CITY OF ALBUQUERQUE
OFFICE OF INTERNAL AUDIT

Nicole Kelley
City Auditor

STRATEGIC REVIEW

No. 22-401

FROM: Nicole Kelley, City Auditor
Office of Internal Audit

DATE: June 29, 2022

SUBJECT: Department of Finance and Administration Accounting Division – Strategic Review of Electronic Fund Transfer Vendor Account Changes

EXECUTIVE SUMMARY

Pursuant to a request received from the Director of the Department of Finance and Administration (DFAS), the Office of Internal Audit (OIA) conducted a strategic review to determine whether its Accounting Division's (DFAS - Accounting) internal controls over electronic fund transfer (EFT) account changes for third-party vendors, follow best practices in design, and are working efficiently and effectively to mitigate potential fraud and safeguard City of Albuquerque (City) funds.

The strategic review found that DFAS - Accounting's revised procedures follow best practices in design and appear to be working efficiently and effectively to mitigate potential fraud and safeguard City funds. Specifically, the strategic review found that:

- Appropriate segregation of duties was present.
- Account ownership was independently verified and documented.
- Levels of review and approval regarding vendor verification were conducted and documented.
- Proper level of system access rights was in place.

Opportunities to further enhance current written policies exist. For instance, current written policies are not entirely reflective of actual practices or the internal control framework observed by the auditors. Additionally, the City's overarching citywide EFT policy should be updated to reflect the procedural changes made by DFAS.

BACKGROUND, OBJECTIVES & METHODOLOGY

Background

EFTs refer to the disbursement of funds between institutions at the direction of an institution's customer by means of wire, direct deposits, Automated Clearing House, or other electronic means. A funds transfer can generally be described as a series of payment instructions between the originator (sending customer), the beneficiary (receiving customer), and their participating financial institutions in order to make payment to the beneficiary.

The City offers and processes EFTs as a safe and efficient method to provide payments to third-party vendors and employee claimants. DFAS - Accounting is responsible for processing these EFT transactions.[1] As such, DFAS - Accounting personnel are responsible for ensuring that

[1] The City is self-insured for workers' compensation benefits DFAS' Risk Management Division is responsible for processing employee claims and determining any benefit amounts to be paid on behalf of the City.

internal controls involving EFTs are maintained and that operational procedures are in place to prevent loss of City funds arising from fraud, employee error, misrepresentation by third parties, or imprudent actions by City employees.

The City often receives requests from vendors to add or change their banking account information. In March 2021 the City experienced a fraudulent transaction attempt through an unauthorized EFT[2] in the amount of approximately $1.9 million, whereby a fraudulent bank account change request was made by an imposture posing as a legitimate City vendor. The City's Office of Inspector General (OIG) investigated the matter and found staff training, as well as policies and procedures, should be enhanced. In its response to the investigation, DFAS detailed actions taken to address the fraudulent transaction attempt.[3]

As a result of the fraudulent attempt, DFAS - Accounting revised its policies in September 2021 and then again in April 2022. At the request of DFAS management, OIA conducted a strategic review of its updated policies and procedures for verifying and completing EFT account changes for third-party vendors. From April 1, 2022 to May 10, 2022, DFAS - Accounting received and processed 25 EFT account change requests from vendors.

Objectives

The objective of the strategic review was to determine whether DFAS - Accounting's internal controls over EFT account changes for third-party vendors follow best practices in design, and are working efficiently and effectively to mitigate potential fraud and safeguard City funds. Specifically, OIA:

- Evaluated the design and operating effectiveness of internal controls over EFT vendor account modifications.
- Reviewed the appropriateness of staff access to the City's financial system.
- Determined whether any opportunities for improvement to the process exist.

Scope

DFAS - Accounting implemented its most recent policy changes effective April 1, 2022. The scope of the strategic review included all vendor EFT information changes that occurred from April 1, 2022 through May 10, 2022.

