Bureau du vérificateur général

Enquête sur le virement de fonds à un faux fournisseur

Déposée devant le Comité de la vérification
Le 8 avril 2019

Table des matières

Remerciements

L’équipe responsable de cette enquête, constituée de PricewaterhouseCoopers s.e.n.c.r.l. et placée sous la supervision d’Ed Miner, vérificateur général adjoint et sous les ordres de Ken Hughes, vérificateur général, tient à remercier les personnes qui ont participé à ce projet, et en particulier ceux et celles qui ont exprimé des avis et fait des commentaires dans le cadre de cette enquête.

Original signé par :

Le vérificateur général

Résumé

Objet

Cette enquête a été menée pour donner suite au rapport déposé auprès du Bureau du vérificateur général (le « BVG ») relativement au virement de 97 797,20 $ US effectué par la Ville dans le compte d'un faux fournisseur qui avait fait appel à des moyens frauduleux (le « paiement frauduleux »).

Dans l'ensemble, les objectifs de cette enquête ont consisté à :

1. mener une enquête factuelle sur la réception de la demande de paiement et sur le processus qui a donné lieu au paiement frauduleux;
2. déterminer si des paiements frauduleux comparables à celui qui fait l'objet de cette enquête ont pu être traités auparavant;
3. examiner les contrôles en vigueur en ce qui a trait à ces processus et recommander les améliorations à y apporter dans les cas nécessaires.

Avec l'accord du BVG, la Ville a aussi porté la question à la connaissance du Service de police d'Ottawa (le « SPO »).

Renseignements généraux et justification

La Direction de la trésorerie traite les virements électroniques destinés à tous les fournisseurs qui ont des comptes de banque à l'étranger, puisque le module des comptes fournisseurs du système financier de la Ville ne permet pas, à l'heure actuelle, de traiter les virements électroniques de fonds (VEF) en dollars américains.

Le 6 juillet 2018, la trésorière municipale et directrice générale des Services organisationnels (la « trésorière municipale »), a reçu un courriel (le « courriel ») apparemment envoyé par le directeur municipal. Dans ce courriel, qui s'est par la suite révélé être un courriel frauduleux[1], on demandait de traiter un virement électronique pour la somme de 97 797,20 $ US (les « fonds ») afin de permettre de mener à bien une acquisition.

[1] L'usurpation d'une adresse de courriel consiste à contrefaire cette adresse de courriel pour que le destinataire croie que le message provient d'un expéditeur digne de confiance, alors qu'il est envoyé par quelqu'un d'autre. La correspondance est acheminée à l'adresse de courriel réelle du présumé fraudeur.

Plus tard dans la journée, la demande a été traitée avec l'approbation de la trésorière municipale, et les fonds ont été virés.

Le 11 juillet 2018, la trésorière municipale a reçu, apparemment toujours de la part du directeur municipal, un autre courriel dans lequel on demandait de virer dans l'avant-midi le solde du paiement (154 238 $ US) se rapportant à cette acquisition.

La trésorière municipale a décidé d'en discuter avec le directeur municipal, qui lui a fait savoir qu'il n'était pas du tout au courant de ces demandes de virement électronique.

La Ville n'a pas traité la demande de virement électronique que lui a adressée le présumé fraudeur le 11 juillet 2018, et la trésorière municipale a aussitôt signalé l'incident de virement frauduleux aux Services de sécurité de la TI de la Ville.

Constatations

Voici les constatations des vérificateurs dans la foulée de l'enquête qu'ils ont menée, ainsi que les recommandations proposées.

1. Dépistage de la manœuvre frauduleuse : la « fraude du faux PDG »

Les cybercriminels mènent, partout dans le monde, des cyberattentats contre les organismes et les entreprises dans le cadre d'une manœuvre frauduleuse courante appelée la « fraude du faux PDG ». Dans ces cyberattentats, dont la Ville a été victime en raison de ce virement frauduleux, les fraudeurs envoient des courriels d'aspect réaliste, en demandant des virements de fonds urgents pour des motifs professionnels soi-disant légitimes, par exemple pour « obtenir un contrat important », « réaliser une transaction confidentielle » ou la « mettre à jour l'information sur les paiements d'un fournisseur ».

Convaincu qu'il s'agit d'une vraie demande, l'employé victime de cette manœuvre transfère les fonds, pour ensuite constater qu'il s'agit d'une fraude et que les fonds se sont volatilisés.

Les pertes attribuables à ce type de manœuvre frauduleuse sont généralement comprises entre des dizaines de milliers et des millions de dollars. La fraude du faux PDG constitue une menace mondiale grandissante pour les entreprises et les organismes de plus ou moins grande envergure.

