SERVICES
CUSTOMER CARE CENTER
FINANCIAL OPERATIONS
Report SS001-2122-02

BACKGROUND

The Office of Strategic Services (Strategic Services) oversees the operation of the city's Customer Care Center. The Customer Care Center is a centralized operation where citizen calls are initially directed and where citizens can make various types of payments (e.g. sewer bills, parking citations, pet license fees, code enforcement fines, business licensing fees, building and permit fees).

The Customer Care Center was opened in March 2020. The Customer Care Center is managed by the Strategic Initiatives Manager and Administrative Officer. There are three Senior Call Center Specialists and seven Call Center Specialists within the Customer Care Center. In addition to other responsibilities, four of the Call Center Specialists are cashiers and they process payments from customers using seven different systems.

OBJECTIVES

Our audit objectives were to review the financial operations of the Customer Care Center and determine whether:
- Customer Care Center is complying with the city's cash handling policies and procedures.
- Payments made at the Customer Care Center are being accurately processed, balanced, and recorded to the respective systems.
- Customer Care Center deposits are being properly prepared, remitted to the armored car service, reconciled to the bank records, and posted to the general ledger.
- Cash box keys being used by the Customer Care Center are properly secured during business hours and after hours.
- Combinations to the safes being used by the Customer Care Center are provided only to appropriate personnel and the combinations are being changed in accordance with city policy.
- Access to the doors of the non-public areas of the Customer Care Center are appropriately restricted.
- System access permissions assigned to the Customer Care Center personnel are appropriate for their job responsibilities.

SCOPE AND METHODOLOGY

The scope of our work was limited to the management controls within the context of the audit objectives and scope of the audit. The last date of fieldwork was February 3, 2022.

Our audit methodology included:
- Observations of the Customer Care Center financial operations.
- Interviews with Customer Care Center management and staff.

- Review of a sample of payment transaction documentation.
- Review of card key access reports.
- Review of system access permissions.

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 reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

The following findings and conclusions to our audit objectives were noted:

Objective 1: *Determine whether the Customer Care Center is complying with the city's cash handling policies and procedures.*

Our audit identified areas of non-compliance with the city's cash handling policies and procedures. See Finding #1.

Objective 2: *Determine whether payments made at the Customer Care Center are being accurately processed, balanced, and recorded to the respective systems.*

Our audit included testing a sample of payments made at the Customer Care Center during fiscal year 2021. We found that payments are being accurately processed, balanced, and recorded to the respective systems.

Objective 3: *Determine whether Customer Care Center deposits are being properly prepared, remitted to the armored car service, reconciled to the bank records, and posted to the general ledger.*

Our audit included testing a sample of deposits prepared by the Customer Care Center during fiscal year 2021. We found that deposits are being properly prepared, remitted to the armored car service, reconciled to the bank records, and posted to the general ledger.

Objective 4: *Determine whether cash box keys being used by the Customer Care Center are properly secured during business hours and after hours.*

Our audit found that a cashier was not always locking their cash drawer when it was unattended. See Finding #1.

Objective 5: *Determine whether combinations to the safes being used by the Customer Care Center are provided only to appropriate personnel and the combinations are being changed in accordance with city policy.*

Our audit found that management is not maintaining a record of all staff with access to the safes and the dates of safe combination changes. In addition, the safe combination change records from the city locksmith are not being retained. See Finding #1.

Objective 6: *Determine whether access to the doors of the non-public areas of the Customer Care Center are appropriately restricted.*

Our audit found that the number of badges with access to the Customer Care Center office along with the hours of access may be excessive. In addition, there are generic badges (i.e., not assigned to a specific individual) with access to the office that increase the risk of unauthorized access without accountability. See Finding #2.

Objective 7: *Determine whether system access permissions assigned to the Customer Care Center personnel are appropriate for their job responsibilities.*

Our audit found:
- The Customer Care Center cashiers were found to have different access permissions for certain systems despite having the same roles and responsibilities.
- The access permissions of certain employees who transferred into the Customer Care Center from other city departments were not changed before starting their new jobs.
- The access permissions of certain employees are not compatible with their current job responsibilities. See Finding #3.

