

# **OFFICE OF THE INSPECTOR GENERAL**

## **CITY OF BALTIMORE**



**Isabel Mercedes Cumming**  
**Inspector General**

## **Investigative Report Synopsis**

**OIG Case # 25-0028-I**

**Issued: August 27, 2025**



OFFICE OF THE INSPECTOR GENERAL  
Isabel Mercedes Cumming, Inspector General  
City Hall, Suite 635  
100 N. Holliday Street  
Baltimore, MD 21202



August 27, 2025

Dear Citizens of Baltimore City,

The mission of the Office of the Inspector General (OIG) is to promote accountability, efficiency, and integrity in City government, as well as to investigate complaints of fraud, financial waste, and abuse.

On March 19, 2025, the OIG received a complaint that City of Baltimore (City) electronic fund transfer (EFT) payments intended for a City vendor (Vendor) were diverted to a potentially fraudulent bank account.

### **BACKGROUND**

The Department of Accounts Payable (AP) manages City payments and disbursements, excluding payroll and debt management. AP functions were previously under the Bureau of Accounting & Payroll Services (BAPS) in the Department of Finance (DOF) but were officially moved under the Comptroller's Office in January 2023.

On August 8, 2022, the City implemented Workday as its procurement and supplier platform to replace its previous purchasing and invoice systems. Through Workday, suppliers can view and create invoices, access payments, respond to requests for quotes, and maintain data such as contact information, addresses, and bank accounts. Suppliers can submit a supplier contact form to add, update, or remove contacts from their Workday profile. The Bureau of Procurement (BOP) and AP manage the contact change requests.

### **INVESTIGATION**

#### *Fraudulent Transactions and the City's Response*

Between February and March 2025, AP completed two EFT payments totaling \$1,524,621.04 to a bank account not associated with or authorized by the Vendor. A fraudulent user (Fraudster) gained access to the Vendor's Workday account and changed its financial institution (Vendor's Bank) to another financial institution (Fraudster's Bank).

The OIG confirmed that on February 21, 2025, and March 10, 2025, AP completed two EFT payments, one for \$803,384.44 and the other in the amount of \$721,236.60. The total amount of fraudulent transactions amounted to \$1,524,621.04. The City was able to retrieve the \$721,236.60 payment but at the time of this report, has been unable to recover the \$803,384.44 payment from the Fraudster's Bank. AP filed an insurance claim related to that payment, and the Vendor was reissued payments for both EFT transactions.

On March 13, 2025, the City's financial institution (City's Bank) notified DOF about a call they received from the Fraudster's Bank regarding potential fraud. Upon DOF's notification, AP personnel informed the Vendor about the fraudulent activity. Baltimore City Information and Technology (BCIT) removed the Fraudster's account from Workday, and a temporary hold was placed on the Vendor's account while BCIT investigated the account.

#### **REPORT FRAUD, WASTE AND ABUSE**

HOTLINE: 443-984-3476/800-417-0430 EMAIL: [OIG@BALTIMORECITY.GOV](mailto:OIG@BALTIMORECITY.GOV) WEBSITE: [OIG.BALTIMORECITY.GOV](http://OIG.BALTIMORECITY.GOV)

*This public synopsis is only a summary of a more comprehensive report of investigation submitted to the appropriate City management official*

The OIG received the fraud complaint on March 19, 2025, approximately six (6) days after the Comptroller's Office received the notification. The OIG requested additional information from AP on March 21, 2025. AP provided the OIG with a summary of the fraudulent activity on March 24, 2025, and noted that the Baltimore Police Department (BPD) would be contacted that day. After learning AP did not successfully make contact with BPD, the OIG spoke with law enforcement on March 31, 2025, so a criminal investigation could be initiated.

On April 1, 2025, a media interview with the Comptroller's Office was published about the fraudulent activity. During the interview, it was stated that the Fraudster bypassed the City's geofencing by using an IP address set up through Starlink.<sup>1</sup> However, interviews with BCIT staff indicated that Starlink did not impact the Fraudster's Workday access. The OIG confirmed that BCIT submitted a notification of the activity to another law enforcement entity. However, the OIG learned that the City did not verbally speak with the law enforcement entity or follow up with them.

#### *Fraudster's Access to Workday*

On December 9, 2024, the Fraudster submitted a supplier contact form to gain access to the Vendor's Workday account. The name on the supplier form matched that of a Vendor employee. The Vendor's President confirmed that the employee the Fraudster posed as does not have a role in, or access to, the Vendor's financials. The email provided on the form by the Fraudster was not the Vendor employee's company-issued email address.