2. Impossibilité de connaître l'identité de l'auteur véritable du courriel (origine interne ou externe)

À la date à laquelle s'est produit l'incident de virement frauduleux, les courriels transmis aux employés de la Ville ne permettaient pas de savoir s'ils provenaient d'un expéditeur interne (de la Ville) ou externe. Cette précision permet de mieux attirer l'attention du destinataire sur les pourriels ou les autres courriels suspects, qui pourraient servir à l'hameçonnage[2] ou comprendre des maliciels dangereux.

Le personnel des Services de sécurité de la TI a demandé aux groupes responsables du serveur d'échange de courriels dans l'exploitation des réseaux et en nuagique de mettre en œuvre un mécanisme pour permettre de dépister visuellement tous les courriels d'origine externe.

3. Intervention louable des Services de sécurité de la TI

Dès que la trésorière municipale a signalé l'incident de virement frauduleux et avant que le BVG lance son enquête, les Services de sécurité de la TI sont intervenus conformément à leur Plan d'intervention en cas d'incident informatique.

Les procédures appliquées par les Services de sécurité de la TI ont consisté à prévenir la Direction des services juridiques et le BVG, à confirmer que l'on s'était servi d'une adresse de courriel frauduleuse, à procéder à des recherches de courriels, à protéger la correspondance éventuelle par courriel contre le présumé fraudeur, à préserver des courriels et à déposer un rapport auprès du SPO.

Les Services de sécurité de la TI ont apporté leur entière collaboration au BVG dans le cadre de cette enquête et ont fourni au BVG tous les documents réunis à la suite de leur intervention. En sachant que les Services de sécurité de la TI ont pris en charge le dossier avant que le BVG prenne la responsabilité de l'enquête, il faut les féliciter de leur intervention rapide, puisqu'ils ont démontré qu'ils étaient prêts à intervenir dans ces incidents informatiques regrettables.

[2] Il s'agit d'une tentative de fraude destinée à obtenir des renseignements confidentiels comme des noms d'utilisateur, des mots de passe et des détails sur des cartes de crédit, en faisant croire que le message électronique provient d'une entité digne de confiance.

4. Non-conformité à la *Politique sur le paiement des fournisseurs* et aux *Procédures relatives au paiement des fournisseurs de la Ville*

La *Politique sur le paiement des fournisseurs* (la « politique ») et les *Procédures relatives au paiement des fournisseurs* (les « procédures ») de la Ville font état de la marche à suivre par rapport au traitement des paiements. Nous avons constaté que la politique et les procédures n'ont pas été parfaitement respectées.

La trésorière municipale a reconnu que la politique et les procédures n'ont pas été respectées dans le traitement du virement frauduleux, puisque le directeur municipal a le pouvoir de déroger aux politiques dans les cas urgents. La trésorière municipale s'est conformée, selon elle, à la demande du directeur municipal en donnant suite à des courriels qu'elle croyait légitimes.

Le *Règlement municipal sur la délégation de pouvoirs* (le « Règlement ») comprend effectivement des articles se rapportant aux « *urgences ou circonstances particulières* ».

Nous avons consulté l'ancien directeur municipal et le titulaire actuel de cette fonction, qui ont tous deux affirmé qu'ils n'avaient jamais directement demandé qu'un paiement soit traité par les Comptes créditeurs ou qu'un virement électronique soit traité par la Direction de la trésorerie. L'actuel directeur municipal a déclaré qu'à son avis, certains pouvoirs permettent de demander des paiements urgents; il y a toutefois un certain nombre de critères à respecter; il faut notamment déclarer immédiatement ces paiements au Conseil municipal.

5. Contrôles insuffisants relativement au processus de virement électronique

Nous avons relevé de dangereuses lacunes de contrôle dans les processus de virement électronique. Nous avons appliqué certaines procédures de juricomptabilité afin de savoir s'il avait pu y avoir auparavant des virements électroniques frauduleux comparables à la manœuvre frauduleuse faisant l'objet de cette enquête.

Le lecteur trouvera ci-après nos constatations en ce qui a trait aux procédures d'enquête juricomptable précises que nous avons appliquées :

- rien ne prouve qu'on a traité d'autres paiements frauduleux, comparables à celui de cette manœuvre frauduleuse;
- toutes les transactions que nous avons analysées faisaient l'objet de pièces justificatives suffisantes. Toutefois, même si ces pièces justificatives comportaient les signatures de l'approbateur, l'identité ne pouvait pas toujours être établie,

puisque les noms des signataires n'étaient pas reproduits en caractères d'imprimerie;

