Office of the Auditor General
City of Hamilton

Accounts Payable Special Investigation #2 (Fraud and Waste Report #71958)

Summary, Recommendations, and Management Responses

May 22, 2025

Charles Brown, Auditor General
Brigitte Minard, Deputy Auditor General
Delta Consulting Group

Management Responses provided by Finance and Corporate Services.

Contents

Investigation Summary

In late November 2023, the City of Hamilton received an email from a person, posing as a vendor, asking to change the vendor’s banking information for payments (known as Electronic Fund Transfers, or EFTs). After exchange of emails, and the submission by the imposter of the required forms and documentation, the vendor’s banking information was changed.

About a month later, another email request came in from the imposter asking to change the vendor’s banking information for payments in January. Again, after some exchange of emails, and submission of the required forms and documentation, the vendor’s banking information was changed for a second time.

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

Ultimately, several payments totalling over $274,000 had been diverted to a fraudster’s two bank accounts.

City of Hamilton Accounts Payable informed the Office of the Auditor General (OAG) of the incident, and the OAG reported the matter to the Hamilton Police Service. A “Serious Matter” Report was then provided to Council in late February 2024 (AUD24002). The OAG engaged Delta Consulting Group Canada Ltd. (Delta Consulting) to complete an investigation on behalf of the Office of the Auditor General.

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, including receiving, sending, and intercepting emails using their email account. This enabled them to pose to the City as a legitimate vendor.

A business email compromise (BEC) scam is a type of cybercrime where attackers gain access to and/or make use of a company’s email system. The main components include:

- **Unauthorized access:** Attackers may obtain access to the target’s email system, either by stealing login credentials or using other methods.
- **Impersonation:** Once the attacker is inside, they study communication patterns and identify key people.
- **Social Engineering:** The attacker then uses the information obtained to impersonate trusted individuals in the company and send fraudulent emails that seem legitimate.
- **Deceptive Requests:** The fraudulent email contains a request to do something that is “urgent” (e.g. transfer money) or make changes to banking information.

- **Financial Loss:** The target may not detect the scam and may comply with the request. If changes to banking information were made, payment is sent to the attacker’s bank account.

Source: ChatGPT, December 18, 2023, search term: “explain business email compromise scam in plain language”, edited and summarized by Office of the Auditor General for initial use in Report AUD24001.

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 funds were traced to multiple bank accounts, including one in another city, and we continued to follow the money until the funds were found to be dissipated. A Mareva Injunction was also used so that any funds that were located could be frozen. However, the investigation found that the funds were quickly depleted out of the relevant bank accounts.

Ultimately, the City made payments totalling $274,243.48 to two illegitimate vendor bank accounts in the November 27, 2023 to January 29, 2024 period. The vendor did not notice that payments were not being made which exacerbated the fraud. The Accounts Payable department had three specific opportunities to detect the business e-mail compromise that resulted in the loss to the City, including the 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.

Ultimately no funds were recovered despite the combined efforts of the OAG, our investigator Delta Consulting, and City Hamilton Legal Services. Any recoveries are expected to be nominal, as the fraudsters’ bank accounts have minimal remaining account balances.

We found no evidence of any involvement in the fraud by City of Hamilton employees. However, 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 investigation was completed and 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. Stolen identity information is bought and sold on the dark web.

The Hamilton Police Service were provided with our investigation report for use in their investigation, and the OAG, with the assistance of Delta Consulting, set out to identify how procedures could be improved to prevent future occurrences, and to minimize such risk. This report summarizes our findings and conclusions.

This is the second such incident that the OAG has investigated. The previous investigation summary (Report AUD24001) included six recommendations. These recommendations are again repeated here because they are again relevant to this investigation, along with four additional recommendations. Management agreed with the previous recommendations. The observations and corresponding recommendations are included below:

Previous Recommendations

1. Authorized Vendor Personnel for Vendor Information Change

Recommendation 1

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.

Management Response - Update

Agree.

The medium-term enterprise resource planning (ERP) system implemented in Q2 2025 includes a workflow approval for all new vendor requests. Furthermore, the system includes a 2-level workflow approval for all new bank records and bank changes. In addition, banking change procedures include the requirement for documented approvals, including the signature of an officer of the vendor who has the authority to bind the organization. Furthermore, these procedures include the additional step of direct contact with the vendor, using suitable contact information. Additionally, verification questions to those confirming bank details will be asked. This further validates that the information provided is correct and not from a single source.

Expected Completion: Completed.

2. Vendor Communications on Information Change

Recommendation 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.

Management Response - Update

Agree.

Accounts Payable staff have been trained to verify requestor information. Staff are trained and are required to use appropriate vendor contact information. Staff have been trained which source(s) of contact information is appropriate, including the exclusion of the vendor phone number on the EFT change form.

Staff will be trained to initiate a new email communication with vendor using the appropriate contact information when actioning any vendor information changes. Furthermore, all bank changes still require a verbal confirmation using the procedures put in place.

Expected Completion: Q2 2025.

3. Confirmation Procedures of Vendor Information Change

Recommendation 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.

Management Response - Update

Agree.

Accounts Payable staff have been trained to verify requestor information by verbally contacting vendor using appropriate vendor contact information, excluding the EFT change form. Vendor contact information will include documentation executed by an officer who has authority to bind the company.

