Ottawa

Office of the Auditor General

Investigation into the Transfer of Funds to a Fraudulent Supplier

Tabled at Audit Committee
April 8, 2019

Table of Contents

Acknowledgements

The team responsible for this investigation, comprised of PricewaterhouseCoopers LLP under the supervision of Ed Miner, Deputy Auditor General and the direction of Ken Hughes, Auditor General, would like to thank those individuals who contributed to this project, and particularly, those who provided insights and comments as part of this investigation.

Original signed by:

Auditor General

Executive summary

Purpose

This investigation was conducted in response to the Office of the Auditor General ("OAG") receiving a report relating to the City's transfer of US$97,797.20, to an alleged fraudulent supplier under fraudulent pretenses (the "fraudulent payment").

The overall objectives of the investigation were as follows:

1. Conduct a fact-finding investigation surrounding the receipt of request for payment and the resulting payment process with respect to the fraudulent payment;
2. Determine if fraudulent payments, similar to this fraudulent payment, may have been processed before; and
3. Review the controls in place related to these processes and recommend improvements where required.

With the OAG's concurrence, the matter was also reported by the City to the Ottawa Police Service ("OPS").

Background and rationale

The City's Treasury Branch processes wire transfer payments to all vendors with foreign bank accounts, as the accounts payable module of the City's financial system is currently unable to facilitate Electronic Funds Transfers (EFT) in US funds.

On July 6, 2018, the General Manager, Corporate Services and City Treasurer (the "City Treasurer"), received an email (the "Email") apparently from the City Manager. The Email, which was later identified as a spoofed email[1], requested that a wire transfer in the amount of US$97,797.20 (the "Funds") be processed for the completion of an acquisition.

With the City Treasurer's approval, later that day the request was processed, and the Funds were issued.

[1] Email spoofing is the forgery of an email address so that the message appears to have originated from someone other than the actual source. Correspondence is received by the alleged fraudster's actual email address.

On July 11, 2018, the City Treasurer received further email correspondence, again apparently from the City Manager. The email requested that the balance of the payment (US$154,238) relating to the acquisition be issued that morning.

The City Treasurer proceeded to discuss the matter with the City Manager who advised her that he had no knowledge with respect to the wire transfer requests.

The City did not process the alleged fraudster's July 11, 2018 wire transfer request, and the City Treasurer immediately notified the City's Technology Security Branch of the fraudulent payment incident.

Findings

The findings as a result of the investigation along with the proposed recommendations are as follows:

1. Identification of fraud scheme – the "fake CEO scam"

Cyber criminals have been attacking organizations globally with a common fraud scheme called the "fake CEO scam". In these attacks, which is what the City fell victim to in relation to the fraudulent payment, the fraudsters send realistic-looking emails, requesting urgent wire transfers for what appear to be legitimate business reasons, like "securing an important contract", "a confidential transaction" or "updating a supplier's payment information".

Believing that the request is real, the employee transfers the money, only to find out later that the email was a scam and the money is gone.

Losses to this type of scam typically range from tens of thousands to millions of dollars. The fake CEO scam is a growing global threat to businesses and organizations of all sizes.

2. No identification of email source (internal versus external)

At the time of the fraudulent payment incident, emails received by City employees did not reflect the source in terms of being an internal City or external sender. Providing such identification can heighten the recipient's awareness of spam or other suspicious emails, which may used for phishing[2] or contain dangerous malware.

[2] Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Technology Security staff are requesting that the groups responsible for the email exchange server in network operations and the cloud implement a mechanism to visually identify all emails coming from an external source.

3. Commended Technology Security response

Immediately upon being notified by the City Treasurer of the fraudulent payment incident, and prior to the OAG commencing its investigation, the Technology Security Branch implemented their response in accordance with their Computer Incident Response Plan.

The Technology Security Branch's procedures performed included: notifying the City's Legal Services and the OAG, confirming the use of a spoofed email address, conducting email searches, controlling future email correspondence from the alleged fraudster, preservation of emails and meeting with OPS to file a report.

Technology Security fully cooperated with the OAG as part of this investigation and provided all documentation obtained from their incident response to the OAG. Recognizing that Technology Security took the initial lead prior to the OAG assuming responsibility for the Investigation, they are commended for their prompt actions, demonstrating their readiness to address unfortunate computer incidents.

4. Non-compliance with the City's *Payment to Vendors Policy* and *Payments to Vendors Procedure*

The City's *Payment to Vendors Policy* (the "Policy") and *Payments to Vendors Procedures* (the "Procedures") outlines the procedures to be followed in relation to processing payments. We found that the Policy and Procedures were not fully complied with.

The City Treasurer acknowledged that the Policy and Procedures were not complied with in relation to processing the fraudulent payment as the City Manager has the ability to override a policy in an urgent situation. It was her position that she was complying with City Manager's request pursuant to the content of the emails, which she believed were legitimate.

The Delegation of Authority By-law (the "By-law") does contain sections in relation to "*Emergency or Special Circumstances*".

We enquired with the former and current City Managers both of whom stated that they have never directly requested that either a payment be processed by Accounts Payable or a wire transfer by Treasury Branch. The current City Manager stated that he believes

that there is some authority to request urgent payments; however, there are a number of criteria to be met, including subsequent immediate reporting of such payments to Council.

5. Inadequate controls with respect to wire transfer process

We found dangerous control weaknesses with respect to wire transfer processes. We conducted specific forensic investigative procedures to assess whether prior fraudulent wire transfer payments similar to the fraudulent payment scheme may have occurred.

Below are our findings in relation to the specific forensic investigation procedures conducted:

- There was no evidence of any other fraudulent payments being issued, similar to the fraudulent payment scheme.
- All of the transactions we analysed had adequate supporting documentation. However, while the supporting documentation contained signatures of the approver, their identities could not always be determined as their names were not printed.
- City procedures provided effective segregation of duties with respect to the person creating the wire transfer request and the Treasury staff approving and releasing the wire transfer in the RBC banking system (the “RBC System”).
- Wire transfer documentation is filed on a per transaction basis. Wire transfer summary reports are not prepared nor reviewed by senior management.
- The wire transfer RBC System is not directly integrated to the City’s SAP system. Wire transfer payments can be processed without a general ledger account to allocate the payment to or even an entry in the financial system.
- There are no formal written City authorization limits (approval rules) with respect to wire transfer payments.
- To setup a wire payment, an authorized individual first creates it within the RBC System. The individual who created the payment then provides the supporting documentation to an approver and requests that they approve it within the RBC System. If the transaction is less than $25 million, the payment is then released upon approval. If the transaction is greater than $25 million, the payment is held awaiting a second approver. The creator then takes the supporting documentation to a second approver and requests that they approve it within the RBC System. Upon the second approval, the transaction is automatically released.

