Date: May 24, 2023

To: Sheryl M.M. Long, City Manager

From: Lauren Sundararajan, CFE, Internal Audit Manager

Copies to: Internal Audit Committee
William Weber, Assistant City Manager
Bobbi Hageman, Director of Procurement

Subject: **Electronic Funds Transfer Audit**

Attached is the Electronic Funds Transfer audit report. The primary objective of this performance audit was to determine the efficiency and effectiveness of the internal controls in the Office of Procurement (Purchasing) over the electronic funds transfer (EFT) process to ensure proper safeguards are in place to mitigate the loss of City funds. The audit was conducted in accordance with the current audit agenda.

Purchasing disagreed with most of the audit findings and recommendations. They claim that Purchasing staff do not have the credentials or training as it relates to banking practices, and that this function should be overseen by the Finance Department. However, currently, Purchasing is responsible for maintaining the banking information, approving new vendor accounts and changes to vendor account profiles. The audit revealed best practices for safeguarding EFT transactions are not followed, and a weak internal control structure exists within Purchasing.

The department responses display their inability to properly address and understand the significant internal control issues identified within this audit report. IA recommends Purchasing communicate and work cross-functionally with the Finance Department and the Enterprise Technology Solutions Department to create and implement processes to ensure safeguards and internal controls are in place to mitigate the City's financial risk exposure.

If you need any further information, please contact me.

Attachment

Electronic Funds Transfer Audit

May 2023

Lauren Sundararajan, CFE
Internal Audit Manager

Tawana Keels
Internal Auditor

Table of Contents

Executive Summary

Internal Audit (IA) conducted a performance audit of the electronic funds transfer (EFT) process in the City of Cincinnati (City). The primary objective of this performance audit was to determine the efficiency and effectiveness of the internal controls in the Office of Procurement (Purchasing) over the EFT process to ensure proper safeguards are in place to mitigate the loss of City funds.

The EFT process begins in City departments when a payment request is entered in the Cincinnati Financial System (CFS)[1]. Purchasing maintains the banking information saved in CFS, approving new vendor accounts and changes to vendor account profiles. Within the Finance Department, the Accounts and Audits Division generates a file that is sent to the financial institution initiating the EFT. The Treasury Division (Treasury) reconciles the transaction and notifies the department if the EFT is returned or rejected by the financial institution.

The audit revealed several opportunities to improve the internal control structure for the EFT process. For example, established written policies and procedures can assist in managing the risk associated with fraudulent EFT transactions. IA found there are no written policies and procedures for the EFT process, and no escalation protocols for fraudulent activities.

Best practices for safeguarding EFT transactions are not followed. This includes appropriate verification of changes to vendor accounts, segregation of duties, management review and oversight, prenotification process to verify banking information, maintaining centralized vendor records, and limiting access to banking information. These internal controls, if not properly implemented, present opportunities for fraud and increase the financial risk.

Vendors are encouraged to use the Vendor Self Service (VSS)[2] application software to register as a new vendor and maintain vendor records. IA found there is no training available for vendors specifically to establish and maintain vendor accounts and highlight the safeguards in place to protect sensitive banking information. Also, Purchasing has experienced challenges with the VSS application software synchronizing with CFS. Management should ensure the entity's information systems are effective in meeting organizational objectives and responding to risks.

To strengthen the internal controls over the EFT process, the following should be incorporated: establish policies and procedures and include escalation protocols for fraudulent activities, implement best practices for safeguarding EFT transactions, provide vendor training, and resolve software issues. Implementing these internal controls and best practices will ensure proper safeguards are in place to mitigate the loss of City funds.

[1] Cincinnati Financial System (CFS) is the Financial Management System for City accounting functions. CGI Advantage Financial is proprietary to CGI Technologies and Solutions Inc.
[2] Vendor Self Service (VSS) provides secure entry of account and banking information. CGI Advantage Vendor Self Service (VSS) application software is proprietary to CGI Technologies and Solutions Inc.

Background

EFT is a digital movement of money from one bank account to another. As a digital transaction, there is no need for paper documents. EFT has become a predominant method of money transfer since it is a simple, accessible, and direct method of payment or transfer of funds. As businesses increase their usage of EFT, paper checks become obsolete due to expense, slow expedition, and overall effort.[3]

The City offers and processes EFTs as a safe and efficient method of payment to third-party vendors. The process begins in City departments when a payment request is entered in CFS. Purchasing maintains the banking information saved in CFS, approving new vendor accounts and changes to vendor account profiles. Within the Finance Department, the Accounts and Audits Division generates a file that is sent to the financial institution initiating the EFT. Treasury reconciles the transaction and notifies the department if the EFT is returned or rejected by the financial institution. Vendors are encouraged to register and update account information in the VSS application software provided by the City. Finally, vendor profiles in VSS are synchronized with CFS prior to processing EFT payments.

The total amount of EFT payments processed by the City increased from $411,360,940.39 in 2021 to $493,268,926.18 in 2022, an increase of 19.9%. The number of EFT payments increased from 14,080 in 2021 to 16,537 in 2022, an increase of 17.5%. Continued growth of EFT transactions increases the risk of internal and external fraud, requiring comprehensive policies, accounting procedures, and safeguards for approving, processing, documenting, and reporting of disbursements by EFT.

