



Staff Report

TO: City Council
FROM: Jeff Mohlenkamp, Finance Director
DATE: July 7, 2020
SUBJECT: Adoption of Electronic Funds Transfer (EFT) Policy

Background and Analysis:

Staff has prepared a policy to address electronic funds transfers (EFT). This policy was reviewed by the Finance and Audit Committee on June 8, 2020. The Committee suggested a few minor modifications and recommended the policy be brought before the City Council for consideration as amended. This policy provides processes required to initiate an electronic payment to a third party. It also provides direction regarding any modifications to existing payment arrangements. This policy, included as Attachment B, was created to provide the necessary internal controls to ensure EFT payments are completed only after they are authorized and that any changes to payment instructions are completed only after a full review.

This policy has been prepared by staff in response to an audit finding by the City's external auditors. The single audit report which includes the audit finding is attached as Attachment A. The pertinent portion of the report is included below:

Finding 2019-003 Unauthorized Wire Transfers

During the year, the City was subject to a fraudulent payment scheme by a fictitious vendor posing as an authorized vendor of the City. The perpetrator submitted a request for payment change with new routing and bank account information along with a voided check in the amount of \$525,038. This was all done on what appeared to be the real vendor's company letterhead. These invoices were processed through the normal cash disbursements cycles and wire payments were made. The bank account and routing number in the vendor master file were updated by the Accounting Technician without a second level of review in order to make the payment. Before the wire transfers were processed and cleared, the bank notified the City and the City was able to recover \$485,417.

Criminals today are using a variety of techniques, such as phishing e-mails and malware, to take control of business accounts to initiate payments to an accomplice or a foreign account. According to the 2015 survey of the Association for Financial Professionals, 2015 AFP Payments Fraud and Control Survey: Report of Survey Results, 2015. Bethesda, MD, 27 percent of respondent organizations were affected by wire transfer fraud (a nearly 100 percent increase from the 2014 survey), and 10 percent were affected by automated clearing house (ACH) credit fraud (fraud involving an ACH payment order initiated by the person sending the payment).

Status of Corrective Action:

The City has developed a policy regarding electronic funds transfer (EFT) that clearly requires approval of the senior accountant prior to any change in vendor payment instructions. Further, staff are required to complete a secondary verification with the vendor via a phone call to a known and established contact prior to executing any change in payment instructions. Pursuant to the new policy, if fraud is suspected, the Finance Director and City Manager are to be immediately notified and steps initiated with the bank to mitigate the fraud. This policy was effective beginning December 2019.

The City has been operating under a draft policy for several months to address the concerns raised in the audit finding. This policy is now being presented to the City Council for adoption following a review by the Finance and Audit Committee and the incorporation of suggested modifications.

Fiscal Impact:

There is no fiscal impact from this item.

Recommended Action:

It is recommended the City Council review the EFT Policy and either direct changes or adopt the policy.

Attachments:

- A. Single Audit Report for FY 2019
- B. EFT Policy
- C. Vendor Authorization Form (EFT transactions)