- Authorization limits are set within the RBC System and can be changed at any time by a Treasury Branch employee with administrative access rights.
- We were informed by Treasury Branch staff that the segregation of duties controls in the RBC System prevented the same user from both creating and approving a wire transfer. Notwithstanding this, we requested that Treasury Branch perform a test to confirm that this could not occur within the RBC System. This test found that it actually could occur as there was no such control in the RBC System. Any one of five authorized individuals could on their own both create and release a wire transfer up to $25 million. This represented a very dangerous control weakness. Staff stated that this control weakness has since been remedied.

6. Prior fraudulent wire transfer attempt

In the spring of 2018, the City was the target of a prior attempted fraud scheme, similar to this fraudulent payment incident.

A spoofed email, purporting to be sent by the CEO of the Ottawa Public Library, was sent to the City Treasurer requesting a wire transfer of funds.

Treasury Branch staff reviewed the email and requested more information with respect to the wire transfer request as the email did not contain the required banking information.

The Ottawa Public Library CEO was contacted to provide the additional banking details and responded that she had not sent the original email. The wire transfer was not completed. The matter was not reported to Technology Security or to the OAG.

7. OPS response

On July 11, 2018, Technology Security met with an OPS Constable to complete a police report with respect to the fraudulent payment incident and the alleged fraudster's subsequent email correspondence requesting a further US$154,238. At the time of the report, the alleged fraudster was continuing to correspond with the City Treasurer, and Technology Security suggested that OPS take a proactive role in continuing with the communication in an attempt to identify the perpetrator. The OPS Constable assigned advised that he did not have any cyber-security experience. The OPS Constable contacted his colleagues to advise them that there was a live situation. Technology Security advised us that the response provided to the Constable from his colleagues was that the wire transfer was completed, and they could not provide any assistance. As a result, the City ceased all communication with the alleged fraudster.

Technology Security staff indicate that there has been no follow-up by the OPS with respect to this matter.

8. Recovery proceedings

The recipient of the fraudulent payment was a suspect bank account at a bank located in the United States (the "First American Account"). Most of these funds were transferred from the First American Account to another bank account in the same recipient name, held at a different bank also located in the United States (the "Second American Account". Unbeknownst to the City, the Second American Account was being monitored by the United States Secret Service ("USSS") as it was related to fraudulent transfers connected to other American bank accounts.

On or about August 3, 2018, the City was contacted by the USSS, as the funds in the Second American Account had been seized. The USSS advised that funds in the Second American Account can be traced to the fraudulent payment; however, not all of the funds from the City are on deposit. The USSS estimated that approximately US$88,000 was recovered from the Second American Account, but noted that these funds were comingled with funds received fraudulently from another victim of a similar incident to that of the City.

The City Solicitor has taken carriage of this matter and filed the required Petition for Remission or Mitigation of Forfeiture (the "Petition") with the USSS, asserting the City's claim on the funds on deposit in the Second American Account. On November 5, 2018, the USSS Ottawa advised the City Solicitor that a ruling on the Petition will be made by the appropriate US authorities after the investigation and review has been completed.

9. Lack of fraud awareness training

The City does not have a mandatory fraud awareness training program for staff. Such a program assists with the prevention, detection and reporting of fraud. All interviewees stated that fraud awareness training would be beneficial and may have prevented the fraudulent payment from happening.

In January 2018, the findings from a Technology Security phishing test[3] reflected a 26.5 per cent failure rate which is above the industry average of 15 per cent. Technology

[3] A phishing test is where deceptive emails, similar to malicious emails, are sent by an organization to their own staff to gauge their response to phishing and similar email attacks.

Security staff further advised that the City of Toronto is in the process of rolling out a mandatory fraud awareness training program to its employees.

Conclusion

The City fell victim to a common fraud scheme. There is no indication of any fraudulent wrongdoing by City staff related to this incident. There is also no indication of other similar fraudulent wire-transfer payments being processed from October 3, 2016 to October 17, 2018.

Had the City's Policy and Procedures been followed, the fraudulent payment request would have been documented on a Payment Without Reference Form and gone through either Accounts Payable or the Financial Services Unit. In our opinion, it is unlikely that the payment would have been made had either of these groups processed the request.

The City is fortunate that the USSS was monitoring the Second American Account as recovery of any funds by victims of these fraud schemes is extremely rare.

Lastly, the City's controls over issuing wire transfers require significant improvement.

Recommendations and responses

Recommendation #1

That the City implement a process to identify external emails received by staff and display this to the recipient in an obvious manner.

Management response:

Management agrees with the recommendation.

ITS / Technology Security is currently piloting potential solutions with implementation expected in Q3 2019.

Recommendation #2

That the City finalize and approve policy and procedures which require that all wire transfer payments be processed, reviewed and approved by either Accounts Payable or a Financial Services Unit.

Management response:

Management agrees with the recommendation.

Treasury is working with Accounts Payable (AP) to update the Payment to Vendors Policy and Procedures, to incorporate specific policies and procedures for wire transfer payments. This will be completed by Q2 2019. In the interim, Treasury met with AP and the FSU to confirm that going forward they will review and approve all requests for wire transfer payments, prior to processing.

Recommendation #3

That the City issue a communication to all management clarifying that they do not have the authorization to override controls and will be held accountable for non-compliance.

Management response:

Management agrees with the recommendation.

Corporate Finance will work with Procurement to develop a communication to all management that reinforces the financial and procurement policies, procedures and controls in place for authorizing payments to vendors. The communication will be developed and issued by the City Manager's Office to all managers by Q1 2019.

Recommendation #4

That the City ensure that physical approvals are adequately documented for future reference i.e. confirmation that physical signatures are legitimate (compared to a signature specimen sheet) and names printed.

Management response:

Management agrees with the recommendation.

Treasury staff responsible for wire transfer processing now have access to the SAP Signature Authority platform so that they can verify and match all specimen signatures approving a payment by wire transfer.

Treasury is working with Accounts Payable to update the Payment to Vendors Policy and Procedures, to incorporate specific policies and procedures for wire transfer payments to ensure that physical signatures are legitimate and adequately documented and, that there is an audit process to ensure compliance. This will be completed by Q2 2019.

Recommendation #5

That the City prepare monthly summary reports with respect to the wire transfers created and released. These reports should be reviewed and signed off by a senior finance officer and kept on file for future reference. Any identified anomalies should be reported immediately to the Office of the Auditor General.

Management response:

Management agrees with the recommendation.

Monthly activity reports are currently available from existing systems, including Wire Payments, Account Transfers and Administrative activity reports. The new roles and responsibilities for this process will be implemented in Q1 2019. Documentation of this process will be incorporated into the new wire transfer payments section of the updated Payment to Vendors Procedures to be completed by Q2 2019.

Recommendation #6

That the City review its current practices and establish formal authorization limits/approval rules with respect to the issuance of wire transfer payments. Delegate an appropriate owner for these rules who will be accountable to ensure that they are properly established and maintained in the financial institution's system.

