Office of the Auditor General
City of Hamilton

AUD25005

Accounts Payable Special Investigation #2:

Investigation Summary (Fraud and Waste Report #71958)

Charles Brown, Auditor General
Ken Froese, Delta Consulting Group

Audit, Finance and Administration Committee - May 22, 2025

What We Did

- Gained an understanding of the incident involving alleged fraudulent payments of over $274,000 over a period of approx. 2 months.

- Gained an understanding of operational processes regarding Accounts Payable.

- Procured Delta Consulting Group Canada Ltd. to complete the investigation on our behalf, while providing investigation support and maintaining oversight of the investigation process to ensure quality and value were received.

The Incident

- In November 2023, the City received an email from a person, posing as a vendor, to change a vendor's bank account details that were used for electronic funds transfer. The banking changes were processed, diverting any future payments to the fraudster's account.

- A second email was received from the same person in late December 2023/early January 2024, posing as a vendor, to change (again) the vendor's bank account details use for electronic funds transfer. The banking changes were processed diverting any future payments to the fraudster's account.

- In February 2024, the real vendor called the City, claiming they had not received any payments since mid-November 2023.

The Investigation

- The incident was reported to the Auditor General who informed Council in a confidential “Serious Matters Report”. OAG reported it to Hamilton Police Service.

- With the assistance of Delta Group and the City’s Legal Services, funds were traced to multiple bank accounts through Norwich Orders – a court order that compels a third party to produce relevant documents – in this case bank account information.

- The investigation included the use of Norwich Orders, which is a court order that compels a third party to produce evidence in its possession – in this case the banks that were in receipt of funds allegedly procured by fraud. This allowed deposit and banking transaction and ownership details to be obtained.

The Findings

- The investigation found that the vendor did not have any connections with the fraudulent transactions, and in fact had fallen victim to a “Business Email Compromise” scam. An unknown perpetrator was successful in hacking into their computer system and manipulating their emails.

- The Accounts Payable department had three specific opportunities to detect the business e-mail compromise that resulted in the loss to the City, including two vendor bank account change requests and a return of $84,150 from one of the bank accounts which was replenished to another newly opened bank account.

- We found no evidence of any involvement in the fraud by City of Hamilton employees. Rather, City employees made mistakes, overlooked red flags, and did not follow due diligence procedures emphasized in fraud-related training provided a few months prior to the fraudulent transactions.

The Findings - Continued

- No funds were recovered despite the combined efforts of the OAG, our investigator Delta Consulting, and City Hamilton Legal Services.
- The $274,000 of funds were quickly transferred out of the relevant bank accounts.
- Based on information that was collected we believe the fraud was carried out by a person or persons in the United States, using bank accounts in Canada of so-called dupes, or accounts opened with synthetic identities that were created using manipulated identity documents obtained through identity theft.
- The OAG provided its information and reports to Hamilton Police to further their investigation.

Ken Froese, Senior Managing Director

Delta Consulting Group Canada Ltd.

Delta Consulting - Investigation Summary

- Delta Consulting Background
- Investigation Mandate from OAG: investigate alleged fraudulent payments of over $274,000.
    - Review of documentation, interviews with relevant staff and vendors, obtaining Norwich Orders, Mareva Injunction.
    - What happened, what was recovered.
- Investigation findings and recommendations.
    - What internal control issues may have contributed to the issue.
    - What the current risk environment is for these type of issues.

Repeat Recommendations

1) We recommend that the City's Accounts Payable department keep an updated profile of vendor information, including authorized signatories and vendor contact information. Only the vendor's authorized signatory should be permitted to initiate a vendor information change.

2) That Accounts Payable staff use only contact information on the City's vendor profile or vendor invoices (independent of the completed EFT Form) to communicate and confirm vendor information changes. Additionally, we recommend that Accounts Payable staff avoid replying directly to the email request but rather initiate a new email communication with the vendor using the contact information on file.

3) That Accounts Payable staff confirm the identity of the requestor before proceeding with any vendor information change – only an authorized signatory should be permitted to initiate vendor information changes. For example, Accounts Payable staff may ask questions to have the vendor's authorized signatory verify vendor profile information on file, such as its old bank account number, prior vendor payment history or prior invoices.

Repeat Recommendations - Continued

4) That the EFT Form be amended to include the vendor's old bank account information and/or last payment information to deter a scammer from submitting the request without the required information.

5) That Accounts Payable staff familiarize themselves with a standard void cheque and independently verify banking information such as transit branch number and address of the branch, and ensure it is consistent with other vendor information in the circumstances (for example, locations of operations etc.).

6) That all Accounts Payable staff dealing with vendor information change and payments processing receive training on risks related to business email compromise and the need to independently verify vendor information change or requested payments to avoid further losses to the City.

Additional Recommendations

1) We recommend that all Accounts Payable staff dealing with vendor information change and payments processing receive additional periodic training on risks related to business email compromise and “red flags”.

2) We recommend that all vendor bank account changes require a detailed review by a Supervisor with adequate training to detect red flags and anomalies in possible business email compromises and to ensure the vendor been appropriately contacted to confirm the request. We further recommend that the review be appropriately documented prior to updating vendor records.

3) We recommend that the City develop a process to verify appropriate vendor contacts with City departments to ensure that Accounts Payable staff contact appropriate vendor personnel in relation to vendor change requests.

4) We recommend that the City review the current Fraud Policy and Protocol and update the policy based on lessons learned subsequent to June 2019 in relation to investigative and recovery-related procedures and protocols.

Conclusion

- Six recommendations were previously made to the Financial Services Division. We repeat these recommendations and make an additional three recommendations.
    - Management agreed with all recommendations.
- Management is currently working on implementing their management responses.
- OAG is recommending that Council directs the General Manager to report back was a status update by November 2025.

Conclusion - Continued

- One recommendation was made to the OAG to update the Fraud Policy and Protocol.
    - OAG agreed with the recommendation. The Policy update is an agenda item today.


OFFICE OF THE AUDITOR GENERAL
CITY OF HAMILTON
ESTABLISHED IN 2012

THANK YOU