OFFICE OF INSPECTOR GENERAL
City of Albuquerque

Nicole Kelley,
City Auditor & Acting Inspector General

P.O. Box 1293, Suite 5025
Albuquerque, New Mexico 87103
Telephone: (505) 768-3150
Fax: (505) 768-3158

Report of Investigation

FILE NO: 21-0002-I **DATE:** June 23, 2021

SUBJECT: Attempted fraudulent ACH vendor transaction reported by City of Albuquerque's Department of Finance and Administrative Services.

STATUS: Final

INVESTIGATOR: J. S.

DocuSigned by:
Nicole Kelley
07E2FA5E2FAD4AC...

NICOLE KELLEY,
CITY AUDTOR AND ACTING INSPECTOR GENERAL

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

EDMUND E. PEREA, ESQ
ACCOUNTABILITY IN GOVERNMENT OVERSIGHT COMMITTEE
CHAIRPERSON

DISTRIBUTION:

Honorable Mayor
President City Council
Chief Administrative Officer
City Councilors
Director Council Services
City Attorney
Director of Department of Municipal Development
Members, Accountability and Government Oversight Committee
File

Executive Summary

The Office of the Inspector General (OIG) was asked to review an attempted fraudulent ACH transaction from the City of Albuquerque (COA) in the amount of $1.9 million to a vendor. Information was sent to the COA Controllers Office from the fraud department at Wells Fargo Bank (WFB). After initial review by the COA, the transfer was determined to be a fraudulent attempt and immediately placed on hold by WFB. WFB was able to stop the transfer and no funds made it to the fraudulent account.

The OIG reviewed the vendor transaction history. In addition, OIG reviewed the processes and policies implemented and performed by COA staff that are in place to detect, reduce and protect the COA from such fraud.

In conclusion, it was determined that staffs' neglect of duties, complacency and the deliberate deletion of records all played a part in the fraudster nearly succeeding in its attempt to defraud the City. Two of the three staff involved in processing the paperwork relating to this transfer demonstrated a dereliction of their duties.

Abbreviations

OIG – Office of the Inspector General
COA – City of Albuquerque
DFAS – Department of Finance and Administrative Services
DFAS-1 – Accounts Payable Coordinator
DFAS-2 – Senior Administrative Assistant
DFAS-3 – Accounting Manager
EFT – Electronic Funds Transfer
IG – Inspector General
IT – Information Technology
VENDOR – Vendor who Fraudster Presented as, COA Vendor
WFB – Wells Fargo Bank

Initial Complaint and Background

On March 29 and 30, 2021, the OIG received information and held a telephonic meeting with the City of Albuquerque's (COA) Assistant Controller. The Assistant Controller provided background information on the fraudulent ACH transfer in the amount of $1.9 million dollars, made by the COA. This transfer of funds related to a fraudulent bank account change request by a fraudster posing as a COA vendor/supplier. The Assistant Controller provided the following initial timeline:

1. March 24, 2021: COA received a notice from Wells Fargo regarding potential fraud for a payment file.

2. March 24, 2021: The Assistant Controller spoke with COA's vendor/supplier's Office Manager to inquire about banking update and discovered that it was not requested by the vendor/supplier.

3. March 24, 2021: The Assistant Controller called Wells Fargo to confirm banking information was not requested by vendor. Wells Fargo initiated a fraud fund recovery.

4. March 24, 2021: The Assistant Controller emailed the DFAS's Administrative Coordinator and AP Coordinator and requested all documentation and emails regarding this bank account change request.

5. March 25, 2021: The Assistant Controller reviewed supplier information and comprised timeline of the event.

6. March 26, 2021: The Assistant Controller reviewed bank changes for other vendors and proposed changes to current EFT (Electronic Funds Transfer) Policy and requested additional documentation.

7. March 29, 2021: The funds were recovered by Wells Fargo for this ACH Transfer.

Research and Document Review

On March 24, 2021, a Wells Fargo Bank Fraud Prevention Consultant reached out to the COA. Wells Fargo is the bank with which the COA does business. The letter stated:

Wells Fargo Bank's Treasury Management Fraud Prevention department is contacting you to verify a recent ACH transaction submitted via Payment Manager.