Management response:

Management agrees with the recommendation.

Formal authorization limits/approval rules with respect to the issuance of wire transfer payments and roles and responsibilities for maintaining these rules will be included in the new wire transfer payments section of the updated Payment to Vendors Procedures to be completed by Q2 2019.

Recommendation #7

That the City coordinate with their financial institution to deactivate the ability for Treasury Branch employees, who have been assigned administrative rights, to change access/authorization rights. All changes to access/authorization rights should be made by the financial institution only upon receiving written instructions from an authorized senior City official.

Management response:

Management agrees with the recommendation.

Treasury staff have discussed this recommendation with the financial institution and they have indicated that this is not a responsibility they are prepared to assume. They insist that it is up to the client to identify appropriate internal administrators to manage authorities.

Corporate Finance will review the segregation of duties and administrative rights of Treasury Branch, determine best practices and implement the controls, segregation of duties and clear roles and responsibilities required for assigning administrative rights by Q2 2019.

Recommendation #8

That the City make changes to its authorization profiles in the financial institution's system so that no one City employee can both create and approve the same wire transfer transaction and verify that these changes are effective.

Management response:

Management agrees with the recommendation.

The ability of any one employee to both create and approve a wire transfer in the financial institution's system has been removed except for those with administrative rights, based on how the banking system works. Implementing Recommendation 7 will ensure that there is appropriate segregation of duties and controls in place to ensure those with administrative rights cannot create or approve a wire transfer. These changes in roles, responsibilities and procedures will be implemented and included in the new wire transfer payments section of the updated Payment to Vendors Procedures to be completed by Q2 2019.

Recommendation #9

That the City report all attempts to defraud the City where City staff have corresponded with and/or begun taking the requested action, to the Office of the Auditor General.

Management response:

Management agrees with the recommendation.

ITS / Technology Security is currently developing a corporate-wide mandatory cyber awareness training program. A Request for Proposal was issued and awarded for the development of a cyber awareness training program, which will include the requirement to report fraud. Implementation is expected by Q2 2019.

Recommendation #10

That the City create and implement a fraud awareness training program which would encompass the Code of Conduct, the risk of fraud, the employees' role in preventing and reporting fraud.

Management response:

Management agrees with the recommendation.

As indicated in the response to Recommendation 9, ITS / Technology Security is currently developing a corporate-wide, mandatory cyber awareness training program for implementation by Q2 2019. This program will encompass the Code of Conduct, the risk of fraud and the employee's role in preventing and reporting fraud.

In the interim, ITS has developed messaging for staff to better recognise and delete phishing and other security risks they may encounter. An email was sent to all networked staff on October 4, 2018 informing them of these risks. Furthermore, articles were sent corporate-wide via the City's e-newsletter *In the Loop* on July 24, 2018 and information is posted on the City's intranet Ozone, which staff are required to view before proceeding to the landing page. As part of the cyber security awareness program, ITS will deliver quarterly messages to staff that are relevant to risks the City is encountering.

Detailed investigation report

Investigation into the Transfer of Funds to a Fraudulent Supplier

Introduction

On July 11, 2018, the Office of the Auditor General ("OAG") of the City of Ottawa (the "City") received a report relating to the City's transfer of funds, totaling US$97,797.20, to an alleged fraudulent supplier under fraudulent pretenses (the "fraudulent payment").

Under the City's *Fraud and Waste Policy*, the OAG, in consultation with the City Clerk and Solicitor (the "City Solicitor") as required, has the primary responsibility for the receipt of all allegations of fraud or waste as defined in the *Fraud and Waste Policy* and for investigating or referring the investigation of such allegations, as appropriate.

In response to the receipt of the allegation, the OAG investigated this fraudulent payment matter. With the OAG's concurrence, the matter was also reported by the City to the Ottawa Police Service ("OPS").

Background and context

The City's Treasury Branch processes all foreign currency payments via wire transfer, as the accounts payable module of the City's financial system is currently unable to facilitate foreign currency Electronic Funds Transfers (EFT). Additionally, certain Canadian dollar value payments are also made via wire transfer.

On July 6, 2018, the General Manager, Corporate Services and City Treasurer, (the "City Treasurer"), received an email (the "Email") apparently from the City Manager. The Email requested that a wire transfer in the amount of US$97,797.20 (the "Funds") be processed for the completion of an acquisition, that the Email purports the City Manager had been negotiating privately for some time.

The City Treasurer conducted an internet search of the beneficiary and identified it as an Information Technology ("IT") webpage design company located in the United States. The City Treasurer assumed that the acquisition was in relation to locating a vendor that could assist with the required overhaul of the ottawa.ca website.

Later on July 6, the City's Treasury Branch, in accordance with The City Treasurer's approval, processed and issued the funds in US dollars, via international wire transfer, to a bank in the United States.

On July 11, 2018, the City Treasurer received further email correspondence, again apparently from the City Manager. The emails enquired if she was in her office as the balance of the payment (US$154,238) relating to the acquisition needed to be issued that morning. At the time of receiving this email, the City Treasurer was attending City Council meeting and commenced a discussion with the City Manager regarding the wire transfer request. The City Manager advised the City Treasurer that he had no knowledge with respect to the wire transfer requests; and upon being shown the Email, advised the City Treasurer that he did not send it and that the City had been defrauded of the funds.

The City did not process the alleged fraudster's July 11, 2018 wire transfer request. The City Treasurer immediately contacted the Manager, Technology Security, and the Manager, Treasury, to advise them of the fraudulent payment. The Manager, Treasury immediately notified the City's financial institution, Royal Bank of Canada ("RBC"), in an unsuccessful attempt to recover the Funds. The Manager, Technology Security immediately commenced action pursuant to the City's Computer Incident Response Plan and the *Fraud and Waste Policy*. The Office of the Auditor General and the Deputy City Solicitor were notified and a joint decision was taken to notify the Ottawa Police Service.

On July 12, 2018, the OAG advised the City Solicitor that it would be conducting an internal investigation into this matter.

Objectives

The overall objectives of the investigation were as follows:

1. Conduct a fact-finding investigation surrounding the receipt of request for payment and the resulting payment process with respect to the fraudulent payment;
2. Determine if fraudulent payments, similar to this fraudulent payment, may have been processed before; and
3. Review the controls in place related to these processes and recommend improvements where required.

Scope

The scope of the investigation was to ascertain whether the relevant City policies and procedures were complied with in relation to the processing of the fraudulent payment; whether a similar fraudulent payment scheme may have occurred previously; and the controls in place related to these processes. Where potential issues were identified, the scope was expanded to assess and make recommendations as required.