[3] EBANX Website, https://business.ebanx.com/en/resources/payments-explained/electronic-funds-transfer-eft.

Audit Selection
IA conducted this audit in accordance with the current work plan.

Audit Objective
The primary objective of this performance audit was to determine the efficiency and effectiveness of the internal controls in Purchasing over the EFT process to ensure proper safeguards are in place to mitigate the loss of City funds.

Audit Scope and Methodology
To achieve the audit objective, IA reviewed best practices for EFTs, interviewed appropriate City staff, examined EFT transactions and records, and collected other information as needed. Records reviewed included documentation generated during calendar year 2020 through the present.

Statement of Auditing Standards
As required by the Cincinnati Administrative Code Article II §15, this audit was conducted in accordance with the Generally Accepted Government Auditing Standards (GAGAS), except for standard 5.60 pertaining to external peer review requirements. This exception did not have a material effect on the audit.

IA continues to conduct internal quality reviews to assure conformance with applicable GAGAS. IA performed the fieldwork between December 2022 and March 2023.

Commendations
IA commends the management and staff of Purchasing for their assistance and cooperation throughout the audit.

II. Audit Findings and Recommendations

Policies and procedures for the EFT process are not documented.

Policies and procedures are a key component of an internal control system. They provide the framework and guidance needed for staff to support the organization's goals and allow management to hold staff accountable. IA found Purchasing does not have written policies and procedures for the EFT process. This creates an increased risk of fraud and exposure for the City.

An example of a comprehensive policy is one which outlines banking activities that are consistent with statutory and legal requirements and specifies who is authorized to initiate electronic transactions (e-transactions), who is authorized to approve e-transactions, who will transmit and who will record e-transactions. Procedures should be in place to review and authorize EFTs to ensure effective prevention and detection of errors. When there are no written policies and procedures to ensure consistent and accurate compliance and application, the integrity and accuracy of the process may become compromised.

Recommendation 1: Comprehensive policies and procedures for the EFT process should be documented, communicated, and enforced.

Department Response: Disagree. Policies and procedures of this nature would need to be written and provided by Finance as procurement staff have no background or expertise in statutory or legal requirements as they relate to banking practices. These may already exist in Finance but are not a part of procurement's role in this function. In the current state, we only enter the banking information; we manage the record.

After a recent fraud incident, the Office of Procurement did put in an internal policy to attempt to verify information. We went back to the previous 6 months of EFTs submitted to manually telephone the company and verify with a person of authority that information was correct. We continue this process for all new EFT requests that come in outside of the VSS system.

There are no documented escalation procedures for fraudulent activity.

Escalation procedures for suspected fraudulent activity allow for quick action to alert all required parties to limit the loss of public funds. IA found Purchasing does not have documented escalation procedures for fraudulent activity.

Escalation procedures are an essential step in timely notifications to alert City departments, law enforcement and banking institutions of suspected fraudulent activity. Notifications to the FBI Internet Crime Complaint Center (IC3), Auditor of State, and the Adjutant General's Department of Ohio will alert state and federal officials of attempts to commit cybercrime.

Quick action may assist in identifying the bad actor committing the fraud, stopping the funds transfer, and increasing the chances of recovering the funds. Establishing written escalation procedures will strengthen internal controls required to manage the risk associated with fraudulent EFT transactions in the City.

Recommendation 2: Work with the Finance Department to develop and communicate escalation procedures for fraudulent activity to City departments.

Department Response: Disagree. These procedures exist and reside within the Finance Department. Procurement is not even aware when checks are returned, no matter the reason. Again, procurement staff do not have the training or knowledge as it relates to banking information. The investigation should happen within Finance and be reported to procurement to lock/freeze the vendor record.

Requested vendor changes of account information are not properly verified.

Purchasing staff approve vendor account changes in CFS. IA found inconsistencies in how the requested vendor account changes are verified.

Vendor/Customer Modifications (VCMs)[4] are authenticated by Purchasing staff following a Google[5] search and phone call to the contact number listed online or by contacting the individual listed on the Electronic Funds Transfer Agreement. IA was informed that agency contacts have been uneasy responding to calls from City staff asking to verify sensitive banking information. Additionally, IA found Purchasing does not validate account changes with the primary contact in CFS or verify the authenticity of signatures on the Electronic Funds Transfer Agreement.

The current verification process is inconsistent and increases the risk of potential fraud in the City. Purchasing staff may be calling the incorrect vendor location and/or department by using information found on Google. Alternatively, contacting the individual listed on the Electronic Funds Transfer Agreement could turn out to be the perpetrator of the attempted fraud. City staff should have a heightened sense of scrutiny any time they receive a request to change payment banking information.

Recommendation 3: Develop an internal verification process to validate changes of vendor identity, contact, and payment information prior to approval in CFS.

Department Response: Agree. Procurement is in agreement that this is a vulnerable area. We propose that VCM documents containing initial or modification changes to EFT-related fields enter a separate CFS workflow or be initially entered by Finance staff if not entered through the system. Finance would provide the banking verification approve the VCM. It would then be routed to Procurement for review and approval of all other entries in the vendor record. This would address the separation of duties and would shift the verification of financial information to the appropriate department.

