INSPECTOR GENERAL ALERT

PAYMENT DIVERSION

October 23, 2020 **Report # OP-2101**

Situation

In the fall of 2019, an individual fraudulently claiming to be a representative of a City vendor e-mailed a City employee and inquired as to when payment for services would be made by the City. The individual knew enough information about the vendor to convince the City employee to initiate a change in vendor banking information (i.e., payment routing). The change in vendor banking information was communicated to Financial Services, and the change was processed based on the City employee's request. As a result, future payments to the vendor were diverted to a fraudulent account. Financial Services did not become aware of the payment diversion scheme until January 2020, when the vendor inquired about past due invoices.

Actions Taken

Once Financial Services became aware of the payment diversion, they attempted to recover the funds and referred the matter to the Tallahassee Police Department.

In response, Financial Services implemented a new process for changing ANY vendor information. The new process requires all changes to vendor information (including banking information) be sent directly from the vendor to vendors@talgov.com. Vendor Administration staff will verify the data by contacting the vendor directly. Additionally, Financial Services will no longer accept new vendor requests or changes in vendor information requests from City staff.

Current Status

The diverted funds have not been recovered and, as of the issuance of this alert, the Tallahassee Police Department has completed its investigation and referred the matter to the U.S. Secret Service for further investigation.

Red Flags

Red flags are warning signs which can alert us to the possibility something is wrong or needs additional investigation. In this case, the red flags that something may have been wrong with the request to change the City vendor's banking information were:

- E-mail address – look closely. The individual fraudulently claiming to be City vendor's representative used an e-mail address that was very similar to the vendor's actual e-mail address. With just a quick glance, the fraudulent e-mail address could easily be mistaken for the vendor's.
- Poor grammar and excessive errors in punctuation, capitalization. and misspellings are often indication of fraudulent communications. Normally legitimate business communications will have very few if any errors in grammar, punctuation, capitalization, and spelling.
- Pressure to act quickly– The individual fraudulently claiming to be City vendor's representative sent multiple e-mails demanding payment in quick succession (almost daily). Typically, legitimate vendors make an inquiry and then if payment is not received in a reasonable period of time will make contact again, days or possibly weeks later.

What You Can Do

If, during the course of performing your duties, you become aware of these or any red flags which cause you concern, or if you have any questions, please contact the Office of the Inspector General by phone (850-891-8397) or by e-mail (inspector.general@talgov.com).