In addition, Wells Fargo Bank sent the COA Department of Finance and Administrative Services (DFAS) information with Imposter Fraud complaint filing instructions.

The employee who entered the information into COA financial software, PeopleSoft, was identified and will hereinafter be referred to as DFAS-1. A review of DFAS-1's email demonstrated that on Friday, November 20, 2020 an email was sent directly to the COA email address for DFAS-1 from an email address *dotoski@mscontructors.com* The email stated:

Hello,

My name is David Otoski, present, at Mountain States Constructors Inc, of 3601Pan American Fwy Ne Ste 111, Albuquerque, NM 87107. Attached is out completed Ach form and letter from our bank, please take note and update. Thanks

Regards

David Otoski
president/Owner
Mountain States Constructors Inc

Document Review
Email, Associate COA Controller

After receiving the initial information from the COA Bank, the Associate COA Controller sent an email to DFAS-1 and DFAS-2 [staff who is enters and submits for final approval for any transfers] stating:

We had a bank account update for VENDOR. I talked to the vendor and they don't recall making a request to change the bank info. The change was processed by DFA-1. This is potentially a fraud situation. We just issued a payment for $$1.9M and we are trying to recover the monies. Please look for the information asap and send any emails that you have to me. DFAS-1 do you have the email request> IF so please forward the email to me

Review
PeopleSoft/FINPROD

A search and review of the VENDOR in PeopleSoft was conducted and the following was observed:

1. A review of the bank account history screen demonstrated that the VENDOR only had one bank account while being a supplier for the COA. This was evidenced as there was only one screen for the bank account history. However, there should have been three accounts listed for the VENDOR to include the initial account set up bank information, the VENDOR requested a change in September 2020, and the fraudulent change request which occurred in February 2021. The previous two accounts were deleted by DFAS-1 in the system, which is not an accounting practice that should be used, as the historic profile of all account changes should remain in the file.

2. The February 2021 information was timestamped and entered in the evening hours, at 7:09 p.m. A review of timesheet information in Kronos demonstrated that DFAS-1 was working outside of scheduled hours.

Document Review
HR File DFAS-1

DFAS-1 began employment with the COA as a DFAS Accounting Aid in in August 1998.

DFAS-1 was promoted to Administrative Assistant in the DFAS on June 29, 2013.

DFAS-1 was hired into the position of DFAS Accounts Payable Coordinator on October 13, 2014.

DFAS-1 signed the 'DFAS is GREAT' Customer Service Pledges in 2015, 2016 which in part states that:

1. DFAS strived to be a progressive center of excellence that is a valued resource, fostering innovative business solutions, encouraging professional ethics, fiscal integrity, trust and stewardship of city assets; and
2. that DFAS employees will hold themselves accountable and each other accountable for their service commitment.

DFAS-1 was promoted to a new position in the Department of Council Services in February 2021.

DFAS-1 has received certifications in/on the following topics during her employment with the COA:

- Trainer Academy
- Pre-Management Development Program
- Billing/Receivables Accelerated Rel 9 Ed 3
- How to Handle City Revenue/Imprest Funds

Document Review
HR File DFAS-3

DFAS-3 was hired with the COA as a DFAS Accounting Manager in January 2019.

DFAS-3 completed probation six months after hire and as a result received a pay increase on August 14, 2019 that is commensurate with completing probation. The increase was a performance pay increase.

Document Review
COA Electronic Funds Transfer Policy – Accounting Division

The COA Electronic Funds Transfer (EFT) Policy was last updated in March 2021 and the version applicable when the subject funds transfer occurred was dated January 2020.

The City of Albuquerque (City) offers and processes Electronic Funds Transfers (EFTs) as a safe and efficient method to receive electronic deposits from customers, to purchase and redeem investments, to issue refunds to employees and vendors, and to provide payments to suppliers. EFTs are processed through the vehicles described below.

A large volume and cost-efficient method of EFT is the Automated Clearing House (ACH). This is an electronic payment delivery system that processes electronic credit and debit transactions, including direct deposits, within the United States using the American Bankers Association (ABA) number. The ABA number is also known as the "check routing number" or "routing transit number" and should be used as the first identifying number for ACH transactions. The bank account number and name assigned to the account are also required before an ACH transaction can be created, and the exchange of funds processed between two parties.

