Council Auditor's Office

Follow-Up on Electronic Fund Transfers In Audit

November 7, 2023

Report #856A

117 West Duval Street Jacksonville, Florida 32202-3701 Telephone (904) 255-5500 Fax (904) 255-5478
www.coj.net

OFFICE OF THE COUNCIL AUDITOR
Suite 200, St. James Building

November 7, 2023 Report #856A

Honorable Members of the City Council
City of Jacksonville

The purpose of this report is to document our follow-up review of our past report #856, Electronic Fund Transfers In Audit, and to determine whether corrective action has been taken in response to our findings and recommendations. We are providing this special written report in accordance with Ordinance Code Section 102.102. This report does not represent an audit or attestation conducted pursuant to Government Auditing Standards. The initial audit report can be found on our website.

We sent a follow-up letter to Brian Hughes, Chief Administrative Officer on February 22, 2023 inquiring as to the status of the original audit report recommendations. We reviewed the recommendations from our audit report, the auditees' responses to the recommendations, and the auditees' responses to our follow-up letter. We then performed limited testing to verify responses.

Based on the responses received and our follow-up testing, a table detailing the original number of issues noted and the number of issues resolved as of this follow-up is included below.

Types of Issues	Original Number of Issues	Issues Cleared	Remaining Issues
Internal Control Weaknesses	0	0	0
Findings	6	4	2
Opportunities for Improvement	0	0	0
Total	**6**	**4**	**2**

The following is a brief summary of the remaining issues with responses from the Finance and Administration Department.

Finding 1 * Deposits Not Always Recorded Timely in the Financial System*

In the original audit, we identified issues with the timing of when transactions were being recorded in the City's financial system. Out of 643 deposits tested, 392 (or 61.0%) were recorded in the City's financial system over 15 days from the date the payments were deposited at the bank. We were also not able to find when or if an additional 127 of the 643 (or 19.8%) deposits tested were even input into the City's financial system.

During the follow-up we noted that 12 out of 30 (or 40%) deposits tested were not recorded within 15 days of the date the electronic fund transfer was recorded in the bank. Of the 12 deposits not recorded within 15 days, 4 deposits were not recorded within 30 days. However, we were able to confirm that all of the deposits selected for testing were ultimately recorded in the system.

We continue to recommend that the Accounting Division and the Treasury Division implement procedures to ensure that the electronic fund transfers in are recorded in the City's financial system in a timely manner.

Treasury Division Response to the Follow-Up of Finding 1

Agree ☒ Disagree ☐ Partially Agree ☐

Treasury and Accounting have continued to regularly meet to resolve outstanding issues relating to deposits that haven't been recorded in 1Cloud. While we think there have been many improvements in the receipting process, we agree there is room for additional process improvements and will continue to implement and refine procedures to ensure the timely recording of receipts.

Additionally, we are evaluating projects related to incoming deposits that could further improve the process; for example, the evaluation of which deposits could be redirected to the Tax Collector's office.

Supplemental Finding 2 *User Accounts of Terminated Employees Not Deactivated*

In the original audit, we reviewed the list of users with access to the City's new Enterprise Resource Planning System (also referred to as ERP System and includes the City's financial system), used by the City. We found a total of 331 user accounts belonging to terminated employees were still active in the system. Per the City's Information Technology Division (ITD), the only way to log into the system is through single sign on, by using a valid Active Directory account. Per ITD, upon termination, these employees accounts were disabled in the Active Directory by ITD's Security Team. Even though terminated employees were removed from the Active Directory, these employees could be re-hired and their single sign on restored, which could unintentionally grant access to systems that the re-hired employee might not need. We confirmed at the time of the original audit that the 331 user accounts belonging to terminated employees were disabled after we notified ITD.

During this follow-up we found 315 user accounts belonging to terminated employees or contractors were still active in the ERP System.

We continue to recommend that user access be deactivated at the system level for all terminated employees. This additional layer of defense will prevent unauthorized access to a specific system when the single sign on of a terminated employee is restored or compromised. We additionally recommend that ITD work with the applicable system owners (e.g., Procurement for the Procurement Module) to facilitate quarterly access rights verification with using departments to confirm that access rights are appropriate for personnel in the area and the separated and transferred employees have had access appropriately removed.

Information Technology Division Response to the Follow-Up of Supplemental Finding 2

Agree ☐ Disagree ☐ Partially Agree ☒

For systems which use single sign-on, such as 1Cloud, the user loses access to the system whether onsite or remote when their Active Directory account is deactivated.

Security deactivates 1Cloud user accounts as part of the employee separation workflow. In addition, there is a daily automated report that compares terminated employees to active users in 1Cloud, so that any discrepancy can be remedied. ITD's process for a departing employee includes removing 1Cloud roles/permissions. If a previous employee returns to City employment, they have no default 1Cloud roles/permissions and must go through the approval process to be granted appropriate roles/permission for their new position.

For external users such as auditors and contractors, ITD is dependent upon the Department that submits an external user access request to provide notification when that access is no longer required. In order to mitigate the risk of notification failure, ITD will limit external user and contractor 1Cloud access to the term of the engagement, i.e. 90 days, 6 months, or 1 year.

In addition, ITD will consult with Oracle and with other municipalities using Oracle Fusion Cloud ERP to benchmark best practices for account security and implement those findings in FY2023-2024.

We would like to thank the Finance and Administration Department for their cooperation in conducting this follow-up review.

Respectfully submitted,

Kim Taylor

Kim Taylor, CPA
Council Auditor