Further information on these issues is contained in the following sections. While other issues were identified and discussed with management, they were deemed less significant for reporting purposes.

Contributors to this report included:

Radford K. Snelding, CPA, CIA, CFE
City Auditor

Bryan L. Smith, CPA, CFE
Internal Audit Section Manager

James Burnett, CIA
Senior Internal Auditor

Louis Hlad, CISA
Senior IT Auditor

1. CASH HANDLING POLICIES COMPLIANCE

Criteria

The city's Cash Handling Policy/Procedure (FN302) states the following:

- *A Department Director whose department receives cash shall:*
  - *Ensure that the department has written cash handling procedures that are consistent with the city's cash handling policy/procedure. (1a)*
  - *Ensure that cash handling procedures are followed (1d)*
- *All cash collections, regardless of amount, shall be deposited intact within 24 hours. (3g)*
- *Money stored in drawers, desks, and filing cabinets must be locked when left unattended. (4b)*
- *Combinations for department safes shall be changed annually or when an employee with safe access separates from employment.*
  - *i. The combination shall be restricted to the department director, or designee.*
  - *ii. A log shall be kept of all people with access to the safe and when the safe combination was last changed.*
  - *iii. The invoice from the locksmith shall be kept as backup. (4e)*
- *Department procedures must provide for periodic audits of all cash handling locations and field collections. The results of these audits must be reported to the Finance Department, Accounting Operations Manager. Major exceptions must be reported to the Director of Finance and City Auditor. (4f)*

The city's Personal Check Acceptance Policy/Procedure (FN304) states the following:

- *The department, division, or office cashier is responsible for ensuring compliance with the city's check acceptance policy and procedure.*
- *The city requires presentation of a driver's license when accepting payments by personal check. If a driver's license is not available, two forms of identification are required, at least one with a picture ID.*
- *For in-person payments, ask for photo identification and write the ID number on the check.*
- *Preventive measures to fight check fraud include, but are not limited to displaying signs at all payment receipting areas showing the city's joint effort with the Clark County District Attorney's Office to minimize the number of bad checks.*

The city's Petty Cash and Change Funds Policy/Procedure (FN305) states the following:

- *Restricted access to the drawer or location must be maintained, and should be limited to the fund custodians and the Department Director, or designee. (B3)*

Audit of Office of Strategic Services
Customer Care Center
Financial Operations
SS001-2122-02
March 23, 2022

Condition

During our audit of the Customer Care Center we identified the following areas of non-compliance with city cash handling policies and procedures:

- Each day's deposits are picked up the following business day by an armored car carrier service. Friday's deposits are held in a safe until Monday or the next business day in the case of a holiday. Therefore, the Customer Care Center is not in compliance with city policy requiring that "all cash collections, regardless of amount, shall be deposited intact within 24 hours."
- A cashier was found to not always be locking their cash drawer when it was unattended.
- Customer Care Center management is not maintaining a record of all staff with access to the Customer Care Center safes and the dates of safe combination changes. In addition, safe combination change documentation from the city locksmith is not being retained as required by policy.
- The Customer Care Center's office procedures do not address the check acceptance requirements found within the city's Personal Check Acceptance Policy and Procedure (FN304) and the staff are not fully complying with these requirements. For example, cashiers are not verifying and documenting the identification of customers paying with personal checks and checks are not being endorsed. In addition, the required fraud prevention signage is not displayed.
- Strategic Services management is not conducting periodic cash handling audits of the Customer Care Center as required by policy.

Cause

- Lack of awareness of all city cash handling policies and procedures by management and staff.
- Documented office procedures do not address all applicable city cash handling policies and procedures.

Effect

- Non-compliance with city cash handling policies and procedures.
- Increased risk of loss.

Recommendations

1.1   Strategic Services management should consult with Finance on how the Customer Care Center can comply with the city's requirement that all cash collections be deposited within 24 hours.

1.2   Strategic Services management should require Customer Care Center staff to lock their cash drawers when unattended and document and implement procedures to periodically verify this is being done.

1.3   Strategic Services management should maintain records of all staff with access to the Customer Care Center safes and the dates of safe combination changes along with supporting documentation from the city locksmith. Management should also document and implement procedures to have the combinations to the safes changed in accordance with city policy.