The process and procedure for verifying an ACH Account addition, change or modification is:

A domestic supplier may receive an ACH debit transaction by completing the Supplier Authorization Payment (SAP) and the Release of information (ROI) forms. All other forms other than the SAP & ROI forms are invalid and are not to be used for making any additions or changes to ACH/Banking information. The completed and signed forms can be emailed to SAPRequest@cabq.gov with the subject line "Supplier Authorization Payment Form". The form must be accompanied by a letter from the supplier's bank representative on bank letterhead. The letter must contain the ABA number, bank account number, name on the bank account and the respective taxpayer identification number (TIN); along with the bank officer's name and contact info (phone, address, email) and signed by the bank officer. Additionally, we require an authorized release of information letter. This information will be used to verify the supplier's banking information. Incomplete forms or missing required documentation will not be accepted.

2.1 Procedures for Verifying Account Additions, Changes, and Other

Modifications

1. There are three assigned individuals for completing the process; the first individual receives the request, documents the request & checks the forms for completeness (Senior Administrative Assistant). The second individual vets & enters the information for the respective vendor profile. The third individual reviews the changes and either approved or denies the vendor updates (Accounting Manager). The first and third individuals receiving and verifying the information should have view access to the supplier database. The Controller's Office should verify and validate the security roles in the PeopleSoft of the individuals assigned.

2. If the form is for setting up a new payment authorization, AP should work in conjunction with the Purchasing Division to review Contract or Purchase Order information to verify name of the supplier and contact info.

3. If the form is requesting to stop ACH payments, the supplier should be contacted in the same manner as Step 6 c. below.

4. Individual 1 Role: (DFAS-Accounting's Senior Administrative Assistant)
    a. Receive the SAP request to add, update, or cancel ACH enrollment. Review the form for completeness. Incomplete forms will not be sent for further verifications. Receiver should notify the requestor of the missing information and request a new and complete form is sent to the City.
        i. Documents the request via a log spreadsheet
        ii. Requests for Entity Name Change, Address, Contact Information, or Tax ID Change must have an accompanying updated City Alternate W-9 Form.
        iii. Compare data on the form to data in Peoplesoft. Any changes from this form to Peoplesoft has to have a new W-9
        iv. All information on the financial information form has to match the bank letter.
        v. Review if the Supplier is an existing supplier, review Supplier name, tax ID number and contact information to review discrepancies.
        vi. Verify the two contacts under "Supplier/Vendor Information" section of the SAP form is accurate.

If the form is complete and all supporting documentation is present, forward the information to the second individual.

    a. Review the ABA number, bank account number, and name as shown on bank letterhead provided with the form. (Accounting is looking into getting Account Validation through Wells Fargo

through CEOP Portal)

i. Verify bank letter information to the SAP form.
ii. Ensure that all discrepancies identified in step 1 have been cleared.
iii. Ensure all verifications were complete.
iv. Counter checks, or checks with no name and address info on the check are not authorized forms of documentation. Cancelled checks are not an appropriate form of documentation.

b. Call the bank to verify if the information is from the bank represented and if information matches the supplier.
    i. Reference the release of information form with a bank's representative
    ii. Obtain a signed copy of the verification
c. Call the supplier to verify the information in the SAP form and that a form was sent on the supplier's behalf. Indicate to the supplier what the form is requesting (add, update, cancel or modifying name/tax ID info).
    i. Individual should not solely rely on the phone number noted on the SAP form. Additional Verification of the supplier should be done by reviewing past payments to the supplier. This can be done by reviewing past invoices and contacting the number on the invoice. If prior invoices or payment are unavailable, individual should review other means of verifying the supplier (internet search, etc.).

d. If (a.) (b.) and (c) above are complete, changes can be made in the Supplier Database.
    i. A correct history or overriding existing information is not permitted. Changes and modifications to the supplier database must done by adding a new section in PeopleSoft with new effective dates. Previous information should not be deleted.
    ii. Ensure PeopleSoft Supplier Database has all relevant information in the file (contact names, titles, numbers, email addresses, etc.)
e. All documentation must be scanned and saved as an attachment to the PeopleSoft Supplier Database. Changes to the database will be tracked by the PeopleSoft system.
f. Complete verification box in the bottom right hand corner of the SAP form. The box includes Active Directory user name (the same username to log onto email or computer) and date verification was completed.
g. Notify the Supplier that final changes have been made to Supplier Database and when the change will take effect.

h. Forward signed and completed SAP Form to individual responsible for making changes in the Supplier Database.