Vendor account profiles are not updated in a timely manner.

Purchasing staff is responsible for approving and activating VCMs entered by City departments, vendors, or Purchasing staff. Vendor profiles in CFS are not updated until this process is completed. Failure by the Purchasing staff to actively approve VCMs may result in incorrect banking information being used to process EFT payments to third-party vendors and could result in EFT payments being refused or rejected by the financial institution.

IA found 2,348 VCMs waiting for approval by Purchasing on March 8, 2023. This includes incomplete VCMs in pending or draft status. IA was unable to obtain submission dates for all

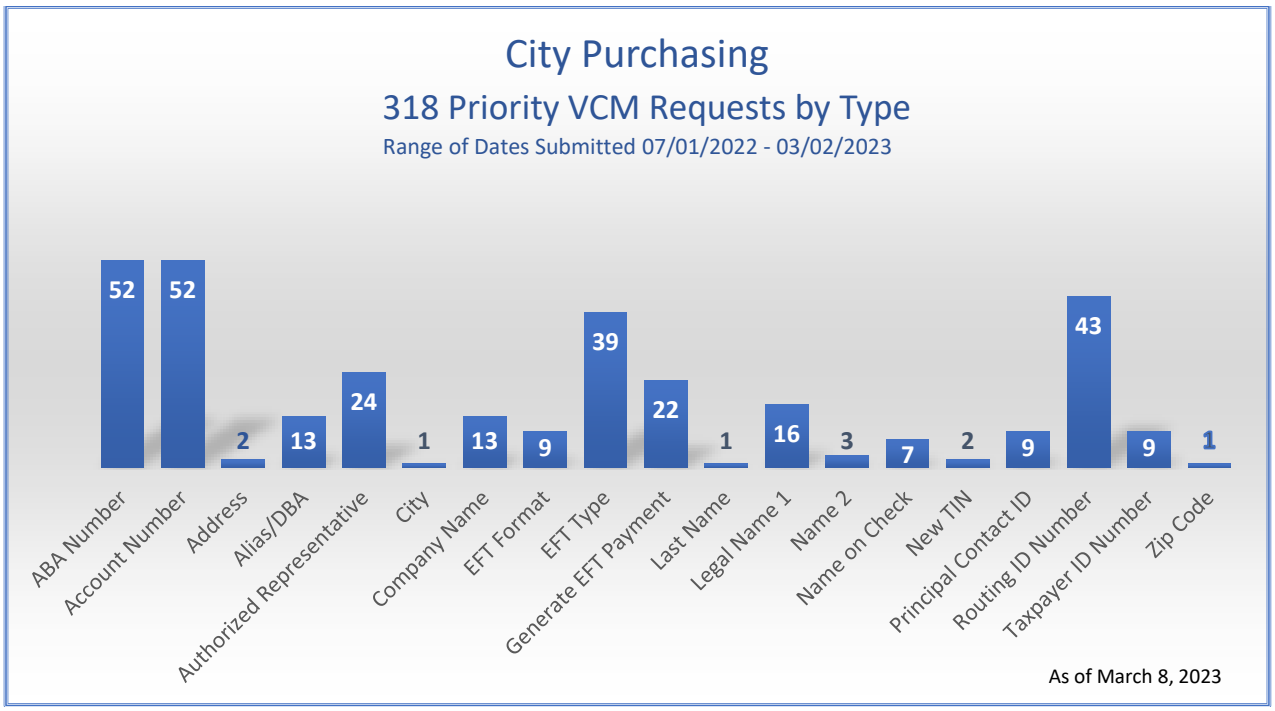
[4] Vendor/Customer Modifications (VCMs) are used to modify vendor records entered in the VSS or CFS.
[5] Google is a trademark of Google Inc.

2,348 VCMs; therefore, unable to ascertain the oldest open VCM. However, IA was informed by the Enterprise Technology Solutions (ETS) Department, that one pending VCM was dated April 18, 2018. IA also found management does not have a plan to approve the backlog of open VCMs in a timely manner.

IA further analyzed 318 VCMs identified as priority, and found the following:

- 208 (65.4%) VCMs were entered in calendar year (CY) 2022.
- 110 (34.6%) VCMs were entered in CY 2023.
- The top five request types for VCMs were: ABA Number, Account Number, Routing ID Number, EFT Type and Authorized Representative.

Below is a graphical depiction of the priority VCM requests by type:



Recommendation 4: Develop a plan to address the backlog of VCMs, prioritizing the highest risk VCMs first.

Department Response: Disagree. This finding is not accurate as it relates to the Office of Procurement. Procurement was unaware that there were VCMs that were “stuck” in the system. ETS indicated to IA during their interview that there was no issue with the system and that everything was in good working order; however, within a few days of that interview, Procurement’s work list showed 2,348 VCM’s dating back to 2018 that were released by the financial system.

This should no longer be an issue and Procurement has already addressed the backlog. We have been in contact with ETS to work to make sure that this doesn’t happen again.

Procurement is currently working through this backlog and will completed by the end of the fiscal year. We have addressed the high priority requests and are working through the remaining.