The OIG confirmed that on December 11, 2024, an AP employee (AP Employee 1) reviewed and approved the Fraudster's contact form and added them to the Vendor's Workday account. AP Employee 1 stated they verified the information provided by the Fraudster on the form; however, Workday records indicated that some Vendor information supplied by the Fraudster was incorrect. A different Vendor employee (Vendor Contact) was listed as the Vendor's point of contact in Workday at the time of the fraudulent activity. AP did not contact the Fraudster or the Vendor Contact to confirm the Fraudster's identity. According to AP Employee 1, verifying email addresses and calling suppliers were not AP protocol at the time of the fraudulent activity. The OIG did not find evidence that the Fraudster was an employee of the Vendor or the City.

On December 11, 2024, the Fraudster attempted to change the Vendor's Bank to the Fraudster's Bank. They made multiple subsequent attempts. The Fraudster submitted a voided check in the Vendor's name for the Fraudster's Bank on January 4, 2024, and created a bank account change request to add the Fraudster's Bank to the Vendor's Workday account. The OIG determined that the voided check submitted was fraudulent.

The Fraudster submitted another bank account change request on January 7, 2025. Another AP employee (AP Employee 2) reviewed and approved it on January 10, 2025. AP Employee 2 told the OIG they did not recall viewing the voided check. According to Workday records, a third AP employee (AP Employee 3) approved the bank account request. AP Employee 3 did not recall viewing the voided check submitted by the Fraudster.

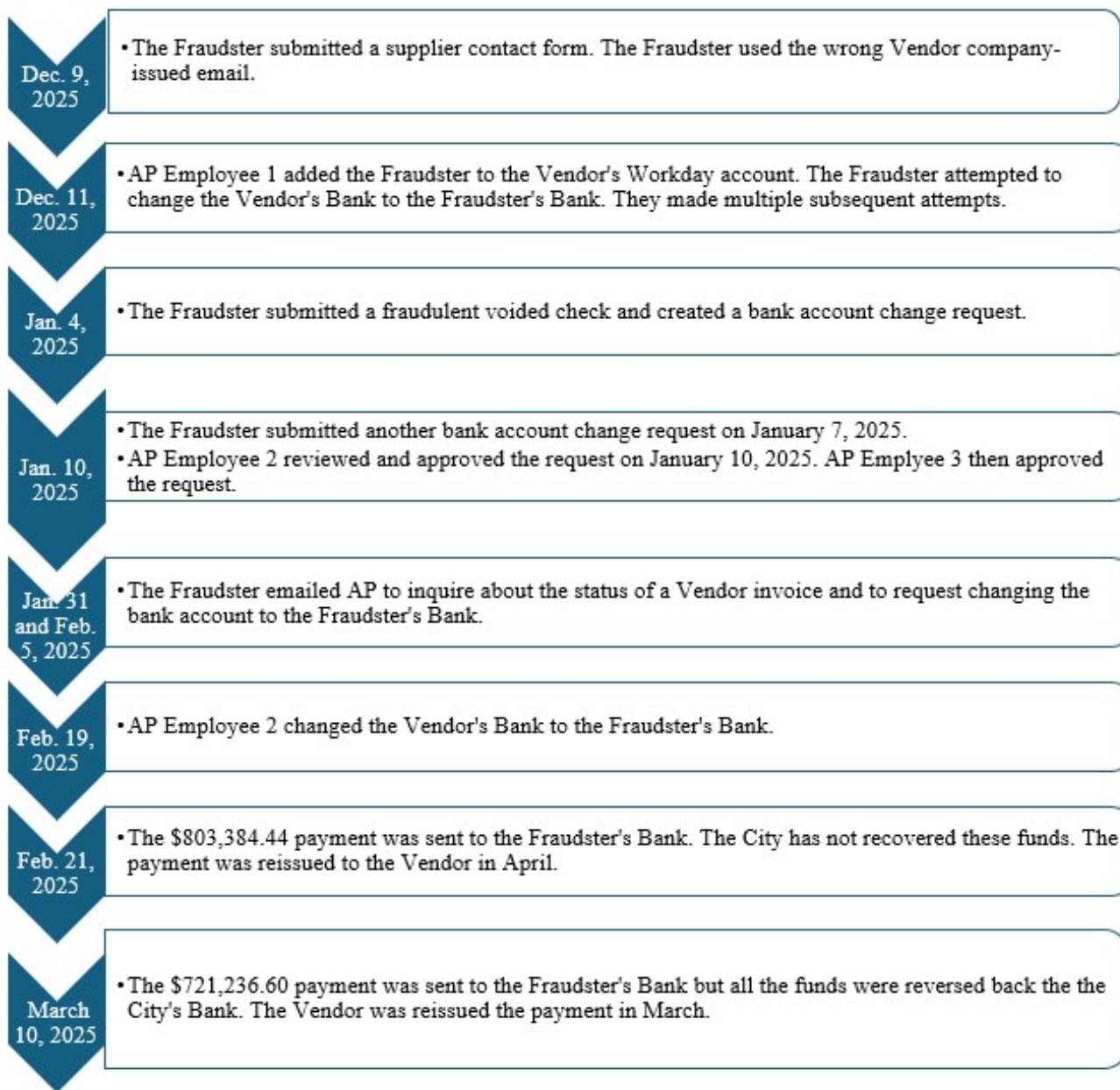
The OIG reviewed correspondence between AP personnel and the Fraudster during January and February 2025 that showed the Fraudster requested the Fraudster's Bank account to be listed as the Vendor's active