2. Supplier Approval:
   a. Check for supporting SAP, ROI and Bank Letter
   b. Check for due diligence documentation
   c. Check to make sure Supplier ID and no duplicates on the SAP.
   d. Check Peoplesoft and SAP match the legal names
   e. Check Peoplesoft and SAP match the federal tax ID's
   f. Check Peoplesoft and SAP match address information
   g. Check Peoplesoft and SAP match contact information.
   h. Check Peoplesoft and SAP match the Financial Institution Information and Bank Letter
   i. Approve supplier.

If there has been any indication that fraud or suspicious activity has occurred, a supervisor must be notified immediately. If it is noted that payments have been made to a bank account or supplier that is fraudulent, a supervisor must be notified immediately. All future ACH/wire payments should be suspended and the supplier should be defaulted to receive paper checks. A/P should contact the City's merchant services bank to notify them of the fraudulent activity. A/P processes all supplier payments nightly and generates a daily check/ACH register. All ACH direct deposit payments have file detail and total amounts submitted to the bank for processing. Treasury and Accounting verifies that the totals submitted to the bank have been received and posted by the bank for processing. If file totals do not agree between City and the bank, Treasury and A/P researches the issue with Wells Fargo to obtain resolution.

ACH Transfer Request
Vendor – 1

The VENDOR submitted a Supplier Authorization Payment (ACH) Form for a change to their current ACH Account on September 11, 2020. This was sent to the SAPRequest email, was signed and completed on the appropriate COA Form and included a letter from the Bank involved verifying their good standing and that the Bank was informed of the change request of the ACH settlement account with the COA. This was signed on Bank letterhead. However, the COA Accounting Use Only signature box was not completed or signed. This signature box is used as a verification by staff that the review was completed to verify the validity of the change (this will be described again in staff interviews).

This account change, submitted in September 2020, was submitted through the proper process and was verified as correct by the VENDOR. It was a change to the VENDOR'S bank account number; not the bank name or routing number.

Document Review
Training and Policy/Process Review

DFAS management was asked for documentation that staff were trained on this approval process for ACH additions and changes and entry into PeopleSoft FINPROD. OIG was informed that is no formal training documentation.

Documentation was provided that DFAS-1, DFAS-2, and DFAS-3 all participated in a meeting, in person, in which the Electronic Funds Transfer Policy was reviewed for 'completeness and compliance of the policy' on February 6, 2020.

Interview
DFAS – 2

An in-person interview was held on April 19, 2021 at the Office of the Inspector General with two OIG Investigators and DFAS-2. During this interview, DFAS-2 stated the following:

DFAS-2 has been employed with the DFAS for over 15 years in various roles.

DFAS-2 detailed the process whereas a vendor or supplier would add an ACH account or request a change to the ACH account. All ACH forms would be sent to the SAPRequest email box. DFAS-2 monitors this mailbox. DFAS would receive a request, verify all required documents are present (bank letter and vendor change request form), log the receipt of request on a spreadsheet and forward the Request Form to the Coordinator for processing.

DFAS-2 stated that once this is forwarded to the Coordinator, that is the end of any log entries on the aforementioned spreadsheet; DFAS-2 stated she is not made aware if/when these requests are processed or completed.

DFAS-2 stated that if the appropriate documents are not attached, she will contact the vendor/supplier to make the correction.

DFAS-2 is unaware of who else has access to this mailbox but knows that additional people do.

DFAS-2 stated that on average there is between zero to five requests in that box per week. DFAS-2 checks the inbox, on average, one time per week at a minimum, usually on Thursdays.

DFAS-2 stated that no staff reviews the log or even requests to see the log. In addition, there is no reconciliation process. DFAS-2 provided the log to the OIG to review [it should be noted that there is no entry of this ACH change request on the log].