1.4   Strategic Services management should have Customer Care Center staff fully implement the city's personal check acceptance procedures. Management should incorporate these procedures into the office's documented procedures.

1.5   Strategic Services management should develop, document, and implement the completion of periodic cash handling audits of the Customer Care Center in accordance with city policy. Management should also provide periodic training to the Customer Care Center staff on cash handling policies and procedures.

2. CUSTOMER CARE CENTER OFFICE ACCESS

Criteria

The city's Cash Handling Policy/Procedure (FN302) states the following:

- *Cash handling areas must have restricted access. (4a)*

Condition

Entry into the Customer Care Center office space is controlled by three electronic badge access restricted doors. We reviewed a report listing individuals with access to these doors as of July 12, 2021 and access activity reports during the period from March 1, 2021 through August 31, 2021 and noted the following:
- There are 293 badges with access to the Customer Care Center office. All of these badges except three have 24-hour access to the Customer Care Center office. The Operations and Maintenance and Information Technologies departments have 66 and 32 employees, respectively, with badge access to the Customer Care Center. The number of badges with access to the Customer Care Center office, as well as the 24-hour access may be excessive.
- The city's janitorial service contractor has 40 generic access badges (i.e., not assigned to a specific individual) to the Customer Care Center office. These generic badges increase the risk of unauthorized access without accountability.

Cause

- Strategic Services management is not periodically obtaining and reviewing badge access and access activity reports for inappropriate or unusual access to the Customer Care Center office area.

Effect

- Risk of access to the Customer Care Center office area by unauthorized individuals.

Recommendations

2.1   Strategic Services management should document and implement procedures to periodically obtain and review electronic badge access reports from the Department of Public Safety and evaluate the appropriateness of those with access to the Customer Care Center office and their hours of access.

2.2   Strategic Services management working with city management should evaluate whether the generic badges with access to the Customer Care Center office could be assigned to individuals or controls could be implemented surrounding these badges to allow for improved accountability.

3. SYSTEM ACCESS PERMISSIONS

Criteria

The city's Information Security Roles & Responsibilities Policy (IT 134b) states the following:

Department Managers and Supervisors will:
- *Ensure that all staff under their guidance is aware of the need to properly protect our information and resources.*
- *Determine the sensitivity and criticality of the customer information and records for which they are responsible.*
- *Determine who will be permitted to access their information, and the uses to which this information will be put. Any sharing of non-public information with external entities must be carefully scrutinized and documented.*
- *Approve end-user access to their data and performing periodic reviews of access rights.*

Governmental standards for internal controls state the following:

Management designs control activities to limit user access to information technology through authorization control activities such as providing a unique user identification or token to

authorized users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other control activities to promptly update access rights when employees change job functions or leave the entity. Management also designs control activities for access rights when different information technology elements are connected to each other.

Condition

The Customer Care Center cashiers use seven different systems to process customer payments for other departments. We obtained and reviewed the system access permissions of the Customer Care Center staff within these systems and discussed these permissions with the respective system administrators. We noted the following:

- The Customer Care Center cashiers were found to have different access permissions for certain systems despite having the same roles and responsibilities.
- The access permissions of certain employees who transferred into the Customer Care Center from other city departments were not changed before starting their new jobs.
- The access permissions of certain employees are not compatible with their current job responsibilities.

Cause

- Strategic Services management relied on the respective system administrators to provide their staff with the appropriate system access permissions with the opening of the Customer Care Center.
- Strategic Services management is not performing periodic reviews of their employees' access rights as required by policy.

Effect

- Potential for processing of unauthorized transactions without detection.

Recommendations

3.1 Strategic Services management working with system administrators, department management, and Information Technologies should review the appropriateness of the current system access permissions of the Customer Care Center employees and make changes as needed.

3.2 Strategic Services management should document and implement procedures to:
- Alert system administrators when an employee's job responsibilities change and evaluate whether changes are needed to their system access permissions.

- Periodically review the system access permissions of the Customer Care Center employees to ensure they are compatible with their current job responsibilities.

3.3   Strategic Services management should establish and document compensating monitoring controls for systems whose access permissions cannot be adequately restricted to prevent cashiers from performing unauthorized transactions.

