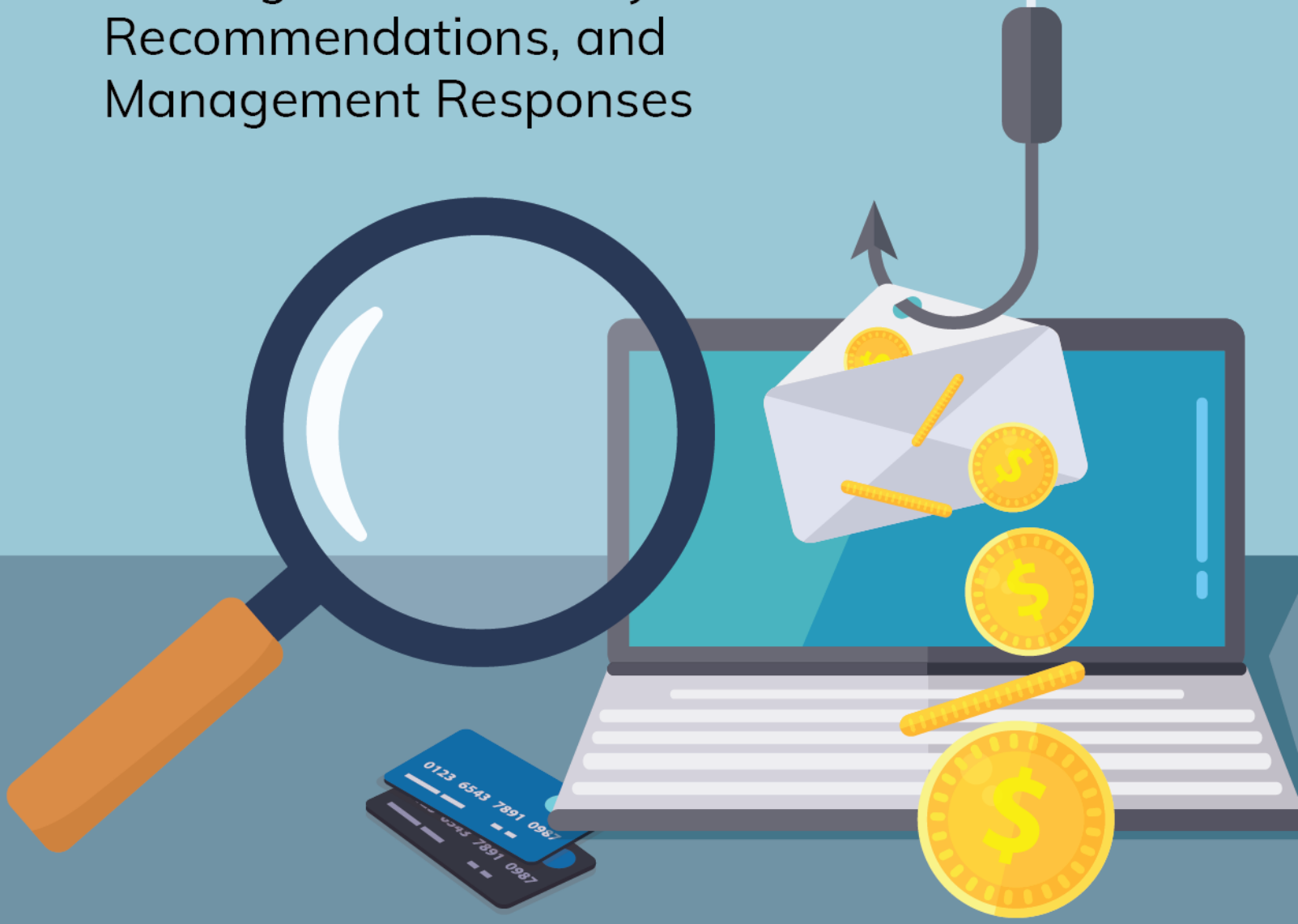
Accounts Payable Special Investigation

(Fraud and Waste Report #65357)

Investigation Summary, Recommendations, and Management Responses



February 22, 2024

Brigitte Minard, Deputy Auditor General
Delta Consulting Group Canada Ltd.

Management Responses Provided by:
Financial Services Division, Corporate Services Department

Hamilton
OFFICE OF THE AUDITOR GENERAL

Investigation Summary

The City of Hamilton received an email request from a person, posing as a vendor, to change the vendor’s banking information for payments (known as Electronic Fund Transfers, or EFTs). After some exchange of emails, and obtaining the required forms and documentation, the vendor’s banking information was changed and a payment of over $52,000 was made to the imposter vendor’s new bank account. The legitimate vendor subsequently inquired as to why they had not received payment which led to the discovery of the fraud.

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 May 2023 (AUD23007). 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.

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, personal communication, December 18, 2023, search term: “explain business email compromise scam in plain language”, edited and summarized by Office of the Auditor General.

The investigation included the use of a Norwich Order which is a court order that compels a third party to produce evidence in its possession – in this case a bank that was in receipt of funds allegedly procured by fraud. This allowed deposit and banking

transaction details to be obtained. The funds were ultimately traced to a bank account in another city, and we determined that the funds were quickly moved out of that account. The Hamilton Police Service were provided with this information 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.

Six recommendations have been made, the observations and corresponding recommendations are included below:

1. Authorized Vendor Personnel for Vendor Information Change

Observation

We were advised by the Accounts Payable staff that anyone from the vendor organization (for example, receptionists) can initiate a 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

Agree.