Interview
DFAS-3

An interview was held on April 19, 2021 via Zoom with two OIG Investigators and DFAS-3. During this interview, DFAS-3 stated the following:

DFAS-3 is an Accounting Manager in the DFAS and has been in that position for approximately one-and-a-half years. Prior to that time period, DFAS-3 was with the State of New Mexico in a similar department and position.

DFAS-3 stated that his primary duties are the review and approval of suppliers information and payments; completing gross payroll accounts; and processing journal entries and composite billings.

DFAS-3 stated that he reports to the Assistant City Controller.

DFAS-3 detailed the process by which a vendor would request a change to their ACH information; the vendor would send an email to Accounts Payable (AP) through the generic mailbox, DFAS-2 would review information, then DFAS-1 would contact the bank to verify, and DFAS-1 would do final review to make sure everything matches. Once DFAS-3 reviews and approves a supplier, he no longer has access to view certain things.

DFAS-3 states that DFAS-1 reviews and verifies all things completed by DFAS-2. DFAS-3 states that he verifies the tax-ID and vendor name and that each 'box was checked, I-dotted and T-crossed'.

DFAS-3 stated that there was an EFT policy that was sent out to be worked on by all in department for review, but the only training he has received since arriving at the department is that he was shown the database and walked through it; many items are learn as you go.

A second interview was held with DFAS-3 on May 7, 2021 via zoom with two OIG investigators. During this interview, DFAS-3 was presented with various screen shots taken from the PeopleSoft program detailing his approvals and electronic verifications.

DFAS-3 stated and clarified from the first interview that the reason he approved some of the vendor changes was because he recently got access to see the attachments, but previously had to verify based on trust of DFAS-1.

When asked about the four (4) month delay between the request coming in (November 2020) to the approval/addition to the system (February 2021), DFAS-3 stated the 'need to be current' for better customer service. However, he could not explain why it was late in this instance. He stated that DFAS-1 was behind and sometimes these do take time. DFAS-3 stated that there are not many people to help. There could be problems with the vendor, problems at the bank which could explain why this was late.

DFAS-3 stated that his personal objective is to respond to everything within 24 - 48 hours and he does not need a form to tell him that.

DFAS-3 stated that he has told the Assistant City Controller that these have been 'taking a while'. This was done verbally and not in writing.

When asked about the 'verification box' on the Change Form and referenced in policy, DFAS-3 stated that this is verifying a 'checking of it all' to include that 'the bank is the bank, accounts match the supplier, etc.'.

DFAS-3 stated that he is not aware of what the process is when staff call the bank but there is now a new checklist.

DFAS-3 stated that tax ID's are not public information so if that is present, the document is usually correct. The OIG conducted an internet search of the VENDOR and showed DFAS-3 that the Tax ID was public information, and DFAS-3 stated that he never knew that.

DFAS-3 stated that he is not robotic or complacent; that he just assumes that his staff and DFAS-1 does her job.

Interview
DFAS-1

An in-person interview was held on May 24, 2021 at the Office of the Inspector General with two OIG Investigators and DFAS-1. During this interview, DFAS-1 stated the following:

DFAS-1 is currently employed in the Office of City Council, but prior to that, worked in the DFAS for 23 years.

DFAS-1 detailed her last position as DFAS Accounts Payable Coordinator and stated that one of her job functions was reviewing, verifying and sending vendor changes for final approval (that is what will be discussed here only from her job functions, as that is the subject of this investigation).

DFAS-1 stated that she would receive vendor requests for additions or changes through the assistant (as received from the SAPRequest mailbox) and start the process of verifying information to see what is missing, if everything matches and looking up previous invoices.

The Fraudster email (allegedly from VENDOR) was sent directly to DFAS-1's email address and the papers attached were dated November 20, 2020. DFAS-1 was asked about this email coming directly to her email (and not through the process described above):

DFAS-1 stated that it is not abnormal for companies to send emails directly to her. That fact alone would not be alarming to her. She would hand this information to the clerk (DFAS-2) to add it to the log.

The documentation subject to this fraudulent transfer was not on the log. When showed the log and asked if she had documentation of giving this information to DFAS-2, DFAS-1 said she did not document it and could not recall. DFAS-1 stated that she does not know why this was not added nor could she recall if she did in the particular instance.