Recommendation 5: Establish deadlines for approving VCMs so vendor information is updated in a timely manner.

Department Response: Disagree. Procurement checks daily for outstanding VCMs and addresses them accordingly, typically within 3-5 business days at most. This is currently being done; the backlog mentioned in Recommendation 4 is skewing the number. In addition, Procurement is not aware when there are system failures and VCMS are not pushed through. We are continually working with ETS to make sure that the system is working properly and that necessary patches are being provided by the vendor of the financial system.

Segregation of duties is needed in Purchasing.

Segregation of duties is a preventative control intended to reduce the opportunity for fraud and error, requiring more than one individual to be responsible for performing the duties to complete a process. IA found job duties for the Purchasing staff are not properly segregated.

Purchasing staff are authorized to enter, review, and approve new vendor accounts and modifications to vendor profiles without review and approval by a second staff member. This increases the risk of fraud, as the person entering the EFT routing and account information is also approving the change. Proper segregation of duties is important to identify “red flags” when processing modification requests. This control makes it difficult for intentional wrongdoing because it requires collusion of two or more individuals.

Recommendation 6: Establish and maintain a segregation of duties within the department.

Department Response: Disagree. Segregation, especially when dealing with banking and financial information is a crucial component to combatting fraudulent activity. However, as noted in recommendation 1, procurement staff do not have credentials to accurately verify banking/financial information. Our recommendation on how to protect the City is documented in recommendation #3 as follows: VCM documents containing initial or modification changes to EFT-related fields enter a separate CFS workflow or be initially entered by Finance staff if not entered through the system. Finance would provide the banking verification and then approve the VCM. That VCM would then be routed to Procurement for review and approval of all other entries in the vendor record.

Interdepartmental coordination needs improvement.

The City pays most of its vendors through EFT. If the banking information is invalid, the payment cannot be delivered and is therefore returned to the General account as a RETURN SETTLE RETURN.[6] IA found gaps in communication between City departments concerning EFT transactions. Ongoing communication between departments is essential to improving operational effectiveness and to mitigate the risk associated with EFT payments.

[6] City of Cincinnati, Treasury, Revised SOP for EFT Return, received from Treasury February 2, 2023.

IA found the Treasury Standard Operating Procedures (SOP) for EFT Return[7] directs Treasury staff to send an email notifying the department that issued the payment of the returned EFT, however, Purchasing is not copied on the email notification. The department is directed to work with Purchasing to have the vendor banking information updated in CFS. "Failure to do so within 30 days of the date of the return, will result in funds being receipted back to your department."[8]

Improved communication is also important to maintain Prompt Pay System requirements per Ordinance 297-2002. This Ordinance, effective January 1, 2003, established the City will pay contractor invoices within 30 days of receipt of a complete and responsive invoice. IA reviewed Treasury EFT Return logs and found instances where EFT funds were held by the Treasury for more than 30 days, then credited back to the department. IA also found vendor payments are not flagged as a priority when processed a second time by Purchasing.

Recommendation 7: Work with the Finance Department to improve the flow of information regarding returned and rejected EFT payments and ensure compliance with Ordinance 297-2002.

Department Response: Disagree. Procurement cannot know nor should we be responsible when we are not notified from the Finance department when EFTs are returned or rejected or when City departments do not contact us – we are unaware of the policy mentioned above. We are responsible for vendor management; we can inactive the vendor or prevent new spending when there is an issue with an EFT; however, without notification by Finance and updating by the vendor of their EFT record, we would not know that payment is being help up in violation of the prompt pay ordinance.

Additional management review and oversight is needed.

Purchasing management is responsible for ensuring department operations are effective and efficient, enforcing policies to minimize risk to the City, evaluating performance, and holding staff accountable for internal control responsibilities. IA found management has not established internal controls and operational structures for vendor account changes and the EFT process. Ongoing monitoring may include generating and reviewing change reports and analyzing vendor issues to identify opportunities to operate more efficiently and reduce the risk of fraud.

Recommendation 8: Establish internal controls and procedures to monitor vendor account activities used to process financial transactions.

Department Response: Disagree. See Recommendation 1 and response. The Office of Procurement staff have no training, background or expertise in this financial area.

Vendor banking information is not verified.

The City offers and processes EFTs as a safe and efficient method of payment to third-party vendors. IA found banking information is not verified prior to processing payments to vendors. This increases the risk of the EFT payment being returned to Treasury by the financial institution due to invalid account and/or routing information.

[7] Ibid.
[8] Ibid.

Nacha[9] supports a prenotification (prenote) process that is sent through the direct deposit network to verify the accuracy of the information (routing number, account number and account type). A prenote electronically tests the accuracy of an automatic deposit bank account before transferring actual funds to the account. If there are problems with the bank account information, the financial institution provides feedback to the account holder. Entering incorrect banking information can result in rejected or refused EFTs, delaying payments to vendors.

IA tested the Treasury EFT Return Logs for CY 2022 and found that Fifth Third Bank returned 48 EFTs to Treasury totaling $1,354,335.47. There were five reasons stated for the returned EFTs including: "No Account – Cannot Locate", "Account Closed", "Receiver Refuses Payment", "Invalid Account Number" or "Invalid ACH Routing No". IA was informed one of the reasons for the receiver to refuse funds is that the funds were sent to the incorrect account.