- les procédures de la Ville prévoyaient une répartition efficace des tâches entre l'employé qui établit la demande de virement électronique et le personnel de la Direction de la trésorerie qui approuve et autorise le virement électronique dans le système bancaire de la RBC (le « système de la RBC »);
- les pièces justificatives des virements électroniques sont versées au dossier pour chaque transaction. Puisqu'on ne prépare pas de rapport de synthèse des virements électroniques, la haute direction ne peut pas revoir ces rapports;
- le système de la RBC pour les virements électroniques n'est pas directement intégré dans le système SAP de la Ville. Il est possible de traiter les virements électroniques sans comptabiliser, dans un compte du grand-livre général, le paiement ni même passer d'écritures dans le système financier;
- il n'y a pas de limite d'autorisation écrite formelle (règles d'approbation) à la Ville en ce qui a trait aux virements électroniques;
- pour paramétrer un virement électronique, l'employé autorisé doit d'abord le créer dans le système de la RBC. L'employé qui a créé le paiement transmet ensuite les pièces justificatives à l'approbateur et lui demande d'approuver la demande dans le système de la RBC. Si la transaction est inférieure à 25 millions de dollars, le paiement est alors autorisé dès l'approbation. Si la transaction est supérieure à 25 millions de dollars, il faut attendre l'approbation d'un deuxième fondé de pouvoir. L'employé qui a créé la demande transmet ensuite les pièces justificatives à un deuxième approbateur et lui demande d'approuver la transaction dans le système de la RBC. Dès réception de la deuxième approbation, la transaction est automatiquement autorisée;
- les limites de l'autorisation sont paramétrées dans le système de la RBC et peuvent être modifiées n'importe quand par l'employé titulaire de droits d'accès administratifs à la Direction de la trésorerie;
- le personnel de la Direction de la trésorerie nous a appris que les contrôles prévus dans le système de la RBC pour la répartition des tâches empêchaient le même utilisateur de créer et d'approuver à la fois un virement électronique. Malgré tout, nous avons demandé à la Direction de la trésorerie de procéder à un sondage pour confirmer que ce problème ne pouvait pas se produire dans le système de la RBC. Ce sondage a permis de constater que le problème pouvait effectivement se produire, puisque ces contrôles n'existent pas dans le système de la RBC. N'importe lequel des cinq fondés de pouvoir pouvait à lui seul créer et

autoriser un virement électronique à concurrence de 25 millions de dollars. Il s'agit d'une lacune de contrôle très dangereuse. Le personnel a fait savoir que cette lacune a depuis été corrigée.

6. Tentative précédente de virement frauduleux

Au printemps 2018, la Ville a été la cible d'une tentative de manœuvre frauduleuse comparable à cet incident de virement frauduleux.

Un courriel frauduleux, censément adressé par la directrice générale de la Bibliothèque publique d'Ottawa, est parvenu à la trésorière municipale pour lui demander un virement électronique de fonds.

Le personnel de la Direction de la trésorerie a passé en revue ce courriel et a demandé de plus amples renseignements à propos de la demande de virement électronique, puisque le courriel en question ne comprenait pas les coordonnées bancaires obligatoires.

On a communiqué avec la directrice générale de la Bibliothèque publique d'Ottawa pour obtenir les coordonnées bancaires voulues; cette dernière a fait savoir qu'elle n'avait pas envoyé le courriel d'origine. Le virement électronique n'a donc pas été traité. Le problème n'a pas été signalé aux Services de sécurité de la TI ni au BVG.

7. Intervention du SPO

Le 11 juillet 2018, les Services de sécurité de la TI ont rencontré un agent du SPO pour remplir un rapport de police sur l'incident de virement frauduleux et sur la correspondance par courriel ultérieure du présumé fraudeur qui demandait le versement d'un supplément de 154 238 $ US. Au moment où nous rédigions le présent rapport, le présumé fraudeur continuait d'adresser des courriels à la trésorière municipale, et les Services de sécurité de la TI ont suggéré au SPO de jouer un rôle proactif en continuant de communiquer avec le présumé fraudeur afin de pouvoir l'identifier. L'agent du SPO auquel le dossier a été confié a fait savoir qu'il n'avait aucune expérience de la cybersécurité. Il a communiqué avec ses collègues pour leur faire savoir qu'il s'agissait d'une fraude en cours de perpétration. Les Services de sécurité de la TI nous ont appris que selon la réponse donnée à l'agent du SPO par ses collègues, le virement électronique avait été effectué et qu'on ne pouvait plus rien faire. La Ville a donc cessé de communiquer avec le présumé fraudeur.

Le personnel des Services de sécurité de la TI a fait savoir que le SPO n'avait fait aucun suivi dans ce dossier.