The Fraudster email (allegedly from VENDOR) was sent directly to DFAS-1's email address and the papers attached were dated November 20, 2020. DFAS-1 signed the verification box on the Vendor Change Request Form with her initials and User ID and dated this verification 12/08/2020). When presented with this information, DFAS-1 stated:

That the verification signature indicates that she verified the banking information was correct, and, in addition, verified with the vendor that this change request is valid. *[Of note, the request came in November 20, 2020, was allegedly verified by DFAS-1 on December 20, 2020 and added to PeopleSoft on February 17, 2021.]*

DFAS-1 stated that this verification is done by telephone and is not required to be documented any further. DFAS-1 stated that "this is not part of the EFT policy that I followed". When the OIG asked if DFAS-1 thought this was a good practice or should be done, DFAS-1 stated that it should be, but was not in policy so she did not do it.

For this particular verification, DFAS-1 does not recall who she spoke with at the VENDOR, but she usually 'googles' the company address to ensure it is valid (and not based off the form) and she typically looks for the name in the system on previous forms.

The Fraudster email (allegedly from VENDOR) was sent directly to DFAS-1's email address on and the papers attached were dated November 20, 2020. It was not added to the PeopleSoft system until February 17, 2021 at 7:09 p.m. When asked why this took so long, DFAS-1 stated:

DFAS-1 cannot recall why it took so long to enter. Usually, it takes time to complete verification process.

DFAS-1 stated that she often worked late at night. DFAS-1 stated she does not log those hours or change time sheets to reflect that. [A review of time sheets demonstrated that DFAS-1 does not log work after hours.]

DFAS-1 stated that if she was away from the office, in general, that her projects would just have to wait until she returned, which is why she sometimes worked at night. [A review of Kronos timekeeping information demonstrated that there was no lengthy leave of absence or vacation to explain the delay in processing/entering this information.]

The Supplier location screen in PeopleSoft shows a note entered which states: SETUP ACH AND CONTACT INFORMATION... 021721....INITIALS. When asked about this note:

DFAS-1 stated that she should have wrote 'change' and not set-up. She does not know why she worded it this way.

Under the Payables Options, Supplier Bank Accounts screen in PeopleSoft, the previous two bank accounts have been deleted. This is evidenced by the screen which should show three accounts for ACH over the history of this vendors business with the COA. However, it only shows one. This screenshot was provided to DFAS-1:

DFAS-1 does not recall deleting the previous bank accounts but admits she must have.

DFAS-1 stated that there is not a departmental audit process involved or any random verification or checks on documents.

DFAS-1 stated that she would and has asked for more information if something did not look or feel right with a vendor change. She did not get that sense looking at each piece individually of this matter.

Conclusion and Recommendations

Based on the documentation and interviews, it is evident that the contributing factors that lead to this fraudulent transfer include staff neglect and complacency. In addition, policies and procedures should be enhanced to provide for a more manageable and trackable process.

DFAS-1 violated procedure and practice on three occasions, as found through the interviews and documentation reviews: 1. DFAS-1 signed a form verifying that steps were completed which could not have been, as the vendor would not have verified this fraudulent information included on the request form; 2. DFAS-1 deleted historical vendor account information in PeopleSoft, which is integral for transparency, efficiency and good practice; and 3. DFAS-1 was complacent when logging information into a vendor's account in PeopleSoft when indicating that the information added on February 17, 2021 was an account 'Set-up' when it was in fact, an account change.

DFAS-3 did not perform a proper review of the vendor ACH request information before approving it and at times, did not appear to understand the levels of review expected of his position. Specifically, DFAS-3 did not perform a thorough review of vendor ACH change requests for both accuracy and completeness. Rather, DFAS-3 simply reviewed the information to ensure that all line items on the request form were filled out and that DFAS-2 has signed the form. DFAS-3 has neither requested nor required his staff to provide the level of detail necessary to perform a thorough review to substantiate the information on the request form. Further, the request letter itself (if properly reviewed) might have raised a red flag, as it was on a bank letterhead but included spelling and grammatical errors that might alert a reviewer to the possibility for fraudulent activity.

By inadequately reviewing vendor ACH request information and not substantiating the requested information, DFAS is unable to detect similar fraudulent attempts.

The U.S. GAO defines control activities as:

.... policies, procedures, techniques and mechanisms that enforce management's directives....