Approach

The approach in conducting the investigation included the following activities:

- Examination of documents, including the following:
  - *Payments to Vendors Policy*[4];
  - *Payments to Vendors Procedures*[5];
  - Payment Without Reference Form[6];
  - Delegation of Authority By-law, being By-law No. 369 of 2016[7];
  - *Delegation of Powers Policy*[8];
  - *Wire Vendor Payments – Procedures* (draft);
  - Wire Payments Process (draft);
  - Organization charts for Corporate Services, Corporate Finance Services, Accounting Branch and Treasury Branch[9]; and
  - Documentation provided by Technology Security Branch in relation to their incident response procedures conducted.
- Conducted a review of supporting documentation in relation to selected wire transfer transactions based on data provided by the Treasury Branch[10] and meeting certain criteria, for the period of January 6, 2015 to August 31, 2018.

[4] Revision Date: March 9, 2017

[5] Revision Date: March 9, 2017

[6] Form FIN001 V1.4 Revised 2010-07-20

[7] Enacted by City Council at its meeting of November 23, 2016

[8] Revised by City Council on February 13, 2013

[9] Dated 08/01/2018

[10] Obtained from the City's accounting system (SAP)

- Performed data analytic procedures with respect to wire transfer data provided by RBC, in relation to the City's bank account, for the period of October 3, 2016 to October 17, 2018. Based on the results of the data analytic procedures, conducted an analysis of supporting documentation in relation to selected wire transfers meeting certain criteria.
- Analyzed the general wire transfer payment process conducted by Treasury Branch.
- Interviews and enquiries with City personnel in Corporate Services Department, including Technology Security Branch, Corporate Finance Service and Treasury Branch.
- Enquiries with the current and former City Managers.
- Other investigation and analysis procedures as deemed necessary for purposes of concluding on the investigation objectives.

Detailed findings

The findings as a result of the investigation are provided under the following headings.

1. Chronology of events – Fraudulent payment

We set out below the chronology of events in relation to the email correspondence with respect to the fraudulent payment, which occurred on Friday, July 6, 2018.

Time (EDT)	Details
10:29 am	Email received by the City Treasurer which appeared to have been sent by the City Manager. The address reflected on the email was [City Manager]@ottawa.ca, which was later identified as a spoofed email address[11]. The alleged fraudster's actual sender email address was "info@e-officenq.com", which could be seen by placing the curser on the email address. The content of the email was as follows: *"Hi [City Treasurer], Are you available at your desk right now? [City Manager]"*

[11] Email spoofing is the forgery of an email address so that the message appears to have originated from someone other than the actual source. Correspondence is received by the alleged fraudster's actual email address.

Time (EDT)	Details
10:31 am	The City Treasurer responds to the alleged fraudster, which is sent to the alleged fraudster's actual email address: info@e-officenq.com: *"Yes, call me"*
10:51 am	The alleged fraudster emails the City Treasurer: *"Okay, I want you to take care of this for me personally, I have just been informed that we have had an offer accepted by a new international vendor, to complete an acquisition that i have been negotiating privately for some time now, in line with the terms agreed, we will need to make a down payment of 30% of their total, Which will be $97,797.20.* *An announcement is currently being drafted and will be announced next week, once the deal has been executed, for now I don't want to go into any more details.* *Until we are in a position to formally announce the acquisition I do not want you discussing it with anybody in the office, any question please email me.* *Can you confirm if international wire transfer can go out this morning?* *[City Manager]."*
11:03 am	Following the City Treasurer's enquiries with the Treasury Branch, she responds to the alleged fraudster: *"International wire transfers to Europe and Asia can no longer go as their banks are closed for the day, so Monday would be the earliest for those locations. We would have to send it before 10:00 am as given the time zones they would be closed for the day after that time here. Of course we can do a transfer to the US but it has to be sent before 11:30 am.* *Let me know."*
11:10 am	The City Treasurer responds to the alleged fraudster, with respect to additional information obtained from the Treasury Branch: *"Just received an update and we have until 4:30 if it going to the US. If it is going in a currency other than US dollars or Canadian dollars it takes 2 business days."*
12:11 pm	The alleged fraudster emails the City Treasurer:

Time (EDT)	Details
	"Okay, see below the wire banking details of the vendor. *BANK NAME:* [redacted] *BANK ADDRESS:* [redacted] *ACCOUNT NAME:* [redacted] *BENEFICIARY ADDRESS..* [redacted] *ACCTOUNT NUMBER:* [redacted] *SWIFT CODE:* [redacted] *ROUTING NUMBER:* [redacted] *CURRENCY: $97,797.20 USD* *Let me know when this is completed and also send the confirmation slip.* *[City Manager]."*
12:16 pm	The City Treasurer responds to the alleged fraudster: *"Will do."*
12:35 pm	Treasury Branch creates wire transfer in the amount of US$97,797.20 (CDN$128,603.32)
12:43 pm	Wire transfer released by Treasury Branch.
12:49 pm	Treasury Branch emails the City Treasurer to advise that the transaction was completed.
12:50 pm	The City Treasurer emails the City Manager directly, not using the spoofed email address, confirming that the transaction was completed. (During our enquiry with the City Manager, he confirmed receipt of this email and that he made a note to follow-up with the City Treasurer at a later date to discuss. This discussion did not occur until July 11, 2018, following the alleged fraudster's subsequent request for additional funds).
1:55 pm	The alleged fraudster emails the City Treasurer: *"Please confirm if the wire have been process.*

Time (EDT)	Details
	Thanks. *[City Manager]"*
1:58 pm	The City Treasurer responds to the alleged fraudster: *"I sent the confirmation at 12:50. Did you not receive it?"*
2:05 pm	The alleged fraudster emails the City Treasurer: *"No I didn't receive it, please a copy of the confirmation.* *Thanks,* *[City Manager]"*
2:21 pm	The alleged fraudster emails the City Treasurer: *"[City Treasurer],* *This wire is still on pending at the bank, please let me know once this payment have been completed by the bank.* *Thanks.* *[City Manager]"*
2:29 pm	The City Treasurer encloses in her email to the alleged fraudster a copy of the Wire Activity – Detailed Report and responds: *"It is now completed."*
2:34 pm	The alleged fraudster emails the City Treasurer: *"Thanks* *[City Manager]"*

2. Identification of fraud scheme – the "fake CEO scam"

In the past two years, cybercrime has become the most reported economic crime experienced by organizations in Canada[12].

Cyber criminals have been attacking organizations globally with a common fraud scheme called the "fake CEO scam"[13]. In these attacks, which is what the City fell victim to in relation to the fraudulent payment, the following occurs:

- Fraudsters gain access to a high-ranking executive's email account, or create a similar email address, and target employees in financial positions within the organization who have the authority to move money;
- The fraudsters send realistic-looking emails, requesting urgent wire transfers for what appears to be legitimate business reasons, like "securing an important contract", "a confidential transaction" or "updating a supplier's payment information";
- Fraudsters often send the targeted fraudulent email when executives are travelling abroad or otherwise difficult to reach; and
- Believing that the request is real, the employee transfers the money, only to find out upon the boss' return that the email was a scam and the money is gone.