8. Procédures de recouvrement

Le bénéficiaire du virement frauduleux est le titulaire d'un compte bancaire suspect domicilié dans une banque aux États-Unis (le « premier compte américain »). La plus grande partie des fonds déposés dans le premier compte américain a été virée dans un autre compte bancaire ouvert au nom du même titulaire auprès d'une banque différente, elle aussi située aux États-Unis (le « deuxième compte américain »). La Ville ne savait pas que le deuxième compte américain était surveillé par l'United States Secret Service (l'« USSS »), puisqu'il était lié à des virements frauduleux se rapportant à d'autres comptes bancaires américains.

Le 3 août 2018 ou aux environs de cette date, l'USSS a communiqué avec la Ville puisque les fonds du deuxième compte américain avaient été saisis. L'USSS a fait savoir que les fonds déposés dans le deuxième compte américain correspondent au virement frauduleux; toutefois, les fonds virés par la Ville n'ont pas été déposés intégralement dans ce compte. L'USSS a estimé qu'environ 88 000 $ US ont été récupérés dans le deuxième compte américain, en faisant toutefois observer que ces fonds étaient regroupés avec les fonds obtenus frauduleusement auprès d'une autre victime d'un incident comparable à celui de la Ville.

L'avocat général a pris en charge le dossier et a déposé, auprès de l'USSS, la demande obligatoire de restitution ou d'atténuation des mesures de confiscation (la « demande »), pour faire valoir les prétentions de la Ville sur les fonds déposés dans le deuxième compte américain. Le 5 novembre 2018, l'USSS à Ottawa a fait savoir à l'avocat général que l'administration américaine compétente rendrait, dans cette demande, une décision à la fin de l'enquête et de l'examen.

9. Absence de formation sur la sensibilisation à la fraude

La Ville n'a pas, pour le personnel, de programme de formation obligatoire sur la sensibilisation à la fraude. Ce programme permet de prévenir, de détecter et de signaler les fraudes. Toutes les personnes que nous avons interviewées ont fait savoir que cette formation de sensibilisation à la fraude serait utile et qu'elle aurait pu permettre d'éviter cet incident de virement frauduleux.

En janvier 2018, les résultats d'un test d'hameçonnage[3] des Services de sécurité de la TI ont révélé un taux de défaillance de 26,5 pour cent, ce qui est supérieur à la moyenne sectorielle de 15 pour cent. Le personnel des Services de sécurité de la TI a par la suite fait savoir que la Ville de Toronto est en train de mettre en place, à l'intention de ses employés, un programme de formation obligatoire sur la sensibilisation à la fraude.

Conclusion

La Ville a été victime d'une manœuvre frauduleuse courante. Rien n'indique que le personnel de la Ville ait commis des actes répréhensibles et frauduleux relativement à cet incident. Rien n'indique non plus qu'on aurait traité, dans la période comprise entre le 3 octobre 2016 et le 17 octobre 2018, d'autres virements électroniques frauduleux comparables.

Si on avait suivi la politique et les procédures de la Ville, on aurait consigné la demande de virement frauduleuse dans le Formulaire de paiement sans référence, que l'on aurait fait suivre aux Comptes créditeurs ou à l'Unité des services financiers. À notre avis, il est improbable que ce virement ait été effectué si l'un ou l'autre de ces groupes avait traité la demande.

La Ville a de la chance puisque l'USSS surveillait le deuxième compte américain et qu'il est extrêmement rare que les victimes de ces manœuvres frauduleuses puissent récupérer leurs fonds.

Enfin, il faut améliorer considérablement les contrôles exercés par la Ville dans l'établissement des virements électroniques.

Recommandations et réponses

Recommandation nº 1

> Que la Ville mette en œuvre un processus pour dépister les courriels externes adressés au personnel et pour les afficher de manière évidente sur l'écran des postes de travail des destinataires.

[3] Dans un test d'hameçonnage, un organisme envoie des courriels trompeurs, comparables à des courriels malveillants, à son propre personnel afin de prendre la mesure de leur réaction à l'hameçonnage et aux attentats par courriel comparables.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services de sécurité de la TI des Services de technologie de l'information (STI) mettent actuellement à l'essai des solutions potentielles qui devraient être mises en œuvre au troisième trimestre de 2019.

Recommandation nº 2

Que la Ville finalise et approuve la politique et les procédures qui obligent les Comptes créditeurs ou l'Unité des services financiers à traiter, examiner et approuver tous les paiements par virement électronique.

Réponse de la direction

La direction est d'accord avec cette recommandation.

La Direction de la trésorerie travaille de concert avec les Comptes créditeurs (CC) pour mettre à jour la Politique et les procédures de paiement des fournisseurs, afin d'y intégrer des politiques et des procédures précises sur les paiements par virement électronique. Ce travail doit être terminé d'ici le deuxième trimestre de 2019. Entretemps, la Direction de la trésorerie s'est réunie avec les CC et l'USF pour confirmer que dorénavant, ils examineront et approuveront toutes les demandes de paiement par virement électronique avant le traitement des transactions.