MANAGEMENT RESPONSE

1.   Cash Handling Policies Compliance

1.1   Strategic Services management should consult with Finance on how the Customer Care Center can comply with the city's requirement that all cash collections be deposited within 24 hours.

Management Action Plan: Strategic Services will consult with Finance to review the cash handling policy in regards to the daily deposit requirement. The revised policy will factor in the operations needs of the Customer Care work unit.

Estimated Date of Completion: 10/01/2022

1.2   Strategic Services management should require Customer Care Center staff to lock their cash drawers when unattended and document and implement procedures to periodically verify this is being done.

Management Action Plan: The Customer Care Center will implement desktop procedures to outline proper cash handling procedures. Periodic audits will be conducted to ensure policies are being adhered to.

Estimated Date of Completion: 7/1/2022

1.3   Strategic Services management should maintain records of all staff with access to the Customer Care Center safes and the dates of safe combination changes along with supporting documentation from the city locksmith. Management should also document and implement procedures to have the combinations to the safes changed in accordance with city policy.

Management Action Plan: Strategic Services will implement desktop procedures to require a safe log is documented with a list of employees with access is maintained. The requirement stipulates at a minimum the combination is changed annually or when there is a change in staff within the work unit.

Estimated Date of Completion: 7/1/2022

1.4   Strategic Services management should have Customer Care Center staff fully implement the city's personal check acceptance procedures. Management should incorporate these procedures into the office's documented procedures.

Management Action Plan: Strategic Services will consult with Finance to review the Cash Handling Policy in regards to personal check acceptance. The current requirements in the policy are antiquated and will be modified to reflect industry standards.

Estimated Date of Completion: 10/1/2022

1.5   Strategic Services management should develop, document, and implement the completion of periodic cash handling audits of the Customer Care Center in accordance with city policy. Management should also provide periodic training to the Customer Care Center staff on cash handling policies and procedures.

Management Action Plan: Strategic Services will implement a periodic cash handling audit process to ensure compliance with the desktop procedures and the Finance cash handling policy.

Estimated Date of Completion: 10/1/2022

2.   Customer Care Center Office Access

2.1   Strategic Services management should document and implement procedures to periodically obtain and review electronic badge access reports from the Department of Public Safety and evaluate the appropriateness of those with access to the Customer Care Center office and their hours of access.

Management Action Plan: Strategic Services has obtained a listing of all individuals with badge access to the Customer Care Center. Access has been reviewed and individuals have been deactivated that no longer need access. Reviewing access will be documented in the desktop procedures.

Estimated Date of Completion: 7/1/2022

2.2   Strategic Services management working with city management should evaluate whether the generic badges with access to the Customer Care Center office could be assigned to individuals or controls could be implemented surrounding these badges to allow for improved accountability.

Management Action Plan: Strategic Services has obtained a list of badge holders who have access to the Customer Care office. Badge holders who are non-essential have been removed.

Estimated Date of Completion: Complete

3.   System Access Permissions

3.1   Strategic Services management working with system administrators, department management, and Information Technologies should review the appropriateness of the current system access permissions of the Customer Care Center employees and make changes as needed.

Management Action Plan: Strategic Services will consult with Finance and Information Technologies to develop a process to conduct periodic access reviews of all customer care staff for all applications. Information Technologies is in the process of reviewing all policies and procedures which deal with provisioning/deprovisioning, access reviews across the organization.

Estimated Date of Completion: 10/1/2022

3.2   Strategic Services management should document and implement procedures to:
- Alert system administrators when an employee's job responsibilities change and evaluate whether changes are needed to their system access permissions.
- Periodically review the system access permissions of the Customer Care Center employees to ensure they are compatible with their current job responsibilities.

Management Action Plan: Strategic Services will develop desktop procedures to encompass the on-boarding process of establishing the appropriate permission levels.

Estimated Date of Completion: 7/1/2022

3.3   Strategic Services management should establish and document compensating monitoring controls for systems whose access permissions cannot be adequately restricted to prevent cashiers from performing unauthorized transactions.

Management Action Plan: Strategic Services will consult with Finance and Information Technologies to establish controls to verify unauthorized transactions are not being performed.

Estimated Date of Completion: 10/1/2022