EFT Returns by "Return Reason" for CY 2022 is provided in Chart 1 below:

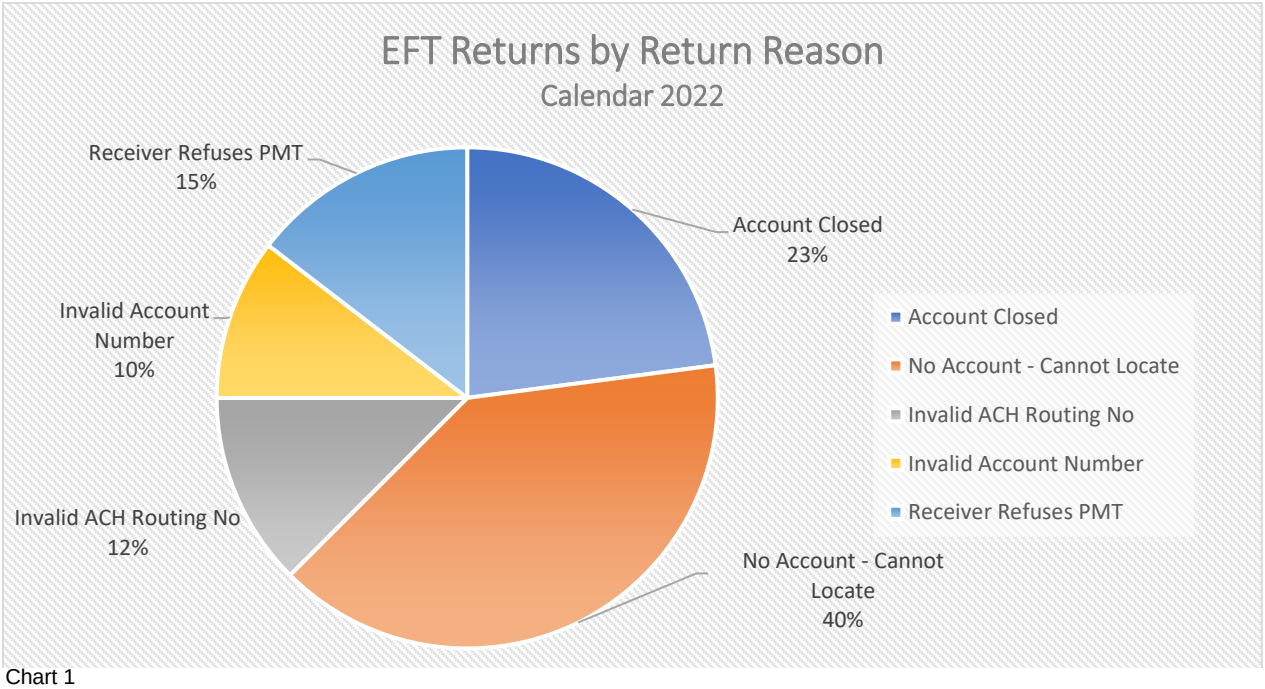


Chart 1

Recommendation 9: Work with the Finance Department and the ETS Department to develop a verification process for banking information.

Department Response: Disagree. While there is pre-note functionality in our current financial system, Procurement would have no access to the banking information and verification under Treasury's authority to effectively provide support for this feature. This used to be a function used by the City until ETS was informed by Finance to inactivate the feature. Procurement is in favor of reactivating the pre-note function as we are in agreeance it will substantially cut down on errors and potential fraud.

[9] Nacha, previously known as the National Automated Clearing House Association, is the governing body that oversees the ACH network that processes electronic payments in the United States.

There are no training requirements for City staff with access to EFT information.

Training and documentation are a necessary part of effective internal controls, designed for consistency and operating effectiveness, while considering organizational exposures and vulnerabilities. Management should design control systems to identify, analyze, and respond to risks related to achieving organizational objectives. This should include the organization's expectations of ethical values in the standards of conduct. IA was informed that Purchasing does not provide or require training specific to EFT policies and safeguards to minimize the risk of loss and prevent fraud.

Ongoing training is required to develop and retain staff knowledge, skills, and abilities to meet changing organizational needs and to make staff aware of the current process and best practices to identity unauthorized EFT attempts and protect vendor information from potential fraud schemes.

Recommendation 10: Develop ongoing training for all City staff with access to vendor banking information to ensure they have the knowledge and resources to effectively manage the EFT process.

Department Response: Disagree. See Recommendation 1 and response. The Office of Procurement staff have no training, background or expertise in this financial area.

VSS and CFS do not synchronize.

Management should ensure the entity's information systems are effective in meeting organizational objectives and responding to risks. IA found Purchasing has experienced challenges with the VSS application software synchronizing with CFS.

During interviews, the Purchasing staff expressed concerns about VCMs being "stuck" in the software. While VCMs are "stuck", vendor changes do not appear in the worklist Purchasing staff monitors for approval, resulting in incorrect vendor information including old bank routing and account information being used by the Finance Department to process vendor payments. This can result in EFTs being deposited in an incorrect bank account and checks mailed to the wrong address. Vendors are also experiencing challenges uploading W-9's using VSS, requiring them to email City Purchasing for assistance.