Recommandation nº 3

Que la Ville adresse un communiqué à tous les membres de la direction pour préciser qu'ils ne sont pas habilités à déroger aux contrôles et qu'ils seront tenus responsables des cas de non-conformité.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services des finances municipales travailleront de concert avec les Services de l'approvisionnement afin de mettre au point un communiqué à l'intention de tous les membres de la direction pour renforcer les politiques, les procédures et les contrôles portant sur les finances et l'approvisionnement afin d'autoriser les paiements destinés aux fournisseurs. Ce communiqué sera élaboré et publié par le Bureau du directeur municipal à l'intention de tous les gestionnaires d'ici le premier trimestre de 2019.

Recommandation nº 4

Que la Ville s'assure que les approbations matérielles sont consignées en bonne et due forme pour consultation ultérieure; il s'agit de la confirmation selon laquelle les signatures matérielles sont légitimes (par rapport à la fiche de modèle de signature) et que les noms sont transcrits en caractères d'imprimerie.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le personnel de la Direction de la trésorerie responsable du traitement des opérations de virement électronique a désormais accès à la plateforme des pouvoirs de signature de SAP pour pouvoir vérifier et faire concorder tous les modèles de signature lorsqu'il s'agit d'approuver un paiement par virement électronique.

La Direction de la trésorerie travaille de concert avec les Comptes créditeurs afin de mettre au point la Politique et les procédures de paiement des fournisseurs pour y intégrer des politiques et des procédures précises pour les paiements par virement électronique afin de s'assurer que les signatures matérielles sont légitimes et qu'elles sont consignées en bonne et due forme, et qu'il existe un processus de vérification pour assurer la conformité. Ce travail sera terminé d'ici le deuxième trimestre de 2019.

Recommandation nº 5

Que la Ville prépare les rapports récapitulatifs mensuels se rapportant aux virements électroniques créés et autorisés. Un cadre supérieur des Finances doit passer en revue et signer ces rapports, qui doivent être versés au dossier pour consultation ultérieure. Toutes les anomalies recensées doivent être signalées immédiatement au Bureau du vérificateur général.

Réponse de la direction

La direction est d'accord avec cette recommandation.

On peut actuellement consulter les rapports mensuels sur les activités produits dans les systèmes existants, notamment les rapports sur les activités relatives aux paiements par virement, aux transferts de compte et à l'administration. Les nouveaux rôles et les nouvelles responsabilités dans le cadre de ce processus seront mis en œuvre au premier trimestre de 2019. La documentation de ce

processus sera intégrée dans la nouvelle section consacrée aux paiements par virement électronique de la version à jour des Procédures sur le paiement des fournisseurs, qui sera terminée d'ici le deuxième trimestre de 2019.

Recommandation nº 6

Que la Ville passe en revue ses pratiques actuelles et établisse les limites d'autorisation et les règles d'approbation en bonne et due forme en ce qui a trait à l'émission des paiements par virement électronique. Que la Ville délègue, au responsable compétent de ces règles, l'obligation de s'assurer qu'elles seront établies et respectées en bonne et due forme dans le système de l'institution financière.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les limites d'autorisation et les règles d'approbation en bonne et due forme en ce qui a trait à l'émission des paiements par virement électronique et aux rôles et responsabilités dans le respect de ces règles feront partie de la nouvelle section consacrée aux paiements par virement électronique de la version à jour des Procédures de paiement des fournisseurs, qui sera terminée d'ici le deuxième trimestre de 2019.

Recommandation nº 7

Que la Ville se concerte avec son institution financière pour désactiver la fonction qui permet, aux employés de la Direction de la trésorerie auxquels on a attribué des droits administratifs, de modifier les droits d'accès et l'autorisation. Tous les changements à apporter aux droits d'accès et d'autorisation doivent l'être par l'institution financière uniquement après avoir reçu par écrit les instructions d'un fondé de pouvoir supérieur de la Ville.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le personnel de la Direction de la trésorerie a discuté de cette recommandation avec l'institution financière, qui a fait savoir qu'elle n'est pas prête à prendre cette responsabilité. Elle insiste pour dire qu'il appartient au client de désigner les administrateurs internes compétents pour gérer ces pouvoirs.

Les Services des finances municipales passeront en revue la séparation des tâches et les droits administratifs de la Direction de la trésorerie, déterminera les pratiques exemplaires et mettra en œuvre les contrôles, la séparation des tâches et les rôles et responsabilités clairs dont il faut s'acquitter pour attribuer les droits administratifs d'ici le deuxième trimestre de 2019.