The current procedure requires new vendors to have their contact information set up in the City’s Accounts Payable vendor file. The Accounts Payable department does not currently track vendor authorized signatories. Accounts Payable staff will work with Procurement and Legal Services to seek their input on how to effectively manage vendor authorized signatories.

In the interim, Accounts Payable staff will contact the individual who signed the electronic fund transfer change form using the vendor information on file. This is the individual who states, “I have the authority to bind the vendor”. Staff will verify the individual is a senior level staff person such as an owner, controller, director, etc. Staff will also have them verbally confirm other information (old banking information, last payment details, HST number, etc.).

A more enhanced audit tracking process is being developed that will track all vendor changes. A second reviewer will verify processes were followed and information changed was accurately updated.

Accounts Payable staff are currently scanning the municipal sector to see what processes are currently in place for vendor information changes. Staff are looking to see how they manage authorized signatories and what technology they leverage for their processes.

The City’s Information Technology division will review current procedures to look for risk points and/or opportunities where information technology equipment could be leveraged to enhance our internal processes, as well as reviewing best practices in the municipal sector.

Estimated Completion: Q2 2024.

2. Vendor Communications on Information Change

Observation

Accounts Payable staff called the telephone number disclosed on the Electronic Funds Transfer (EFT) Form and sent an email to the requestor’s email address for the requestor to call back for confirmation procedures. This information was inconsistent with the vendor profile.

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

Agree.

The current procedure requires an independent confirmation of all changes by verbally contacting the vendor using the vendor information on file. Accounts Payable staff were retrained on procedures in quarter 2 of 2023.

Accounts Payable staff will work with Procurement and Legal Services to seek their input on how to effectively manage vendor authorized signatories.

In the interim, Accounts Payable staff will contact the individual who signed the electronic fund transfer change form using the vendor information on file. This is the individual who states, “I have the authority to bind the vendor”. Staff will verify the individual is a senior level staff person such as an owner, controller, director, etc. Staff will also have them verbally confirm other information (old banking information, last payment details, HST number, etc.).

Procedures will be updated directing staff to initiate a new email communication with the vendor using the contact information on file when dealing with any vendor information changes. All changes still require a verbal confirmation using the vendor number on file.

Expected Completion: Q2 2024.

3. Confirmation Procedures of Vendor Information Change

Observation

Accounts Payable staff are required to verbally confirm vendor information changes with the vendor. This is an appropriate procedure if conducted properly.

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

Agree.

Accounts Payable staff verify requestor information by verbally contacting vendor using vendor information on file. The current procedure has been updated to require vendors to confirm old bank account information and/or last payment details. An audit report for vendor change is reviewed by the Manager of Accounts Payable daily.

Accounts Payable staff will work with Procurement and Legal Services to seek their input on how to effectively manage vendor authorized signatories.

In the interim, Accounts Payable staff will contact the individual who signed the electronic fund transfer change form using the vendor information on file. This is the individual who states, “I have the authority to bind the vendor”. Staff will verify the

individual is a senior level staff person such as an owner, controller, director, etc. Staff will also have them verbally confirm other information (old banking information, last payment details, HST number, etc.).

A more enhanced audit tracking process is being developed that will track all vendor changes. A second reviewer will verify processes were followed and information changed was accurately updated.

Accounts Payable staff are currently scanning the municipal sector to see what processes are currently in place for vendor information changes. Staff are looking to see how they manage authorized signatories and what technology they leverage for their processes.

The City’s Information Technology Division will review our current procedures to look for risk points and/or opportunities where information technology equipment could be leveraged to enhance our processes, as well as reviewing best practices in the municipal sector.

Estimated Completion: Q2 2024.

4. Information Required on the EFT Form

Observation

The EFT Form did not require the requestor to provide vendor’s old bank account information.

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

Agree.

The EFT form has been updated. Vendor is required to provide old banking information and/or last payment details, as well as other additional information.

Completed Q1 2024.

5. Review of Information on the Void Cheque

Observation

The Accounts Payable department requested a copy of a void cheque from the new bank account. However, details of the void cheque were modified by the scammer and the Accounts Payable staff did not independently verify the banking information. For example, the transit branch number was inconsistent with the disclosed branch location.

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

Agree.

Accounts Payable staff are required to verify transit branch number and address of branch using vendor information on file to ensure it is consistent with vendor information. Accounts Payable staff require the vendor to verify old bank account and/or last payment details. Accounts Payable staff verbally verify changes with the vendor using the vendor information on file. Staff were retrained on verifying banking information in quarter 2 of 2023. Staff are continuing to be updated on procedural changes. The Manager of Accounts Payable reviews the audit report for vendor changes daily.

A more enhanced audit tracking process is being developed that will track all vendor changes. A second reviewer will verify processes were followed and information changed was accurately updated.

Estimated Completion: Q2 2024.

6. Training of Accounts Payable Staff

Observation

The Hamilton Police Service advised that business email compromise is a common tool used by scammers to phish or lure fraudulent payments. In this case, the scammer

hacked into the vendor’s email account or set up an identical email account address in order to request payments be made to a fraudulent bank account.

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

Agree.

Accounts Payable procedure has been updated. Upon receipt of an EFT change request, Accounts Payable staff verify old banking information and/or last payment details provided by vendor. The Accounts Payable staff verbally confirm the requested change with the vendor using the vendor information on file. The Manager of Accounts Payable reviews the audit report for vendor changes daily.

Accounts Payable procedural training took place in quarter 2 of 2023. 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. Training took place in quarter 2 of 2023. Staff are continuing to be updated on procedural changes.

Staff will look to develop a training schedule for staff to be retrained on vendor information changes annually or more frequently if procedures change.

Estimated Completion: Q1 2024.