---

<sup>1</sup> Starlink is a satellite constellation system that provides internet coverage.

bank. According to Workday, AP Employee 2 changed the Vendor's Bank to the Fraudster's Bank on February 19, 2025.

#### *Timeline – Fraudster's Access to Vendor's Workday Account and Funds*



#### *Lack of Internal Processes*

The OIG received copies of AP policies in place during this fraudulent activity, but the AP policies did not address the steps taken when verifying account changes. The OIG found that AP employees were not required to call vendors to confirm their identity and did not have a list of signatories for vendors. The OIG also found internal controls within Workday could be improved and made recommendations to AP.

The OIG investigated similar fraud incidents in 2020 and 2022 due to a lack of internal controls within

#### **REPORT FRAUD, WASTE AND ABUSE**

HOTLINE: 443-984-3476/800-417-0430 EMAIL: [OIG@BALTIMORECITY.GOV](mailto:OIG@BALTIMORECITY.GOV) WEBSITE: [OIG.BALTIMORECITY.GOV](http://OIG.BALTIMORECITY.GOV)

*This public synopsis is only a summary of a more comprehensive report of investigation submitted to the appropriate City management official*

the Bureau of Accounting and Payroll Services (BAPS).<sup>2</sup> Office of the Comptroller leadership told the OIG that changes may have been made in the City's previous accounting system as a result of the OIG's previous investigations, but those changes were not implemented when the City transitioned to Workday. Since the discovery of the fraudulent activity in the OIG's current case, AP staff informed the OIG that they are now required to call suppliers when requests to change banking information are made.

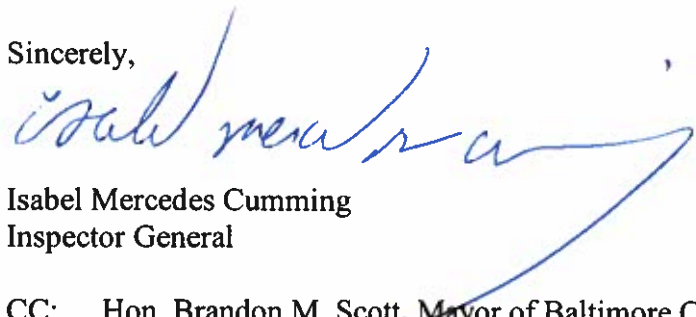
### **Investigative Findings**

The OIG found that between February and March 2025, two fraudulent payments totaling \$1,524,621.04 intended for the Vendor were diverted to the Fraudster's bank account. The Vendor has been reissued both payments at the time of this report. The City has not received any funds from the \$803,384.44 payment. AP has submitted an insurance claim related to the \$721,236.60 payment to the Bureau of Risk Management, and the OIG has referred this matter to law enforcement.

The investigation revealed a lack of internal policies and procedures in AP regarding supplier verification. The OIG determined that the internal controls established as a result of the former OIG investigations were not being utilized at the time of these incidents. The OIG strongly recommended that AP create a list of authorized users for supplier accounts. At the time of this report, AP informed the OIG that new policies have been implemented for internal review processes. The investigation revealed that AP staff should receive training in handling supplier bank information and recognizing the signs of fraud, particularly related to fraudulent checks.