The Treasury Division (Treasury) of DFAS also processes EFTs on behalf of various City departments. However, the scope of this strategic review was limited to DFAS - Accounting and did not include evaluation of Treasury's policies and procedures related to EFT account changes. Further, while employee claimants and employee petty cash custodians are set up as vendors in the City's financial system in order to process applicable payments, account change requests made by employees were not included as part of this strategic review.

Methodology

Methodologies used to accomplish the objectives include but are not limited to the following:

- Analyzing DFAS - Accounting's revised policies and procedures.
- Conducting interviews and observations with key departmental personnel about the procedures for EFT vendor account modifications.
- Evaluating and verifying existing internal controls for account change requests as compared to industry best practices.

---

[2] The Consumer Financial Protection Bureau defines an unauthorized EFT as an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.

[3] Report number 21-0002-I was issued by the Office of Inspector General on June 23, 2021.

- Reviewing DFAS user access rights to the City's financial system.
- Performing detailed testing of 100 percent of all account modifications requested from third-party vendors during the period under review.

OIA then documented the results of the fieldwork. Additionally, OIA's strategic review considered the fraud risk identified during the OIG's 2021 related investigation.

No system of internal controls can completely eliminate the risk of fraud. However, well-designed and effective internal controls can deter fraud from occurring by reducing the opportunity for fraud to be committed and increasing the perception that if committed, the fraud will be detected. To this point, City management is responsible for ensuring resources are managed properly and used in compliance with laws and regulations; programs are achieving their objectives; and services are being provided efficiently, effectively, and economically.

RESULTS

Finding 1 – Procedures for verifying and completing EFT vendor account change requests follow best practices in design and appear to be working efficiently and effectively.

OIA tested the operating effectiveness of internal controls by determining whether controls are functioning as designed and whether the person performing the control possesses the necessary authority and competence to perform the control effectively. OIA tested 100 percent of EFT third-party vendor account change requests made during the review period and found that all 25 requests adhered to the process described by management.

Appropriate Segregation of Duties and System Access Controls – OIA found that controls are in place to properly segregate the verification, processing and authorization of vendor account change requests. Specifically, DFAS has established dual controls through segregation of duties so that no single individual can execute an account change from beginning to end. Duties such as receiving account change requests and related supporting documentation, entering, reviewing, and approving information are appropriately segregated among different employees to reduce the possibility of errors, theft, and mishandling of account modifications. Additionally, procedures now include a dual control whereby a secondary review by the Risk Finance Manager is required for final approval.

Further, OIA reviewed the user access rights to edit, review, and approve vendor account changes in the financial system and found employees involved possess the appropriate level of system access given their role.

Evidence of Account Ownership Verification – Procedures now require two-step independent verification of account ownership, which is accomplished by a callback procedure for all account change requests. For instance, the Authorization Form is independently verified with a "known" contact at the requesting entity and a notarized bank letter is required and the information is independently verified with the bank. Further, procedures now require staff to document all verification steps performed and retain them in a central repository. Retaining evidence of verification procedures decreases the likelihood that errors or procedural steps go overlooked, and enhances employee accountability and the detection of attempted fraud.

In March 2022, DFAS - Accounting began utilizing the Wells Fargo Application Programming Interface (API) to assist in detecting and preventing fraud associated with bank accounts and payment transactions. If the vendor's financial institution participates in the Early Warning Services (EWS), the API is used to verify bank information by comparing the vendor and bank information between the City's financial system and EWS.

Inclusion of Red Flag Indicators – According to the Federal Trade Commission (FTC) a "program must include reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations. Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft[4]." DFAS' revised policies now include such "red flag" indicators to assist staff in identifying instances of suspected fraudulent activity.

Finding 2 – Opportunities exist to further enhance revised electronic transfer policies.