Recommendation 11: Work with the ETS Department to resolve technical issues.

Department Response: Agree. The Office of Procurement agrees that the VSS 4.0 upgrade has been problematic since its go-live and we have escalated such concerns to ETS. However, it has been discovered that until the financial side (CFS) is upgraded, these issues may continue. We are often not aware of EFT issues as they happen and are often looped in after the issue escalated.

Procurement has dedicated a lot of hours testing and implementing patches as issues arrive; this is not a good use of limited staff time, and we are anxious to get this rectified sooner than later.

VSS support for vendors needs to be improved.

Vendors are encouraged to use the VSS application software to register as new vendors and maintain vendor accounts. IA found there is no training available for vendors specifically for establishing and maintaining vendor accounts and highlighting the safeguards in place to protect sensitive banking information. IA was informed that vendors email City Purchasing or call the department with questions about entering banking information in VSS. A lack of training, videos, and reference materials has resulted in vendor frustration, data entry errors, and overall operational inefficiencies.

Additionally, IA was informed the system software can be used to explain entry fields like "ABA", hide fields that the City does not need, and post banner messages to be viewed by all VSS users. Updating the VSS screens and providing support materials will improve vendor effectiveness using VSS and reduce inquiries to City Purchasing.

Recommendation 12: Develop vendor training and support materials for VSS.

Department Response: Disagree. There are training and support materials developed for the Vendor Self-Service System, including a manual and online bidding instructions. The manual was available before the update to VSS happened in November 2021 and due to functionality missing in the update, the manual is no longer visible.

The Office of Procurement does agree that these materials may be outdated and need updated. We have been hesitant to do so until the issue within the system are fixed to what we expected initially from the product. The need for patches on such a consistent basis would require constant updating of the manual and added confusion to vendors. Until this happens, the manual from the software vendor is available on our site.

In addition, our office is readily available to assist with vendor questions, including a fully staffed customer service representative, open office hours with computers available to assist and the ability to screenshare with vendors to assist them visually.

Procurement will work with both Finance and ETS for their respective portions of what should be included in the updated materials.

Recommendation 13: Work with the ETS Department to modify entry screens to make the software easier to use and post banner messages for all VSS users.

Department Response: Disagree. The information provided to IA regarding this functionality is inaccurate. This functionality is not yet operational; this was promised by the vendor at upgrade in November 2021. ETS is aware of the concerns that Procurement has had since go-live. This functionality was a major selling point for us to upgrade and it is disheartening that this functionality is yet to be available.

Central vendor files are not maintained.

Vendors use VSS to establish and change vendor files that are uploaded and saved in CFS. This includes attaching the W-9 required to activate the account and Electronic Funds Transfer Agreement used to set up EFT banking information. IA found vendor documents are saved by date in the Vendor Management File folder for Purchasing, in the appropriate calendar year, on

the shared drive. Central vendor files with all supporting documentation are not available in one place, requiring staff to search various locations for a comprehensive view of vendor account history.

Central files will allow the department staff to quickly search for and access historical records for City vendors. Central files can also be used to save emails, letters, notes, and correspondence, creating an audit trail that can be referred to when needed. IA was informed that the attachment function in CFS can be used to save historical documents with vendor records.

Recommendation 14: Work with the ETS Department to develop a central file system to store historical records for vendors.

Department Response: Disagree. Per the record retention requirements, Finance is to keep all EFT documents for vendors. As the data entry point for this information, Procurement did develop its own internal files for these records by year, which we currently have easily assessable and on our secure network. However, we agree that secure banking information should not be housed with Procurement as it does pose a potential risk, nor should we internally be able to see that information either. The separation of duties between Finance and Procurement will limit that information to the financial people who need access to this sensitive information.

The VSS system is supposed to keep these records electronically. Issues discovered since the upgrade in November 2021 have prevented much of this functionality from going live.

Vendor banking information is accessible to CFS users.

Fraud involving the exploitation of valid online banking credentials is a significant risk facing any local government that processes financial transactions. Access to vendor banking information could allow a bad actor to impersonate the legitimate user, initiating a fraudulent e-transaction. Management is responsible for ensuring resources are managed and properly used in compliance with laws and regulations, programs are achieving their objectives, and services are provided efficiently, effectively, and safely.

Vendor account and banking information is stored in CFS. With a quick search, IA found sensitive banking information can be viewed by CFS users, providing the opportunity for theft or fraud.

Recommendation 15: Work with the ETS Department to develop internal controls limiting access to vendor account and banking information in CFS.

Department Response: Disagree. Procurement is not aware that this information is visible; currently we manage the vendor record in VSS. What is shown on the financial side and who has access to what is foreign to us. This is a role/rights issue in the financial system and we have no control over this function. Additionally, the established process is for agencies to create customer accounts which may contain EFT information.

Purchasing has experienced turnover in key department positions.