Lastly, the OIG advises City agencies to develop policies that require immediate reporting of suspected fraud or theft to the OIG. Prompt reporting is essential to avoid hindering investigations, as time is a critical factor in theft cases.

Sincerely,



Isabel Mercedes Cumming  
Inspector General

CC: Hon. Brandon M. Scott, Mayor of Baltimore City  
Hon. Zeke Cohen, Baltimore City Council President  
Hon. Bill Henry, Baltimore City Comptroller  
Honorable Members of the Baltimore City Council  
Hon. Ebony Thompson, Baltimore City Solicitor

---

<sup>2</sup> OIG Cases 20-0015-I and 22-0009-I

**Office of the Comptroller  
Response  
Case # 25-0028-I**





**BILL HENRY**  
**OFFICE OF THE COMPTROLLER**

City Hall – Room 204  
100 Holliday St Baltimore, MD 21202

**To:** Isabel Cumming, Inspector General  
**From:** Timothy Goldsby, Director of Accounts Payable  
**Date:** July 31, 2025

---

**Re: Agency Response to OIG Case #25-0028-I – Fraudulent Supplier Account Access and EFT Diversion**

The Department of Accounts Payable (AP) acknowledges the findings outlined in the Office of the Inspector General's Report of Investigation #25-0028-I regarding the diversion of electronic funds originally intended for a legitimate supplier. We thank the OIG for its diligent investigation, as well as our partners in the Bureau of Treasury Management (Treasury), Bureau of Procurement (Procurement), Baltimore City Office of Information and Technology (BCIT), the Office of Risk Management, and the Office of the City Administrator (CAO). Their collaborative efforts to address this incident reflect a shared commitment to safeguarding public funds through stronger oversight, accountability, and modernized controls.

AP concurs with the Inspector General's assessment that the incident was enabled by vulnerabilities in verification procedures and insufficient supplier account safeguards. We also acknowledge that controls recommended in previous reports were not fully institutionalized prior to AP's transition from the Department of Finance to the Office of the Comptroller in January 2023.

Once made aware of the fraudulent transactions, AP immediately conducted an internal audit of the supplier's Workday activity, worked with BCIT to deactivate the fraudulent user's business contact account, notified the legitimate supplier, and collaborated with the Bureau of Treasury Management to initiate partial payment recovery. We also attempted to contact BPD's Cybercrime Unit; however, per the OIG, the contact information used was outdated.

AP then convened an interagency workgroup consisting of BCIT, Procurement, Treasury, and the City Administrator's Office. To address this incident, ensure the security of supplier accounts and strengthen the rigor of the City's processes, this workgroup has implemented a series of both immediate and long-term reforms which include:

**1. Internal Controls and SOP Development**



- Full revision and implementation of a new SOP for supplier contact and banking updates;
- Mandatory cross-verification with supplier contacts for all banking changes;

## **2. Workday Safeguards**

*The following safeguards have been tested and approved by BCIT and will be implemented in August 2025.*

- Creation of a restricted user role authorized to initiate sensitive updates to supplier profiles;
- Automated email alerts to all listed supplier contacts upon pending profile changes;
- Introduction of a 48-hour approval delay with layered reviews for settlement account modifications;
- Flags and alerts for rapid, duplicate, or unusual activity on supplier profiles.

## **3. Enhanced Verification and Oversight**

- Ongoing conversations between Treasury and [REDACTED] to add additional bank account validation tools into the City's existing contract with [REDACTED]
- Expanded training for AP staff on fraud detection and social engineering red flags;
- Daily monitoring of supplier activity within Workday to detect anomalies.

Our office will continue to evaluate opportunities for systemic improvement and share lessons learned with other City agencies as part of a broader risk management strategy.

Sincerely,

*Timothy L. Goldsby, Jr.*

**Timothy L. Goldsby, Jr.**

**Director – Accounts Payable**

Assistant Deputy Comptroller

Office of Comptroller Bill Henry

O: 410-396-0930

C: 410-598-8499

Web: [Comptroller.BaltimoreCity.gov](http://Comptroller.BaltimoreCity.gov)

E-mail: [timothy.goldsby@baltimorecity.gov](mailto:timothy.goldsby@baltimorecity.gov)

100 N. Holliday St., Baltimore MD 21202