Recommandation nº 8

Que la Ville apporte des modifications à ses profils d'autorisation dans le système de l'institution financière pour éviter qu'un même employé de la Ville puisse à la fois créer et approuver la même transaction de virement électronique et vérifie que ces modifications sont en vigueur.

Réponse de la direction

La direction est d'accord avec cette recommandation.

La fonction qui permet au même employé de créer et d'approuver à la fois un virement électronique dans le système de l'institution financière a été supprimée, sauf à l'intention des employés qui ont des droits administratifs, selon le mode de fonctionnement du système de l'institution bancaire. L'application de la recommandation nº 7 permettra de s'assurer que la séparation des tâches est appropriée et qu'il existe des contrôles permettant de s'assurer que les employés titulaires de droits administratifs ne peuvent pas créer ou approuver de virements électroniques. Ces modifications des rôles, des responsabilités et des procédures seront mises en œuvre et seront intégrées dans la nouvelle section consacrée aux paiements par virement électronique de la version à jour des Procédures de paiement des fournisseurs, qui sera terminée d'ici le deuxième trimestre de 2019.

Recommandation nº 9

Que la Ville déclare au Bureau du vérificateur général toutes les tentatives de fraude contre la Ville dans les cas où des employés municipaux auraient établi une correspondance avec les fraudeurs ou déjà entrepris les mesures requises.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services de sécurité de la TI des Services de technologie de l'information (STI) mettent actuellement au point un programme de formation sur la sensibilisation à la cybersécurité obligatoire dans l'ensemble de l'administration municipale. On a publié une demande de propositions et attribué un contrat pour

mettre au point ce programme, qui prévoit l'obligation de déclarer les tentatives de fraude. On s'attend à ce que cette recommandation soit mise en œuvre d'ici le deuxième trimestre de 2019.

Recommandation nº 10

Que la Ville crée et mette en œuvre un programme de formation pour la sensibilisation à la fraude, qui s'étendrait au Code de conduite, aux risques de fraude, ainsi qu'au rôle des employés dans la prévention et la déclaration des fraudes.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Comme l'indique la réponse apportée à la recommandation nº 9, les Services de sécurité de la TI des Services de technologie de l'information (STI) mettent actuellement au point, pour toute l'administration municipale, un programme obligatoire de sensibilisation à la cybersécurité qui sera mis en œuvre d'ici le deuxième trimestre de 2019. Ce programme s'étendra au Code de conduite, aux risques de fraude et au rôle de l'employé dans la prévention et la déclaration des fraudes.

Dans l'intervalle, les STI ont mis au point, à l'intention du personnel, un message pour lui permettre de dépister les risques d'hameçonnage et les autres risques de sécurité auxquels il pourrait être soumis et de supprimer les courriels d'hameçonnage. Le 4 octobre 2018, on a adressé un courriel à tous les membres du personnel qui ont accès au réseau pour les informer de ces risques. En outre, des articles ont été publiés dans l'ensemble de l'administration municipale, dans l'infolettre de la Ville (*Au courant*) le 24 juillet 2018 et l'information a été publiée sur le site intranet de la Ville (Ozone), que les employés sont obligés de lire avant d'avoir accès à la page de renvoi. Dans le cadre du programme de sensibilisation à la cybersécurité, les STI adresseront chaque trimestre aux employés des messages se rapportant aux risques auxquels la Ville est soumise.

Rapport d'enquête détaillé

Enquête sur le virement de fonds à un faux fournisseur

Introduction

Le 11 juillet 2018, le Bureau du vérificateur général (le « BVG ») de la Ville d'Ottawa (la « Ville ») a reçu un rapport relatif à un virement de fonds de la Ville totalisant la somme de 97 797,20 $ US versée dans le compte d'un présumé fraudeur qui avait fait appel à des moyens frauduleux (le « paiement frauduleux »).

En vertu de la *Politique en matière de fraude et d'abus* de la Ville, le BVG est essentiellement chargé, de concert avec le greffier municipal et avocat général (l' « avocat général »), le cas échéant, de prendre connaissance de toutes les allégations de fraude ou d'abus au sens défini dans la *Politique en matière de fraude et d'abus*, et de mener ou de recommander des enquêtes sur ces allégations, le cas échéant.

Pour donner suite aux allégations dont il a pris connaissance, le BVG a mené une enquête sur cette question de paiement frauduleux. Avec l'accord du BVG, la Ville en a également saisi le Service de police d'Ottawa (le « SPO »).

Renseignements généraux et contexte

La Direction de la trésorerie de la Ville traite tous les paiements en monnaies étrangères par virement électronique, puisqu'à l'heure actuelle, le module des comptes créditeurs du système financier de la Ville ne permet pas de traiter les virements électroniques de fonds (VEF) en monnaies étrangères. En outre, certains paiements en dollars canadiens sont également effectués par virement électronique.

