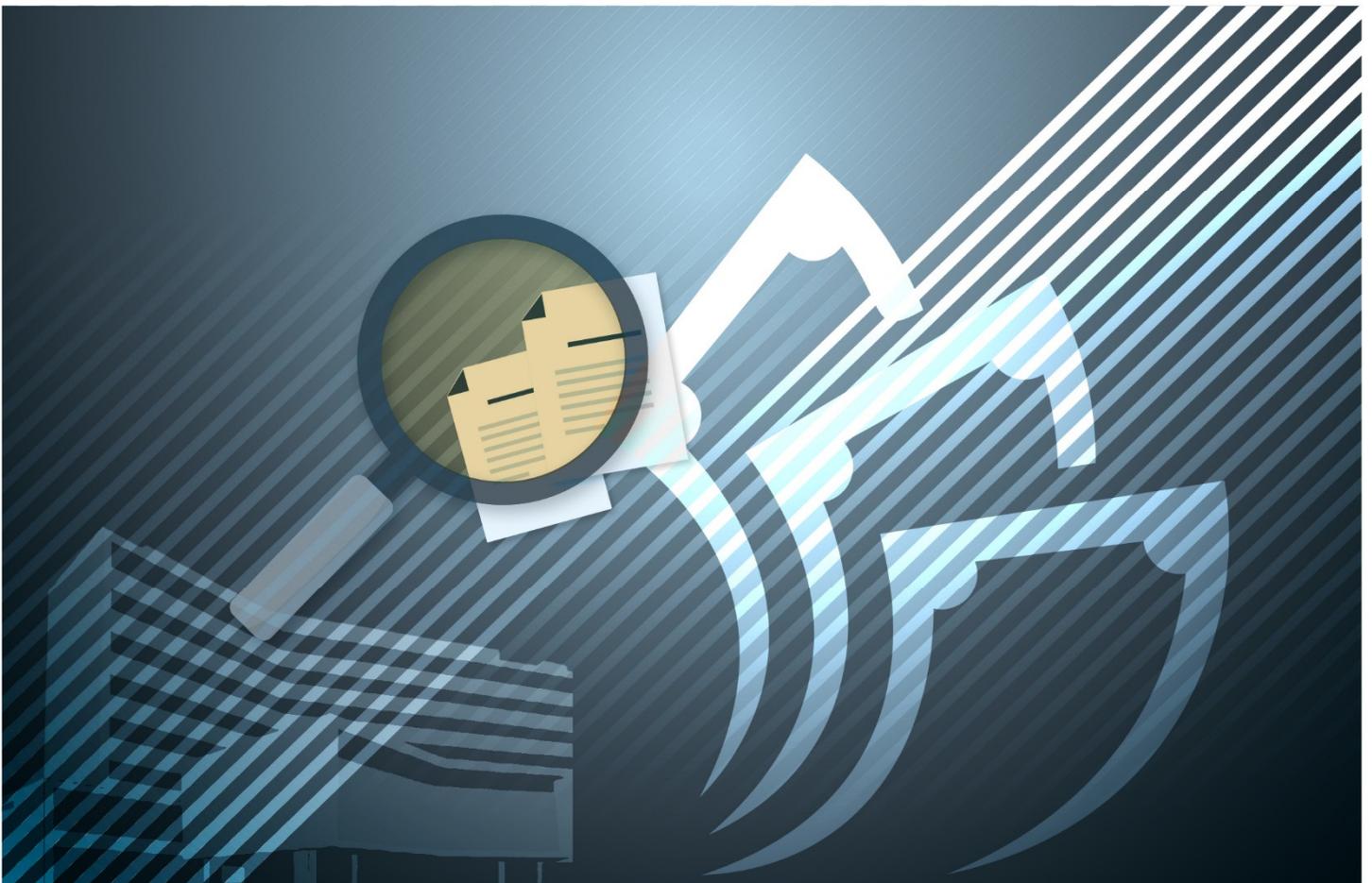




Office of the  
Auditor General  
City of Hamilton

# Accounts Payable Special Investigation: CityHousing Hamilton Investigation Summary (Fraud and Waste Report #73367)



**CityHousing Hamilton Corporation Board of Directors - April 22, 2025**  
**Audit, Finance and Administration Committee - May 1, 2025**

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

## Contents

Investigation Summary .....	3
1. Supervision .....	4
Recommendation 1 .....	5
Management Response .....	5
2. Documentation of Fraud Risks Needed .....	5
Recommendation 2 .....	5
Management Response .....	5
3. Vendor Banking Information.....	6
Recommendation 3 .....	6
Management Response .....	6
4. Capital EFT Payments Were Not Reviewed .....	6
Recommendation 4 .....	7
Management Response .....	7
5. Up-to-Date Signing Authorities Not Maintained.....	7
Recommendation 5 .....	7
Management Response .....	7
6. Centralization of Accounts Payable.....	8
Recommendation 6 .....	8
Management Response .....	8
7. Need for Specialized Training .....	9
Recommendation 7 .....	9
Management Response .....	9

## Investigation Summary

In March 2024, shortly after the City of Hamilton's cyber security incident (a ransomware attack), CityHousing Hamilton (CHH) realized two vendors had their electronic funds (EFT) payment amounts transposed in the data that was submitted to the bank, resulting in one vendor being paid about \$137,000 instead of about \$552,000 (an underpayment of about \$415,000) and the other vendor being paid about \$552,000 instead of about \$137,000 (an overpayment of about \$415,000). Manual workaround processes had been put in place for finance and accounts payable due to the impacts of the cyber security incident.