Losses to this type of scam typically range from tens of thousands to millions of dollars. The fake CEO scam is a growing global threat to businesses and organizations of all sizes.

3. No identification of email source (internal versus external)

At the time of the fraudulent payment incident, emails received by City employees did not reflect the source in terms of being an internal or external sender. Providing such identification can heighten the recipient's awareness of spam or other suspicious emails, which may used for phishing[14] or contain dangerous malware.

---

[12] https://www.pwc.com/ca/en/media/release/economic-crime-hits-record-levels-in-canada-in-the-past-5-years.html

[13] https://www.canada.ca/en/competition-bureau/news/2017/06/show_them_who_s_thebossshutdownthefakeceoscam.html

[14] Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

In our interviews, Technology Security staff stated that in response to the fraudulent payment incident, they are requesting of the groups responsible for the exchange server in network operations and the cloud that a mechanism be implemented to identify emails coming from an external source.

Recommendation #1

That the City implement a process to identify external emails received by staff and display this to the recipient in an obvious manner.

Management response:

Management agrees with the recommendation.

ITS / Technology Security is currently piloting potential solutions with implementation expected in Q3 2019.

4. Commended Technology Security response

As noted previously, on July 11, 2018, the Technology Security Branch was notified of the fraudulent payment incident and immediately implemented their response in accordance with their Computer Incident Response Plan (the "Plan").

The goal of the Plan as outlined therein, is to:

- Identify/Understand:
  - The threat;
  - Scale of the incident; and
  - Impact of the incident on the City.
- Contain the incident:
  - Identify controls/actions required to stop the event from causing more harm.
- Remediate the incident:
  - Remove the threat from the systems/network returning the environment back to a 'trusted' state.
- Recover from the incident:
  - Return the affected systems/data back in a priority order to the point where normal business operations can resume.

- Learn from the incident:
    - Complete an After Action Report detailing the findings of the incident as well as any gaps identified which can be mitigated and reduce the likelihood of future occurrence.

The procedures taken by the Technology Security Branch, included the following:

- Scheduled and conducted a conference call with the City's Legal Services to discuss the incident;
- Appointed a senior resource as the incident commander;
- Confirmed that the City Manager's email was not hacked and that a spoofed email address was used to perpetrate the fraud;
- To prevent further spoofing emails reaching employees, they implemented a process whereby all emails, containing the @e-officenq.com component of the alleged fraudster's email address, would be directed to a secured folder that only select Technology Security employees could access;
- Conducted searches and confirmed that there was no other unknown email communication with other City employees involving the alleged fraudster's email address, info@e-officenq.com, since March 1, 2018[15];
- Preserved all email correspondence between the alleged fraudster and the City Treasurer;
- Conducted an interview with the City Treasurer to obtain details surrounding the fraudulent payment;
- After contacting and receiving direction from the Deputy City Solicitor and the Office of the Auditor General, contacted and met with the OPS to file a report[16] with respect to the fraudulent payment incident and the alleged fraudster's subsequent fraud attempt;
- Confirmed with the Treasury Branch that the financial institution (RBC) has placed a special watch on all transactions moving forward, as the alleged fraudster may have some of the banking details;
- Documented all actions taken; and
- Provided fraud training to the Treasury Branch employees.

[15] Emails available on the City's server

[16] Case number (18-169146)

Technology Security fully cooperated with the OAG as part of this investigation and provided all documentation obtained from their incident response to the OAG. Recognizing that Technology Security took the initial lead prior to the OAG assuming responsibility for the investigation, they are commended for their prompt actions, demonstrating their readiness to address unfortunate computer incidents.

5. Non-compliance with the City's *Payment to Vendors Policy* and *Payments to Vendors Procedure*

As part of the investigation, we assessed whether the processing of the fraudulent payment was in compliance with the City's *Payment to Vendors Policies*[17] (the "Policy") and *Payments to Vendors Procedures* (the "Procedures"). We found that proper procedures were not followed.

The Policy states:

- Policy Statement

  "All payments to vendors shall be made using the most efficient method available ensuring proper authority has been obtained and all conditions for payment have been met."

- Payment Conditions and Invoicing Processing

  "…Invoices are processed either through MarkView (the City's automated invoice processing system), or outside of MarkView as required. The preferred method is MarkView…"
  "Payments may be processed outside of the MarkView in the following circumstances:
  - *Where adherence to this Policy does not apply or is not adopted (i.e. local boards and elected officials);*
  - *Where confidentiality is a concern;*
  - *When an invoice does not exist (Payment Without Reference Form should be used);*
  - *When the payment voucher is processed via direct post (Refer to Payment to Vendors Procedures)."*

[17] Revision Date: March 9, 2017

The Procedures states:

- Application

  "These Procedures apply to all City staff who are involved in paying a vendor for a good, a service and/or construction. These Procedures do not apply to the City's local boards or elected officials".

- Non-Purchase Order Invoice Processing

The table below describes the Non-PO invoice to payment process:

Invoice Source	**Process**
Non-MarkView	• Business user codes for the invoice. • Business user ensures appropriate delegated authority approved the invoice. • Business user attaches the Payment Without Reference (PWR) Form (Appendix A), with supporting payment documents, where appropriate. • Business user sends the invoice, PWR and/or any copies of supporting documents to the FSU[18] for review. • FSU reviews and if appropriate, stamps and signs the invoice/PWR Form to demonstrate review. • FSU enters payment information in SAP. • FSU writes the document number on the invoice, scans and emails the invoice to AP-Attachments@ottawa.ca.

Based on the findings from the investigation, we note the following:

- The processing of the fraudulent payment occurred outside of the MarkView system.
- The FSU (Financial Services Unit) was not involved in this transaction.
- There was no Payment Without Reference Form prepared.
- The delegated authority approval was based on the content of emails allegedly from the City Manager.
- There was no supporting documentation provided to the Treasury Branch to process the payment. The only information provided to Treasury Branch was the

[18] Financial Services Unit

content of the alleged fraudster's email sent on July 6, 2018 at 12:11 pm, which outlined the alleged fraudster's banking information.
- There were no codes (GL account, budget, cost or profit centre) provided to Treasury Branch for processing the transaction.
- The Treasury Branch has no formal approved wire transfer policies and procedures. Subsequent to the fraudulent payment incident, draft versions were prepared and are in the process of being finalized.

During our interview with the City Treasurer, she stated the following:

- She confirmed that the Policy and Procedures are to be governed by all City staff for the payment of goods and services.
- The Policy and Procedures were not complied with in relation to processing the fraudulent payment as the City Manager has the ability to override a policy in an urgent situation. She was complying with City Manager's request pursuant to the content of the emails, which she believed were legitimate.