Le 6 juillet 2018, la directrice générale des Services organisationnels et trésorière municipale (la « trésorière municipale ») a reçu un courriel (le « courriel ») apparemment adressé par le directeur municipal. L'auteur de ce courriel demandait qu'un virement électronique pour la somme de 97 797,20 $ US (les « fonds ») soit traité pour effectuer une acquisition que, selon ce qu'affirmait l'auteur du courriel, le directeur municipal négociait à huis clos depuis un certain temps.

La trésorière municipale a mené sur Internet une recherche à propos du bénéficiaire, qu'elle a identifié comme une entreprise de conception de pages Web qui exerce ses

activités dans le domaine de la technologie de l'information (« TI ») et qui a son siège aux États-Unis. La trésorière municipale a supposé que l'acquisition se rapportait à un fournisseur qui pouvait apporter de l'aide dans la refonte indispensable du site Web ottawa.ca.

Toujours le 6 juillet 2018, la Direction de la trésorerie a, conformément à l'approbation de la trésorière municipale, traité et émis les fonds en dollars américains, par virement électronique international à destination d'une banque aux États-Unis.

Le 11 juillet 2018, la trésorière municipale a reçu un autre courriel, qui provenait à nouveau, en apparence, du directeur municipal. L'auteur de ce courriel demandait si elle était à son bureau, puisqu'il fallait émettre dans l'avant-midi même le solde du paiement (154 238 $ US) se rapportant à l'acquisition. Lorsqu'elle a reçu ce courriel, la trésorière municipale participait à une séance du Conseil municipal et a amorcé une discussion avec le directeur municipal à propos de la demande de virement électronique. Le directeur municipal a fait savoir à la trésorière municipale qu'il n'était pas du tout au courant de ces demandes de virement électronique; après avoir pris connaissance des courriels, il a fait savoir à la trésorière municipale qu'il ne les lui avait pas envoyés et que la Ville avait été victime de fraude.

La Ville n'a pas traité la demande de virement électronique adressée le 11 juillet 2018 par le présumé fraudeur. La trésorière municipale a aussitôt communiqué avec le directeur des Services de sécurité de la TI, et avec le gestionnaire de la Direction de la trésorerie, pour porter à leur connaissance le paiement frauduleux. Le gestionnaire de la Direction de la trésorerie a aussitôt prévenu l'institution financière de la Ville, soit la Banque Royale du Canada (la « RBC »), afin de recouvrer les fonds, en vain. Le directeur des Services de sécurité a aussitôt commencé à intervenir, conformément au Plan d'intervention en cas d'incident informatique et à la *Politique en matière de fraude et d'abus* de la Ville. Le Bureau du vérificateur général et l'avocat général adjoint ont été prévenus et ont pris ensemble la décision d'en saisir le Service de police d'Ottawa.

Le 12 juillet 2018, le BVG a fait savoir à l'avocat général qu'il mènerait une enquête interne dans cette affaire.

Objectifs

Voici en quoi consistaient, dans l'ensemble, les objectifs de l'enquête :

1. mener une enquête factuelle sur la réception de la demande de paiement et sur le processus de traitement du paiement frauduleux;
2. déterminer si des paiements frauduleux comparables à celui qui a fait l'objet de cette enquête ont pu être traités auparavant;
3. examiner les contrôles en vigueur en ce qui a trait à ces processus et recommander les améliorations à y apporter dans les cas nécessaires.

Portée

La portée de l'enquête consistait à savoir si les politiques et les procédures de la Ville avaient été respectées en ce qui a trait au traitement du paiement frauduleux, si une manœuvre de paiement frauduleux comparable avait pu se produire auparavant et s'il existait des contrôles relativement à ces processus. Dans les cas où des problèmes potentiels ont été relevés, la portée de l'enquête a été élargie afin de les évaluer et de faire les recommandations nécessaires.

Approche

L'approche adoptée dans le déroulement de l'enquête comportait les activités suivantes :

- examen de documents, notamment :
  - la Politique sur le paiement des fournisseurs[4];
  - les Procédures relatives au paiement des fournisseurs[5];
  - le Formulaire de paiement sans référence[6];
  - le Règlement municipal sur la délégation de pouvoirs, soit le Règlement nº 369 de 2016[7];
  - la Politique sur la délégation de pouvoirs[8];

[4] Date de la révision : le 9 mars 2017.

[5] Date de la révision : le 9 mars 2017.

[6] Formulaire FIN001 V1.4, révisé le 20 juillet 2010.

[7] Règlement adopté par le Conseil municipal à sa séance du 23 novembre 2016.

[8] Politique révisée par le Conseil municipal le 13 février 2013.