As a result, CHH was in touch with both of these vendors to resolve the error. However, one of the vendors informed CHH that they had not received any funds at all. Subsequent enquiries led to the discovery that this vendor's banking information had been changed by someone unknown to them, and funds diverted to a different bank account that was not a CHH bank account.

CHH Finance informed the Office of the Auditor General (OAG) of the incident, and CHH reported the matter to the Hamilton Police Service. A confidential "Serious Matter" Report was then provided to Council in April 2024 (AUD24003). 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 CHH had fallen victim to a "Business Email Compromise" scam. An imposter, posing as the vendor, contacted CHH Finance staff via email to change the banking information. Due to a combination of human error, poor process, and elevated risks from workaround procedures put in place in response to the cybersecurity incident the \$552,000 payment was approved for electronic transfer and paid.

In fact, the vendor that did not receive payment had emailed CHH about two weeks prior to the fraudulent incident as a precautionary measure, advising CityHousing Hamilton that they had experienced a security breach and asking CHH to call them if any requests to change their banking were made. Notwithstanding the warning, the imposter's request to CHH for banking changes were processed, and funds were electronically transferred to a bogus bank account.

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 multiple Norwich Orders, which is a court order that compels a third party to produce evidence in its possession – in this case account information for any bank that was in receipt of the funds procured by fraud. This allowed deposit and banking transaction and ownership details to be obtained. The transferred electronic funds were traced initially to a bank account in another city and province, from which they were depleted. OAG continued to use Norwich Orders to follow the monies transferred to other banks until substantial funds were located in one particular bank account, which were frozen through the use of a Mareva Injunction.

Ultimately about \$417,000 of funds have been recovered through the combined efforts of the OAG, our investigator Delta Consulting, City Hamilton Legal Services, CHH, and CHH's legal counsel.

The Hamilton Police Service have been 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.

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

## 1. Supervision

### Observation

The finance staff at CityHousing were not properly supervised, with risky transactions, as elaborated upon below, not subject to review.

## Recommendation 1

We recommend that CityHousing implement a senior level (non-union) supervisor position that requires the supervisor to possess suitable accounting credentials and experience, to assist in the supervision of the finance staff's work.

## Management Response

**Agree.**

CityHousing Hamilton Corporation Board of Directors has approved an FTE to add a Manager (title yet to be determined) position to support the Chief Financial Officer. They will be required to possess appropriate accounting credentials (i.e. CPA or equivalent). Recruitment is expected to be completed in Q4 2025.

Expected Completion: November 2025.

## 2. Documentation of Fraud Risks Needed

### Observation

CityHousing Finance did not properly consider the elevated risks, of both fraud and error, associated with the Cyber Incident as it pertained to making Capital vendor payments by EFT.

## Recommendation 2

We recommend that CityHousing Finance document a set of procedures to mitigate the risks of fraud and error as it pertains to vendor Capital payments made by EFT.

## Management Response

**Agree.**

CityHousing Hamilton updated its a procedure to guide capital payments made by EFT during an emergency to mitigate risks. These updated procedures are being reviewed and will be formalized. The normal (i.e. not associated with the cyber security incident) procedure for capital payments are currently being reviewed as part of the organization's transition back to Arcori Financial.

Estimated Completion: June 2025.

### 3. Vendor Banking Information

#### Observation

The lack of controls around changes to vendor banking information poses a significant fraud risk. The OAG found that there was an inadequate segregation of duties and inadequate review.

#### Recommendation 3

We recommend that vendor banking information be stored securely and locked for editing and that adequate segregation of duties be implemented for this process.

#### Management Response

**Agree.**

The functions of verifying banking information will shift from the FAI (as described below) to the Sr. Risk & Compliance Officer, a non-union position under recruitment and expected to be in place by June 2025.

Pending recruitment, the following system is used. Vendor banking information is view-only for all Finance staff but editable by only the Financial Assistant II (FAII) who have no responsibility or control over vendor payment. Currently, the Financial Assistant I (FAI) or Financial Coordinator will verify vendor banking following the established process (includes calling the vendor and verifying HST and banking information. CFO validates the vendor changes and communicate these to the FAII to update in the system. The Financial Assistant I would then process the capital payments based on the updated and validated banking information.