We enquired with the former and current City Managers both of whom stated that they have never directly requested that either a payment be processed by Accounts Payable or a wire transfer by Treasury Branch. The current City Manager stated that he believes that there is some authority to request urgent payments; however, there are a number of criteria to be met, including subsequent immediate reporting of such payments to Council.

Based on our review of the Delegation of Authority By-law (the "By-law"), we note the following sections in relation to "*Emergency or Special Circumstances*":

> *"5 – In cases of emergency or special circumstances where it is necessary to act within the normal mandate of a department, but such action is not strictly within the terms of a delegated authority, a General Manager, in respect of his or her specific Department, may take such action as necessary to rectify the situation.*
>
> *6 – All action taken pursuant to Section 5 shall be reported immediately to the appropriate Standing Committee.*
>
> *7 – In cases of emergency or special circumstances where it is necessary to take an action outside of the normal mandate of a department, the City Manager may take such action as necessary to rectify the situation.*
>
> *8 – All action taken pursuant to Section 7 shall be reported immediately to the appropriate Standing Committee and subsequently to Council."*

The Policy clearly states that all conditions must be met, and the Procedures are applicable to all City staff. The City Treasurer did not comply with the Policy and Procedures. Had Policy and Procedures been followed, the request would have gone through either Accounts Payable or a Financial Services Unit. In our opinion, it is far less likely that the payment would have been made had either of these groups processed the request.

Recommendation #2

That the City finalize and approve policy and procedures which require that all wire transfer payments be processed, reviewed and approved by either Accounts Payable or a Financial Services Unit.

Management response:

Management agrees with the recommendation.

Treasury is working with Accounts Payable (AP) to update the Payment to Vendors Policy and Procedures, to incorporate specific policies and procedures for wire transfer payments. This will be completed by Q2 2019. In the interim, Treasury met with AP and the FSU to confirm that going forward they will review and approve all requests for wire transfer payments, prior to processing.

Recommendation #3

That the City issue a communication to all management clarifying that they do not have the authorization to override controls and will be held accountable for non-compliance.

Management response:

Management agrees with the recommendation.

Corporate Finance will work with Procurement to develop a communication to all management that reinforces the financial and procurement policies, procedures and controls in place for authorizing payments to vendors. The communication will be developed and issued by the City Manager’s Office to all managers by Q1 2019.

6. Inadequate controls with respect to wire transfer process

We found dangerous control weaknesses with respect to wire transfer process. In order to assess whether prior fraudulent wire transfer payments similar to the fraudulent payment scheme may have occurred, the following specific forensic investigative procedures were conducted:

- Analyzed the general wire transfer payment process conducted by Treasury Branch.
- Conducted an analysis of supporting documentation in relation to selected wire transfer transactions, based on data provided by the Treasury Branch[19], for the period of January 6, 2015 to August 31, 2018. Nineteen transactions were selected for analysis based on the following criteria:
    - Missing vendor names;
    - Questionable vendor names; and
    - Possible duplicate payments.
- Performed data analytic procedures with respect to wire transfer data provided by RBC, in relation to the City's bank account used for processing wire transfers, for the period of October 3, 2016 to October 17, 2018. Eight transactions were selected for analysis based on the results of the following data analytic procedures conducted:
    - An analysis of the names of the creator and approver/releaser was conducted to identity whether the same person acted in both capacities. There were none identified.
    - Wire transfers were initially filtered based on the volume of transactions made to each beneficiary during a fiscal year.
    - Beneficiaries that were known to have legitimate business relationships with the City i.e. school boards, National Capital Commission, law firms, were filtered out of the population.
    - For the remaining population of wire transfers, beneficiaries were identified having a low volume of transactions (four or less), especially those made in currencies other than CAD$. The resulting wire transfers (eight) were selected for review.

[19] Obtained from the City's accounting system (SAP)

We set out below our findings in relation to the above-noted specific forensic investigation procedures conducted:

- There was no evidence of any fraudulent payments issued, similar to the fraudulent payment scheme.
- All of the transactions we analysed had adequate supporting documentation. The supporting documentation contained signatures of the approver; however, their identities could not always be determined as their names were not printed.
- There was a segregation of duties with respect to the person creating the wire transfer request and the Treasury staff approving and releasing the wire transfer in the RBC banking system (the “RBC System”).
- Wire transfer documentation is filed on a per transaction basis. Wire transfer summary reports are not prepared nor reviewed by senior management.
- The wire transfer RBC System is not directly integrated to the City’s SAP system. Wire transfer payments can be processed without a general ledger account to allocate the payment to or even an entry in the financial system.
- There are no formal written City authorization limits (approval rules) with respect to wire transfer payments.
- To setup a wire payment, an authorized individual first creates it within the RBC System. The individual who created the payment then provides the supporting documentation to an approver and request they approve it within the RBC System. If the transaction is less than $25 million, the payment is released upon approval. If the transaction is greater than $25 million, the payment is held awaiting a second approver. The creator then takes the supporting documentation to a second approver and request they approve it within the RBC System. Upon the second approval, the transaction is automatically released.
- Authorization limits are set within the RBC System and can be changed at any time by a Treasury Branch employee with administrative access rights. The authorization limits in place at the time of our investigation were as follows:
- Authorized to create new payment recipients in the RBC System

    1. Senior Investment Officers (two)
    2. Treasury Business Analyst
    3. Treasury Analyst
    4. Treasury Manager
    5. Deputy City Treasurer
    6. City Treasurer

- Authorized to approve new payment recipients (requires two of the below)
    1. Senior Investment Officers (two)
    2. Treasury Manager
    3. Deputy City Treasurer
    4. City Treasurer (also authorized to approve their own new vendors they created)
- Authorized to create wire transfers:
    1. Senior Investment Officers (two)
    2. Treasury Business Analyst
    3. Treasury Analyst
    4. Treasury Manager
    5. Deputy City Treasurer
    6. City Treasurer
- Authorized to approve wire transfers:
    1. Senior Investment Officers (two)
    2. Treasury Manager
    3. Deputy City Treasurer
    4. City Treasurer
- Wire transfers less than $25 million – can be approved and released by any one of the individuals noted above authorized to approve.
- Wire transfers greater than $25 million – require the approval of any two of the individuals noted above authorized to approve.
- Administrative access rights:
    - Senior Investment Officer (one only)
    - Treasury Manager
    - Deputy City Treasurer
    - Treasurer
- We were informed by Treasury Branch staff that the segregation of duties controls in the RBC System prevented the same user from both creating and approving a wire transfer. Notwithstanding this, we requested that Treasury Branch perform a test to confirm that this could not occur within the RBC System. It turns out that it could occur. The result was that there was no such control in the RBC System. Any one of five authorized individuals could on their own both create and release a wire transfer up to $25 million. This represents a dangerous control weakness.

In response to this finding, Treasury Branch management has indicated that they had the necessary changes made to mitigate this risk.