Management defines succession and contingency plans for key roles to help the entity continue achieving its objectives, working to recruit, train, mentor and retain competent staff. IA found Purchasing is experiencing turnover in key positions responsible for supporting City vendors and

City departments. These individuals have access to sensitive vendor accounts and banking information for all City vendors, increasing the risk of fraud.

Resignations of staff in key positions weakens the internal control systems required to maintain a level of security when working with vendor records. Management should continually assess the knowledge, skills, and ability needs of the entity so that the organization is able to obtain a workforce that has the required knowledge, skills, and abilities to achieve the organization's goals.

Recommendation 16: Management should demonstrate a commitment to recruit, develop, and retain individuals to fill key positions within the department.

Department Response: Agree. Procurement has done this consistently. The issues in this audit are not due to staff turnover but rather due to inconsistencies and outdated practices of how this information is gathered, entered and verified. Responsibility of the EFT function needs to be defined and responsibilities outlined for this operation to be successfully executed across all city agencies.

III. Conclusion

EFT is a digital movement of money from one bank account to another. As a digital transaction, there is no need for paper documents. EFT has become a predominant method of money transfer since it is a simple, accessible, and direct method of payment or transfer of funds. As businesses increase their usage of EFT, paper checks become obsolete due to expense, slow expedition, and overall effort.[10]

The audit revealed several opportunities for Purchasing to strengthen the internal controls over the EFT process. IA recommends establishing policies and procedures and including escalation protocols for fraudulent activities, implementing best practices for safeguarding EFT transactions, providing vendor training, and resolving software issues. Implementing these internal controls and best practices will ensure proper safeguards are in place to mitigate the loss of City funds.

[10] EBANX Website, https://business.ebanx.com/en/resources/payments-explained/electronic-funds-transfer-eft.

IV. Office of Procurement Response

As noted in the conclusion, EFT is a digital movement of money from one bank account to another – in this vase from the City's banking account as payment for goods/services to the banking account of the vendor. While the Office of Procurement is a compliance agency, compliance is financial policies and procedures is not within our wheelhouse. We maintain the vendor records, but the direction (convert to mandatory EFT for all vendors), the EFT form, authorization to handle fraudulent activities (forms exist in the Treasury Office) and knowledge of best practices in banking activities comes from the Finance Department.

A more robust analysis is needed to achieve the desired outcome of this audit, which is to protect the City from fraudulent activities, especially related to sensitive banking information. Procurement is happy to participate in further discussion in this regard.

Recommendation 1: Comprehensive policies and procedures for the EFT process should be documented, communicated, and enforced.

Department Response: Disagree. Policies and procedures of this nature would need to be written and provided by Finance as procurement staff have no background or expertise in statutory or legal requirements as they relate to banking practices. These may already exist in Finance but are not a part of procurement's role in this function. In the current state, we only enter the banking information; we manage the record.

After a recent fraud incident, the Office of Procurement did put in an internal policy to attempt to verify information. We went back to the previous 6 months of EFTs submitted to manually telephone the company and verify with a person of authority that information was correct. We continue this process for all new EFT requests that come in outside of the VSS system.

Recommendation 2: Work with the Finance Department to develop and communicate escalation procedures for fraudulent activity to City departments.

Department Response: Disagree. These procedures exist and reside within the Finance Department. Procurement is not even aware when checks are returned, no matter the reason. Again, procurement staff do not have the training or knowledge as it relates to banking information. The investigation should happen within Finance and be reported to procurement to lock/freeze the vendor record.

Recommendation 3: Develop an internal verification process to validate changes of vendor identity, contact, and payment information prior to approval in CFS.

Department Response: Agree. Procurement is in agreement that this is a vulnerable area. We propose that VCM documents containing initial or modification changes to EFT-related fields enter a separate CFS workflow or be initially entered by Finance staff if not entered through the system. Finance would provide the banking verification approve the VCM. It would then be routed to Procurement for review and approval of all other entries in the vendor record. This would address the separation of duties and would shift the verification of financial information to the appropriate department.

Recommendation 4: Develop a plan to address the backlog of VCMs, prioritizing the highest risk VCMs first.

Department Response: Disagree. This finding is not accurate as it relates to the Office of Procurement. Procurement was unaware that there were VCMs that were “stuck” in the system. ETS indicated to IA during their interview that there was no issue with the system and that everything was in good working order; however, within a few days of that interview, Procurement’s work list showed 2,348 VCM’s dating back to 2018 that were released by the financial system.

This should no longer be an issue and Procurement has already addressed the backlog. We have been in contact with ETS to work to make sure that this doesn’t happen again.

Procurement is currently working through this backlog and will completed by the end of the fiscal year. We have addressed the high priority requests and are working through the remaining.

Recommendation 5: Establish deadlines for approving VCMs so vendor information is updated in a timely manner.

Department Response: Disagree. Procurement checks daily for outstanding VCMs and addresses them accordingly, typically within 3-5 business days at most. This is currently being done; the backlog mentioned in Recommendation 4 is skewing the number. In addition, Procurement is not aware when there are system failures and VCMS are not pushed through. We are continually working with ETS to make sure that the system is working properly and that necessary patches are being provided by the vendor of the financial system.

Recommendation 6: Establish and maintain a segregation of duties within the department.