OIA evaluated the design of the internal control environment by reviewing DFAS' written policies and conducting a walkthrough with staff of the process. OIA found that while in practice, internal controls were appropriately implemented, not all controls performed were incorporated into the revised policy. Written policies and procedures are essential to ensure that staff can effectively and consistently perform duties in accordance with documented guidelines. Not having complete and updated written policies and procedures increases the risk that employees will use inconsistent practices in handling and processing EFT vendor account change requests.

As a result of the walkthrough, management subsequently updated its policies to reflect current practices and procedures. However, written policies can be further enhanced by the following to further mitigate the risks that EFTs may pose.

- While policies detail the process in which requests are received, they do not explicitly state that no other methods are acceptable. Without doing so, staff may inadvertently accept and process unauthorized requests. The Federal Deposit Insurance Corporation (FDIC) recommends that policies and procedures specify the only acceptable method which third-party vendor account change requests may be received.
- As part of account ownership verification process, staff independently verify with the vendor certain information such as their vendor number and tax identification number. However, the National Automated Clearing House Association (NACHA), recommends that questions related to account activity (i.e. the amount and date of the most recent transaction, etc.) and old and new routing and account information should also be used to validate account ownership.
- While the new policies now include 'red flag" indicators, the policies do not always detail the steps that should be taken, such as escalation parameters, when a red flag is identified. According to the Federal Trade Commission a "program must spell out appropriate actions you'll take when you detect red flags."
- Policies should include ongoing training requirements in order to ensure that staff are aware of the current process and best practices to identify unauthorized EFT attempts. According to management, training is provided to staff annually. However, current written procedures do not specify the training requirements of staff involved in the process. Requiring periodic training can help staff understand the practices of fraudsters and the ways in which their practices evolve, as well as decrease the possibility that staff will execute procedures that do not comply with the department guidelines.

The City's overarching citywide EFT policy is outdated and does not reflect the procedural changes made by DFAS - Accounting. The policy was last updated in January 2020 and is no longer reflective of the division's current EFT account change practices. The U.S. Government Accountability Office (GAO) also supports a comprehensive manual "that lays out in one place policies and rules and standardized procedures and practices" and states that such a manual is critical to ensuring staff have a clear and consistent understanding of rules and processes.

[4] Federal Trade Commission. "Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business". May, 2013.

Recommendations:

1. The Department of Finance and Administration should consider revising its current electronic fund transfer (EFT) policy to:

    - Specify the only acceptable method by which third-party vendor account change requests may be received.
    - Include questions related to account activity (i.e. the amount and date of the most recent transaction, etc.) to validate account ownership.
    - Detail the escalation parameters and actions to be taken when suspected inappropriate activities are found and outline the individuals included in the incident response team.
    - Detail the steps that should be taken when a red flag is identified.
    - Specify the ongoing training requirements of staff involved in the EFT process in order to ensure that staff are aware of the current process and best practices to identify unauthorized EFT attempts.

2. The Department of Finance and Administration (DFAS) should revise its overarching citywide EFT policies to reflect the procedural changes made by the DFAS - Accounting.

Conclusion:

Procedures implemented by DFAS - Accounting related to third-party vendor EFT account changes follow best practices in design and appear to be working efficiently and effectively to mitigate potential fraud and safeguard City funds. While the strategic review identified opportunities to further enhance existing written policies, as of June 6, 2022, DFAS - Accounting has revised its EFT policy based on the recommendations made and is working with the department to revise the City's overarching citywide EFT policies to reflect these changes.

PREPARED:

DocuSigned by:
Stacy Martin
64A7D650EA3F40A...

Stacy Martin, Staff Auditor
Office of Internal Audit

REVIEWED & APPROVED:

DocuSigned by:
Nicole Kelley
07E2FA5E2FAD4AC...

Nicole Kelley, City Auditor
Office of Internal Audit

APPROVED FOR PUBLICATION:

DocuSigned by:
Edmund E. Perea, Esq.
645A1FA5A6314C3...

Edmund E. Perea, Esq., Chairperson
Accountability in Government Oversight Committee