Under the newly implemented medium-term (ERP) solution the Accounts Payable department has built in a two-level approval process which includes one supervisor or delegate approving. All bank requests and changes require two levels of approval by trained staff. Accounts payable staff use a standard form with verification questions to ask vendor when requests for bank changes come through. Approvers verify processes were followed and information changed was accurately updated and documented.

Accounts Payable does not hold a signatory listing for vendors. To mitigate risks to the City, all bank changes require the EFT change request form to be signed by an officer who has binding authority. Verbal verification is done to ensure information is correct and not completed by a single source.

Expected Completion: Completed.

4. Information Required on the EFT Form

Recommendation 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.

Management Response - Update

Agree.

The EFT change form has been updated. Vendor is required to verify old banking information and/or prior payment history as well as additional information.

Expected Completion: Completed.

5. Review of Information on the Void Cheque

Recommendation 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.).

Management Response - Update

Agree.

Accounts Payable staff are required to verify transit branch number and address of branch are consistent with vendor location of operations. Staff are required to verbally confirm bank changes with vendor using appropriate contact information.

Under the newly implemented medium-term ERP solution, Accounts Payable has built in a two-level approval process which includes a supervisor or delegate approving. All

bank requests and changes require two levels of approval by trained staff. Prior to making any bank changes, Accounts payable staff ask vendor verification questions. Approvers will verify processes were followed and information changed was accurately updated and documented.

Expected Completion: Completed.

6. Training of Accounts Payable Staff

Recommendation 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.

Management Response - Update

Agree.

Accounts Payable procedural training took place in 2023 on vendor file changes. Additional fraud prevention training was also conducted with Accounts Payable staff and was extended to city wide employees. Training session topics included impacts of fraud, fraud detection and fraud prevention. This additional training also took place in 2023.

Accounts Payable staff were recently trained on vendor file changes and vendor payment process as part of our newly implemented medium term ERP solution.

The Accounts Payable Manager will ensure regular training is provided to staff annually. New staff will be trained prior to making any vendor changes. Training will include review of procedures, risks of business email compromise and potential red flags to watch for.

Expected Completion: Completed.

Additional Recommendations

Additional Recommendation 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”.

Management Response

Agree.

The Manager of Accounts Payable will continue to keep staff informed of business email compromise and “red flags” related to vendor information change and payment processing. Training will be provided to all Accounts Payable staff who are involved in these processes annually with formal sign off or tracking of attendance. Training will be conducted more frequently if changes in the market occur, or procedures change.

Expected Completion: Completed.

Additional Recommendation 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.

Management Response

Agree.

Under the newly implemented medium-term ERP solution the Accounts Payable department has built in a two-level approval process which includes a supervisor or delegate approving. All bank changes require two levels of approval by separately trained staff. Accounts payable staff will appropriately document all verification questions asked during verbal phone call with vendor. A standard form has been created for Accounts Payable staff to follow. The approvers will ensure form has been completed and appropriate actions taken.

Expected Completion: Completed.

Additional Recommendation 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.

Management Response

Agree.

EFT change form is to be signed by vendor officer that has authority to bind the company. Accounts Payable staff have been directed and trained to confirm contact information from appropriate source(s), excluding the EFT change form. If Accounts Payable staff are unable to verify appropriate vendor contact, they are to reach out to City client area for assistance in contacting appropriate vendor contact information.

Expected Completion: Completed.

Additional Recommendation 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.

Office of the Auditor General Response

Agree.

The Fraud Policy and Protocol has been revised by the OAG and is on the May 22, 2025, Audit, Finance and Administration Committee agenda for review and approval of Committee and Council. The corporate-wide Policy Review Group was consulted and feedback obtained during the revision process.

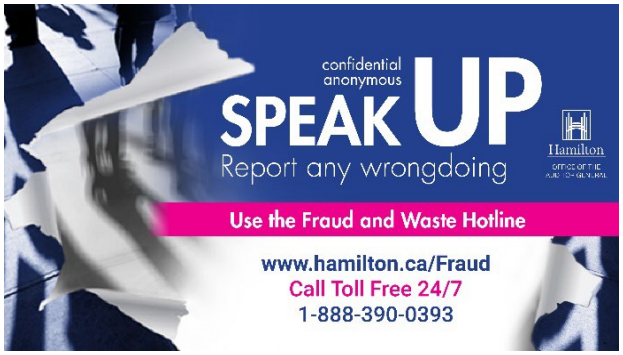
Expected Completion: Completed.

Office of the Auditor General
City of Hamilton

Charles Brown CPA, CA
Auditor General

Brigitte Minard CPA, CA, CIA, CGAP, CFE
Deputy Auditor General

Phone: 905-546-2424 ext. 2257
Email: auditorgeneral@hamilton.ca
Website: hamilton.ca/audit



SPEAK UP – Reporting Fraud and Waste

Online: hamilton.ca/fraud

Phone: 1-888-390-0393

Mail: PO Box 91880, West Vancouver, BC V7V 4S4

Email: cityofhamilton@integritycounts.ca

Fax: 1-844-785-0699

Copies of our audit reports are available at: hamilton.ca/audit

Alternate report formats available upon request.