They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

A thorough review of vendor ACH requests prior to approving them is an example of such a control activity and should be completed by the DFAS, namely, DFAS-3.

The processes involved with PeopleSoft management needs to be reviewed and staff need to be clearly trained on the processes and requirements. In addition, checks and balances need to be implemented to ensure that complacency risks are reduced and errors can be identified to help reduce and eliminate opportunities for fraud.

The following are recommendations made by the OIG:

1. Develop an internal verification/audit process for quality assurance control within the DFAS.

2. Conduct an audit/assessment of the verification process and develop a form so that all vendor verifications are documented with who was spoken to, date they were spoken to, and summary of conversation. In addition, verify with banks if bank verifications can be conducted over the phone.

3. Ensure that all vendors utilize the SAPR email address and that all documents are forwarded back to the Administrative Staff to log and properly closeout. This will allow for tracking and better customer service on one centralized log, that all necessary DFAS staff and review.

4. Based on the documentation and interviews, it is evident that the processes involved with management needs to be reviewed and that staff need to be properly trained on the enhanced process. In addition, checks and balances need to be implemented to ensure that future complacency risks are reduced and errors can be identified to help reduce and eliminate opportunities for fraud.

Department of Finance and Administrative Services' Response:

RESPONSE: DFAS agrees that the primary contributing factors leading to the fraudulent transfer were staff neglect and complacency. It is clear that the staff in question failed to follow the policy and procedures in place at the time of the incident.

While DFAS agrees that policies and procedures may be enhanced, we respectfully disagree that a lack of proper policies and procedures was a factor involved with the incident. We believe that the policies and procedures in place at the time were adequate and if followed, would have prevented this incident. Training on the policy and procedures was provided to the employees involved with the incident in February 2020.

The following are recommendations made by the OIG:

1. Develop an internal verification/audit process for quality assurance control within the DFAS.

RESPONSE: DFAS agrees with the recommendation and has updated (in March 2021) the EFT policy and procedures to incorporate additional verification documentation, including:

- ***a. Require notes on all verification steps***
- ***b. Include the use of a Release of Information Form (ROI)***
- ***c. Validate requesting email address***
- ***d. Conference call between vendor and financial institution***

Training of all appropriate employees on the updated policy and procedures was conducted in April 2021.

2. Conduct an audit/assessment of the verification process and develop a form so that all vendor verifications are documented with who was spoken to, date they were spoken to, and summary of conversation. In addition, verify with banks if bank verifications can be conducted over the phone.

RESPONSE: DFAS agrees with the recommendation and has conducted a review of the verification process as a follow-up to this incident. DFAS has developed, and incorporated into procedures, a checklist that covers all verification steps required. DFAS made other changes/improvements to the process. Please see response to recommendation #1 for details on the changes.

3. Ensure that all vendors utilize the SAPR email address and that all documents are forwarded back to the Administrative Staff to log and properly closeout. This will allow for tracking and better customer service on one centralized log, that all necessary DFAS staff and review.

RESPONSE: DFAS agrees with the recommendation and has updated (in March 2021) policy and procedures to emphasize that SAP Change forms must be received into the proper SAPR email address. Further, the process and procedures for logging and tracking requests has been improved.

4. Based on the documentation and interviews, it is evident that the processes involved with management needs to be reviewed and that staff need to be properly trained on the enhanced process. In addition, checks and balances need to be implemented to ensure that future complacency risks are reduced and errors can be identified to help reduce and eliminate opportunities for fraud.

RESPONSE: While DFAS agrees that policies and procedures may be enhanced, we respectfully disagree that a lack of proper training, policy or procedures was a contributing factor to this incident. We agree with the OIG that the primary contributing factors leading to the fraudulent transfer were staff neglect and complacency. DFAS plans to proceed with the appropriate disciplinary action(s) as a consequence.

DFAS recognizes that vendor payment fraud is a significant and increasing threat. To further mitigate risks, DFAS is working with Wells Fargo, our fiscal agent, to implement a bank verification service that will flag potentially fraudulent bank account changes early

in the verification process. Further, DFAS is reclassifying the vacant Accounts Payable Coordinator position to a higher grade, more equivalent to our Payroll Supervisor position, to recognize the level of executive judgement and awareness that is required of the position.