Recommendation #4

That the City ensure that physical approvals are adequately documented for future reference i.e. confirmation that physical signatures are legitimate (compared to a signature specimen sheet) and names printed.

Management response:

Management agrees with the recommendation.

Treasury staff responsible for wire transfer processing now have access to the SAP Signature Authority platform so that they can verify and match all specimen signatures approving a payment by wire transfer.

Treasury is working with Accounts Payable to update the Payment to Vendors Policy and Procedures, to incorporate specific policies and procedures for wire transfer payments to ensure that physical signatures are legitimate and adequately documented and, that there is an audit process to ensure compliance. This will be completed by Q2 2019.

Recommendation #5

That the City prepare monthly summary reports with respect to the wire transfers created and released. These reports should be reviewed and signed off by a senior finance officer and kept on file for future reference. Any identified anomalies should be reported immediately to the Office of the Auditor General.

Management response:

Management agrees with the recommendation.

Monthly activity reports are currently available from existing systems, including Wire Payments, Account Transfers and Administrative activity reports. The new roles and responsibilities for this process will be implemented in Q1 2019. Documentation of this process will be incorporated into the new wire transfer payments section of the updated Payment to Vendors Procedures to be completed by Q2 2019.

Recommendation #6

That the City review its current practices and establish formal authorization limits/approval rules with respect to the issuance of wire transfer payments. Delegate an appropriate owner for these rules who will be accountable to ensure that they are properly established and maintained in the financial institution's system.

Management response:

Management agrees with the recommendation.

Formal authorization limits/approval rules with respect to the issuance of wire transfer payments and roles and responsibilities for maintaining these rules will be included in the new wire transfer payments section of the updated Payment to Vendors Procedures to be completed by Q2 2019.

Recommendation #7

That the City coordinate with their financial institution to deactivate the ability for Treasury Branch employees, who have been assigned administrative rights, to change access/authorization rights. All changes to access/authorization rights should be made by the financial institution only upon receiving written instructions from an authorized senior City official.

Management response:

Management agrees with the recommendation.

Treasury staff have discussed this recommendation with the financial institution and they have indicated that this is not a responsibility they are prepared to assume. They insist that it is up to the client to identify appropriate internal administrators to manage authorities.

Corporate Finance will review the segregation of duties and administrative rights of Treasury Branch, determine best practices and implement the controls, segregation of duties and clear roles and responsibilities required for assigning administrative rights by Q2 2019.

Recommendation #8

That the City make changes to its authorization profiles in the financial institution's system so that no one City employee can both create and approve the same wire transfer transaction and verify that these changes are effective.

Management response:

Management agrees with the recommendation.

The ability of any one employee to both create and approve a wire transfer in the financial institution's system has been removed except for those with administrative rights, based on how the banking system works. Implementing Recommendation 7 will ensure that there is appropriate segregation of duties and controls in place to ensure those with administrative rights cannot create or approve a wire transfer. These changes in roles, responsibilities and procedures will be implemented and included in the new wire transfer payments section of the updated Payment to Vendors Procedures to be completed by Q2 2019.

7. Prior fraudulent wire transfer attempt

During the course of the investigation, we discovered that the City was the target of a prior attempted fraud scheme, similar to this fraudulent payment incident. The details are as follows:

- In the spring of 2018, a spoofed email, purporting to be sent by the CEO of the Ottawa Public Library, was sent to the City Treasurer requesting a wire transfer of funds;
- The City Treasurer forwarded the email to the Deputy Treasurer requesting that she address it;
- The Deputy Treasurer forwarded the email to the Treasury Branch;
- Treasury Branch staff reviewed the email and requested more information from the Deputy Treasurer with respect to the wire transfer request as the email did not contain the required banking information;
- The Deputy Treasurer emailed the Ottawa Public Library CEO to obtain the additional banking details and was advised by the CEO that she had not sent the original email;
- The wire transfer was not completed; and
- The matter was not reported to Technology Security or to the OAG.

Recommendation #9

That the City report all attempts to defraud the City where City staff have corresponded with and/or begun taking the requested action, to the Office of the Auditor General.

Management response:

Management agrees with the recommendation.

ITS / Technology Security is currently developing a corporate-wide mandatory cyber awareness training program. A Request for Proposal was issued and awarded for the development of a cyber awareness training program, which will include the requirement to report fraud. Implementation is expected by Q2 2019.

8. OPS response

On July 11, 2018, Technology Security met with an OPS Constable to complete a police report[20] with respect to the fraudulent payment incident and the alleged fraudster's subsequent email correspondence requesting a further US$154,238. At the time of the report, the alleged fraudster was continuing to correspond with the City Treasurer, and Technology Security suggested that OPS take a proactive role in continuing with the communication in an attempt to identify the perpetrator. The OPS Constable assigned advised that he did not have any cyber-security experience. The OPS Constable contacted his colleagues to advise them that there was a live situation. Technology Security advised us that the response provided to the Constable from his colleagues was that the wire transfer was completed, and they could not provide any assistance. As a result, the City ceased all communication with the alleged fraudster.

Technology Security staff indicate that there has been no follow-up by the OPS with respect to this matter.

9. Recovery proceedings

The recipient of the fraudulent payment was a suspect bank account at a bank located in the United States (the "First American Account"). Most of these funds were transferred from the First American Account to another bank account in the same recipient name, held at another bank also located in the United States (the "Second American Account". Unbeknownst to the City, the Second American Account was being monitored by the United States Secret Service ("USSS") as it was related to fraudulent transfers connected to other American bank accounts.

On or about August 3, 2018, the City was contacted by the USSS, as the funds in the Second American Account had been seized. The USSS advised that funds in the Second American Account can be traced to the fraudulent payment; however, not all of

[20] Case number (18-169146)

the funds from the City are on deposit. The USSS estimated that approximately US$88,000 was recovered from the Second American Account, but noted that these funds were comingled with funds received fraudulently from another victim of a similar incident to that of the City.

The City Solicitor has taken carriage of this matter and filed the required Petition for Remission or Mitigation of Forfeiture (the "Petition") with the USSS, asserting the City's claim on the funds on deposit in the Second American Account. On November 5, 2018, the USSS Ottawa advised the City Solicitor that a ruling on the Petition will be made by the appropriate US authorities after the investigation and review has been completed.

The City is very fortunate in this regard as recovery of any funds by victims of these fraud schemes is extremely rare.

10. Lack of fraud awareness training

Fraud awareness assists with the prevention, detection and reporting of fraud. All interviewees stated that fraud awareness training would be beneficial and may have prevented the fraudulent payment from happening. Technology Security staff had been proactive in providing discretionary awareness sessions on this topic before this incident occurred; however, they indicate a need for a mandatory awareness program.

In January 2018, Technology Security conducted a phishing test[21] wherein 200 random City users were selected. The results of the test were that 53 of the users clicked on the link in the email, a 26.5 per cent failure rate. Technology Security staff stated that the industry average is 15 per cent and that they believe the results support the need for mandatory cybercrime/fraud awareness training. Technology Security staff further advised that the City of Toronto is in the process of rolling out a mandatory fraud awareness training program to its employees.