Estimated Completion: June 2025.

### 4. Capital EFT Payments Were Not Reviewed

#### Observation

We observed that vendor Capital EFT payments, for material dollar amounts, were not being reviewed at multiple stages of the process, which increases the risk of both fraud and error being undetected.

## Recommendation 4

We recommend that the key banking file be reviewed for accuracy and that all vendor Capital EFT payments be authorized/endorsed by the appropriate signing officers prior to their release.

### Management Response

**Agree.**

Currently, the CFO or Financial Coordinator reviews every invoice to every payment prior to release and signs to demonstrate review. The two signing authorities are each required to take an audited approach (10% of invoices) to their review.

Responsibility for this control will reside with the future Manager and allow for another level of audited review by CFO prior to signing off.

Expected Completion: November 2025.

## 5. Up-to-Date Signing Authorities Not Maintained

### Observation

The bank agreement for signing authorities for wire payments required [any] three signatures for payments over \$10,000. The signing authorities included a former CEO and two employees not included in the bank agreement were also provided authorization to approve EFT payments without the bank agreement being updated. The signatures also did not require the CFO or CEO to authorize payments over a specific dollar amount (such as \$100,000).

### Recommendation 5

We recommend that bank agreements be reviewed and updated whenever employee responsibilities change and whenever changes in employment impact employees who are added or removed from positions with signing authority. We also recommend that CityHousing consider requiring the CFO or CEO to be one of the signing officers for payments over a predetermined threshold.

### Management Response

**Agree.**

CHH will implement this recommendation following an analysis to determine the appropriate predetermined threshold.

Estimated Completion: December 2025.

## 6. Centralization of Accounts Payable

### Observation

The matter at hand is the third vendor fraud experienced by the City and its boards and agencies in less than one year. The OAG recently completed control walk-throughs of the accounts payable departments at each of the Hamilton Public Library, Corporate Accounts Payable, and CityHousing locations. Control deficiencies were identified in all three departments, and that processes are not executed in a consistent manner.

### Recommendation 6

We recommend that the City consider centralizing Accounts Payable or key functions performed by Accounts Payable such that resources can be used most efficiently and processes can be harmonized. We recommend that, at a minimum, the processes associated with new vendor additions and vendor banking changes that are not already centralized be considered for centralization.

### Management Response

#### Alternative To Be Implemented.

Without understanding the details of such an arrangement, CityHousing Hamilton Corporation (CHH) does not agree with this recommendation. However, CHH sees value in the spirit and substance of this recommendation and suggests periodically working with the City's Accounts Payable team to review its practices, share knowledge and harmonize procedures where appropriate.

CHH has been approved to procure and implement a new and comprehensive tenant and financial software system which is widely used by similar organizations and includes enhanced financial controls. As a large landlord, CHH has complex accounts payable needs ranging from vendors for capital projects, routine service contracts to individual tenants, averaging 350 invoices per week. The system is designed to handle this volume but also include flexibility to be able to issue refund payments quickly to individual, often vulnerable, tenants.

Estimated Completion: January 2027.

## 7. Need for Specialized Training

### Observation

Consistent with the OAG's previous investigation findings, business email compromise is a common tool used by scammers to phish or lure fraudulent payments. In this case, the scammer created an illegitimate email account, the sole difference being the pluralized form of the word "constructions", and requested payments be made to a fraudulent bank account.

During our investigation, it was clear that CityHousing Finance did not fully appreciate the potential fraud risks associated with EFT vendor payments in general, and more specifically the risks associated with updating banking information; therefore, CityHousing Finance did not govern itself accordingly.

### Recommendation 7

We recommend that all Accounts Payable staff dealing with vendor information change and payments processing receive additional training on risks related to business email compromise and the need to independently verify vendor information changes in order to avoid further losses to the City.

### Management Response

#### Agree.

Current staff are required to complete all mandatory training offered through the City of Hamilton. There is no outstanding training related to cyber security at this time. In addition, this team includes discussions about fraud at its bi-weekly meetings.

CHH is also implementing a comprehensive training program which will be offered through My Learning Connection and will require staff to complete training and sign off on a variety of policies and procedures.

Estimated Completion: September 2025.



**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](mailto:auditorgeneral@hamilton.ca)

**Website:** [hamilton.ca/audit](http://hamilton.ca/audit)



**SPEAK UP – Reporting Fraud and Waste**

**Online:** [hamilton.ca/fraud](http://hamilton.ca/fraud)

**Phone:** 1-888-390-0393

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

**Email:** [cityofhamilton@integritycounts.ca](mailto:cityofhamilton@integritycounts.ca)

**Fax:** 1-844-785-0699

Copies of our audit reports are available at: [hamilton.ca/audit](http://hamilton.ca/audit)

Alternate report formats available upon request.