Department Response: Disagree. Segregation, especially when dealing with banking and financial information is a crucial component to combatting fraudulent activity. However, as noted in recommendation 1, procurement staff do not have credentials to accurately verify banking/financial information. Our recommendation on how to protect the City is documented in recommendation #3 as follows: VCM documents containing initial or modification changes to EFT-related fields enter a separate CFS workflow or be initially entered by Finance staff if not entered through the system. Finance would provide the banking verification and then approve the VCM. That VCM would then be routed to Procurement for review and approval of all other entries in the vendor record.

Recommendation 7: Work with the Finance Department to improve the flow of information regarding returned and rejected EFT payments and ensure compliance with Ordinance 297-2002.

Department Response: Disagree. Procurement cannot know nor should we be responsible when we are not notified from the Finance department when EFTs are returned or rejected or when City departments do not contact us – we are unaware of the policy mentioned above. We are responsible for vendor management; we can inactive the vendor or prevent new spending when there is an issue with an EFT; however, without notification by Finance and updating by the vendor of their EFT record, we would not know that payment is being help up in violation of the prompt pay ordinance.

Recommendation 8: Establish internal controls and procedures to monitor vendor account activities used to process financial transactions.

Department Response: Disagree. See Recommendation 1 and response. The Office of Procurement staff have no training, background or expertise in this financial area.

Recommendation 9: Work with the Finance Department and the ETS Department to develop a verification process for banking information.

Department Response: Disagree. While there is pre-note functionality in our current financial system, Procurement would have no access to the banking information and verification under Treasury's authority to effectively provide support for this feature. This used to be a function used by the City until ETS was informed by Finance to inactivate the feature. Procurement is in favor of reactivating the pre-note function as we are in agreeance it will substantially cut down on errors and potential fraud.

Recommendation 10: Develop ongoing training for all City staff with access to vendor banking information to ensure they have the knowledge and resources to effectively manage the EFT process.

Department Response: Disagree. See Recommendation 1 and response. The Office of Procurement staff have no training, background or expertise in this financial area.

Recommendation 11: Work with the ETS Department to resolve technical issues.

Department Response: Agree. The Office of Procurement agrees that the VSS 4.0 upgrade has been problematic since its go-live and we have escalated such concerns to ETS. However, it has been discovered that until the financial side (CFS) is upgraded, these issues may continue. We are often not aware of EFT issues as they happen and are often looped in after the issue escalated.

Procurement has dedicated a lot of hours testing and implementing patches as issues arrive; this is not a good use of limited staff time, and we are anxious to get this rectified sooner than later.

Recommendation 12: Develop vendor training and support materials for VSS.

Department Response: Disagree. There are training and support materials developed for the Vendor Self-Service System, including a manual and online bidding instructions. The manual was available before the update to VSS happened in November 2021 and due to functionality missing in the update, the manual is no longer visible.

The Office of Procurement does agree that these materials may be outdated and need updated. We have been hesitant to do so until the issue within the system are fixed to what we expected initially from the product. The need for patches on such a consistent basis would require constant updating of the manual and added confusion to vendors. Until this happens, the manual from the software vendor is available on our site.

In addition, our office is readily available to assist with vendor questions, including a fully staffed customer service representative, open office hours with computers available to assist and the ability to screenshare with vendors to assist them visually.

Procurement will work with both Finance and ETS for their respective portions of what should be included in the updated materials.

Recommendation 13: Work with the ETS Department to modify entry screens to make the software easier to use and post banner messages for all VSS users.

Department Response: Disagree. The information provided to IA regarding this functionality is inaccurate. This functionality is not yet operational; this was promised by the vendor at upgrade in November 2021. ETS is aware of the concerns that Procurement has had since go-live. This functionality was a major selling point for us to upgrade and it is disheartening that this functionality is yet to be available.

Recommendation 14: Work with the ETS Department to develop a central file system to store historical records for vendors.

Department Response: Disagree. Per the record retention requirements, Finance is to keep all EFT documents for vendors. As the data entry point for this information, Procurement did develop its own internal files for these records by year, which we currently have easily assessable and on our secure network. However, we agree that secure banking information should not be housed with Procurement as it does pose a potential risk, nor should we internally be able to see that information either. The separation of duties between Finance and Procurement will limit that information to the financial people who need access to this sensitive information.

The VSS system is supposed to keep these records electronically. Issues discovered since the upgrade in November 2021 have prevented much of this functionality from going live.

Recommendation 15: Work with the ETS Department to develop internal controls limiting access to vendor account and banking information in CFS.

Department Response: Disagree. Procurement is not aware that this information is visible; currently we manage the vendor record in VSS. What is shown on the financial side and who has access to what is foreign to us. This is a role/rights issue in the financial system and we have no control over this function. Additionally, the established process is for agencies to create customer accounts which may contain EFT information.

Recommendation 16: Management should demonstrate a commitment to recruit, develop, and retain individuals to fill key positions within the department.

Department Response: Agree. Procurement has done this consistently. The issues in this audit are not due to staff turnover but rather due to inconsistencies and outdated practices of how this information is gathered, entered and verified. Responsibility of the EFT function needs to be defined and responsibilities outlined for this operation to be successfully executed across all city agencies.