Recommendation #10

> That the City create and implement a fraud awareness training program which would encompass the Code of Conduct, the risk of fraud, the employees' role in preventing and reporting fraud.

[21] A phishing test is where deceptive emails, similar to malicious emails, are sent by an organization to their own staff to gauge their response to phishing and similar email attacks.

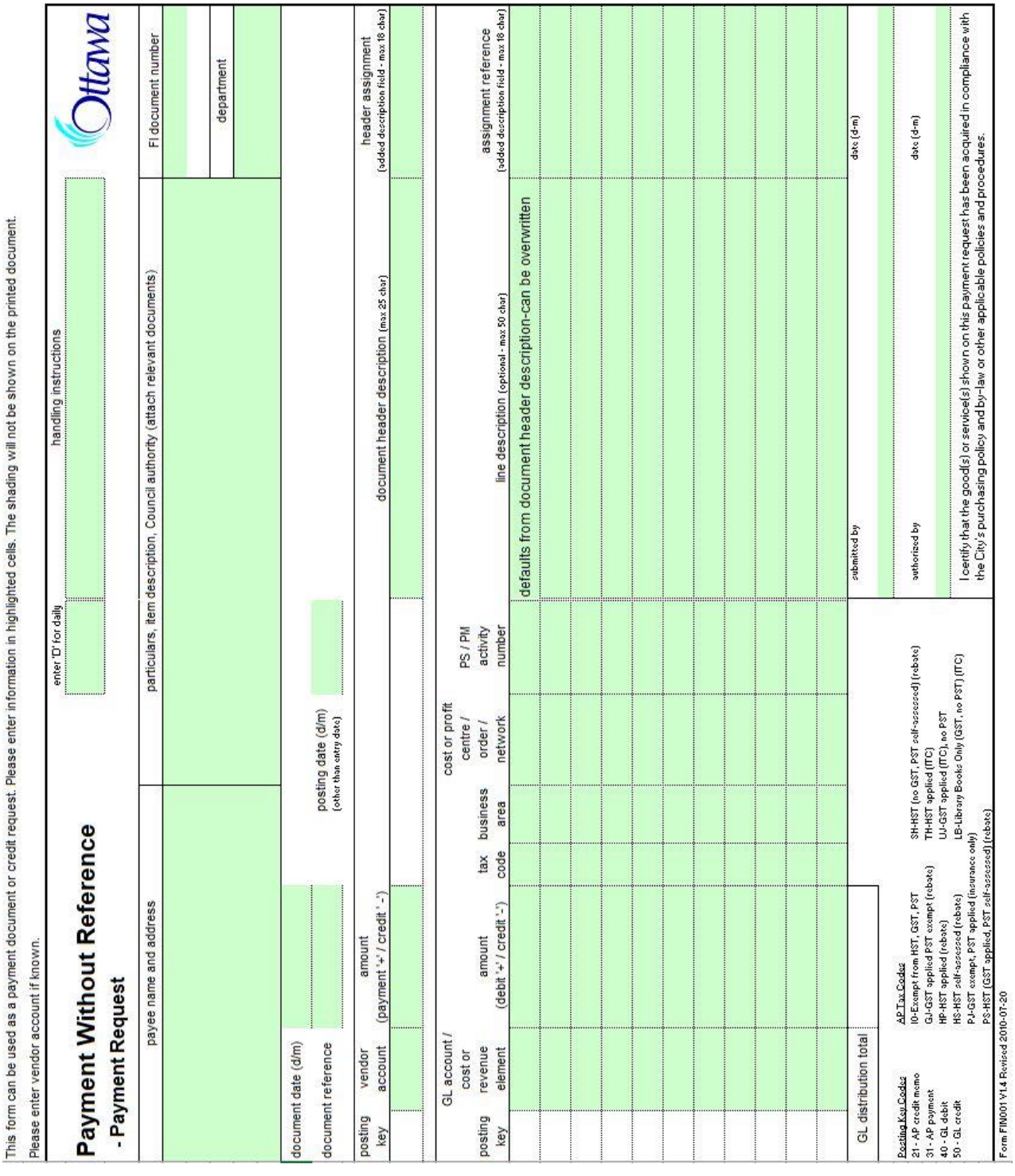
Management response:

Management agrees with the recommendation.

As indicated in the response to Recommendation 9, ITS / Technology Security is currently developing a corporate-wide, mandatory cyber awareness training program for implementation by Q2 2019. This program will encompass the Code of Conduct, the risk of fraud and the employee's role in preventing and reporting fraud.

In the interim, ITS has developed messaging for staff to better recognise and delete phishing and other security risks they may encounter. An email was sent to all networked staff on October 4, 2018 informing them of these risks. Furthermore, articles were sent corporate-wide via the City's e-newsletter *In the Loop* on July 24, 2018 and information is posted on the City's intranet Ozone, which staff are required to view before proceeding to the landing page. As part of the cyber security awareness program, ITS will deliver quarterly messages to staff that are relevant to risks the City is encountering.

Appendix A – Payment Without Reference Form



This form can be used as a payment document or credit request. Please enter information in highlighted cells. The shading will not be shown on the printed document.

Please enter vendor account if known.

Payment Without Reference

- Payment Request

enter 'D' for daily

handling instructions

payee name and address	particulars, item description, Council authority (attach relevant documents)	FI document number
		department

document date (d/m)

document reference

posting date (d/m) (other than entry date)

posting key	vendor account	amount (payment '+' / credit '-')	document header description (max 25 char)	header assignment (added description field - max 18 char)

posting key	GL account / cost or revenue element	amount (debit '+' / credit '-')	tax code	business area	cost or profit centre / order / network	PS / PM activity number	line description (optional - max 50 char)	assignment reference (added description field - max 18 char)
							defaults from document header description-can be overwritten	
	GL distribution total						submitted by	date (d-m)

Posting Key Codes	AP Tax Codes		
21 - AP credit memo	I0-Exempt from HST, GST, PST	SH-HST (no GST, PST self-assessed) (rebate)	authorized by	date (d-m)
31 - AP payment	GJ-GST applied PST exempt (rebate)	TH-HST applied (ITC)		
40 - GL debit	HP-HST applied (rebate)	UJ-GST applied (ITC), no PST		
50 - GL credit	HS-HST self-assessed (rebate)	LB-Library Books Only (GST, no PST) (ITC)	I certify that the good(s) or service(s) shown on this payment request has been acquired in compliance with the City's purchasing policy and by-law or other applicable policies and procedures.	
	PJ-GST exempt, PST applied (insurance only)			
	PS-HST (GST applied, PST self-assessed) (rebate)			

Form FIN001 V1.4 Revised 2010-07-20