



Council Auditor's Office

Follow-Up on Electronic Fund Transfers In Audit

March 18, 2026

Report #856B

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



March 18, 2026

Report #856B

Honorable Members of the City Council
 City of Jacksonville

The purpose of this report is to document our second 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 and follow-up report can be found on our website.

We sent a follow-up letter to the City’s Deputy Chief Administrative Officer on July 11, 2025, inquiring as to the status of the original audit report recommendations after the first follow-up report. We reviewed the recommendations from our audit report and previous follow-up report, the auditees’ responses to the recommendations, and the auditees’ responses to our follow-up letter. We then performed limited testing to verify the 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 reasonably resolved as of this follow-up is included below.

Types of Issues	Original Number of Issues	Issues Cleared Prior to This Follow-up	Remaining Issues Prior to This Follow-up	Issues Cleared During This Follow-up	Remaining Issues
Internal Control Weaknesses	0	0	0	0	0
Findings	6	4	2	0	2
Opportunities for Improvement	0	0	0	0	0
Total	6	4	2	0	2

The following is a brief summary of the remaining issues with responses from the Finance Department and the Technology Solutions Department that we received on March 13, 2026.

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

In the original audit, we identified issues with the timing of when deposits that are not processed by the Tax Collector’s Office (e.g., payments sent directly to the Treasury Division) 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 City’s 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 first 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 City’s 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 the deposits selected for testing were ultimately recorded in the system.

We were unable to confirm if 45 out of 62 (or 72.6%) deposits tested, which total \$478,459, had been recorded in the City’s financial system. These 45 transactions had an “unreconciled” status, which suggests they had not been recorded for an average of 169 days after the close of the month as of the date of testing on October 16, 2025. We did note that for the 17 deposits and associated journal entries that we were able to identify, we found no timeliness issues. However, it appears there are still significant issues with the timeliness of recording deposits in the City’s financial system, which is related to untimely bank reconciliations.

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 as part of a timely bank reconciliation process.

Treasury Division Response to the Follow-Up of Finding 1

Agree Disagree Partially Agree

We agree that deposits have often not been recorded to the City's financial system in a timely fashion. The Accounting and Treasury Departments are working to establish procedures to ensure timely recognition of all cash transactions. To that end, a monthly bank reconciliation routine will be instituted within the current fiscal year.

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, at the time, 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 the first follow-up, we found 315 user accounts belonging to terminated employees or contractors were still active in the ERP System.

During this second follow-up, we found potential issues with 469 user accounts. Of the 469 user accounts, 388 accounts were locked accounts (prevents use) with read-only access. Based on these user accounts being locked with only read-only access, we cleared these items. We did find issue with the remaining 81 user accounts as noted below:

- 59 active “unlocked” user accounts were associated with terminated employees or contractors. Furthermore, we found that 17 of these 59 users accounts appear to have access rights that enable them to make changes in the system. In other words, these 17 users have more than read-only access to the City’s financial system.
- 22 user accounts were locked accounts with more than read-only access. Since their access was more than read-only, if they returned to employment and the accounts were unlocked, there is an increased risk they could have inappropriate access.

While there may be some improvements, 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 Technology Solutions Department (formerly known as ITD) work with the applicable system owners (e.g., Procurement for the Procurement Module) to facilitate quarterly access rights verification by 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.

Technology Solutions Department Response to the Follow-Up of Supplemental Finding 2

Agree Disagree Partially Agree

A process exists to disable iCloud accounts for users that are no longer employed by the City of Jacksonville once the Accounting Technology Team gives confirmation all offboarding processes have run for those users. However, that process is not always followed, either because of miscommunication, user error, or unique edge cases. TS concurs with the Council Auditor's finding that a reconciliation process is necessary on a regular cadence to ensure that user accounts are adequately trued up to their COJ employment status. TS will work with the Accounting Division to develop and implement this reconciliation process.

We would like to thank the Treasury Division of the Finance Department and the Technology Solutions Department for their cooperation in conducting this follow-up review.

Respectfully submitted,

Kim Taylor

Kim Taylor, CPA
Council Auditor