  - les Procédures sur les virements électroniques à l'intention des fournisseurs (ébauche);
  - le Processus de traitement des virements électroniques (ébauche);
  - les organigrammes de la Direction générale des services organisationnels, des Services des finances municipales, de la Direction de la comptabilité et de la Direction de la trésorerie[9];
  - les documents fournis par les Services de sécurité de la TI relativement à leurs procédures d'intervention en cas d'incident.

- examen de pièces justificatives se rapportant à certaines transactions de virement électronique à partir des données fournies par la Direction de la trésorerie[10] et application de certains critères, pour la période comprise entre le 6 janvier 2015 et le 31 août 2018;
- exécution de procédures d'analyse de données en ce qui a trait aux données fournies par la RBC sur les virements électroniques par rapport au compte de banque de la Ville pour la période comprise entre le 3 octobre 2016 et le 17 octobre 2018. À partir des résultats des procédures d'analyse des données, nous avons procédé à l'analyse des pièces justificatives se rapportant à certains virements électroniques respectant certains critères;
- analyse du processus général mené par la Direction de la trésorerie dans le paiement par virement électronique;
- entrevues menées auprès de membres du personnel de la Ville à la Direction générale des services organisationnels, dont les Services de sécurité de la TI, les Finances municipales et la Direction de la trésorerie, et demandes de renseignements adressées à ces membres du personnel;
- demandes de renseignements adressées au directeur municipal actuel et à l'ancien directeur municipal;
- autres procédures d'enquête et d'analyse jugées nécessaires pour permettre de tirer des conclusions sur les objectifs de l'enquête.

[9] En date du 1er janvier 2018.

[10] Document obtenu dans le cadre du système comptable (SAP) de la Ville.

Constatations détaillées

Les constatations découlant de l'enquête sont reproduites sous les rubriques suivantes.

1. Chronologie des événements – paiement frauduleux

Nous reproduisons ci-après la chronologie des événements qui se sont produits le vendredi 6 juillet 2018 par rapport à la correspondance échangée par courriel en ce qui a trait au paiement frauduleux.

Heures (HNE)	Détails
10 h 29	La trésorière municipale reçoit un courriel apparemment adressé par le directeur municipal. On constate ensuite que l'adresse reproduite dans le courriel (« directeurmunicipal@ottawa.ca ») est une adresse frauduleuse.[11] L'adresse de courriel effective du présumé fraudeur est plutôt « info@e-officenq.com », comme on peut le constater en plaçant le curseur sur l'adresse de courriel. Le courriel se lit comme suit : *« Bonjour [Nom de la trésorière municipale]. Êtes-vous à votre bureau actuellement? [Directeur municipal] »*
10 h 31	La trésorière municipale répond au présumé fraudeur, à son adresse de courriel effective (info@e-officenq.com) : *« Oui. Appelez-moi. »*
10 h 51	Le présumé fraudeur adresse le courriel suivant à la trésorière municipale : *« D'accord. J'aimerais que vous vous occupiez de cette affaire pour moi personnellement. Je viens d'apprendre que notre offre a été acceptée par un nouveau fournisseur à l'étranger, pour conclure une acquisition que je négocie à huis clos depuis un certain temps maintenant. Conformément aux conditions convenues, nous devons verser un acompte de 30 % du total, soit 97 797,20 $.* *Nous sommes en train de rédiger un projet de texte pour annoncer la nouvelle la semaine prochaine, lorsque l'accord aura été signé. Pour l'instant, je ne souhaite pas donner d'autres détails.*

[11] L'usurpation d'une adresse de courriel consiste à contrefaire cette adresse de courriel pour que le destinataire croie que le message provient d'un expéditeur digne de confiance, alors qu'il est envoyé par quelqu'un d'autre. La correspondance est acheminée à l'adresse de courriel réelle du présumé fraudeur.

Heures (HNE)	Détails
	Tant que nous ne serons pas en mesure d'annoncer officiellement cette acquisition, je vous invite à ne pas en discuter avec qui que ce soit au bureau. Si vous avez des questions, veuillez m'adresser un courriel. *Pourriez-vous confirmer que le virement électronique à l'étranger peut être traité cet avant-midi?* *[Directeur municipal] »*
11 h 03	Après s'être renseignée auprès de la Direction de la trésorerie, la trésorière municipale adresse la réponse suivante au présumé fraudeur : *« Les virements électroniques à destination de l'Europe et de l'Asie ne peuvent plus être traités aujourd'hui, puisque les banques de ces continents sont maintenant fermées. Le virement serait envoyé lundi au plus tôt pour ces destinations. Il faudrait le faire parvenir avant 10 h, puisqu'en raison des fuseaux horaires, les banques seraient fermées passé cette heure. Il va de soi que nous pouvons traiter un virement à destination des États-Unis, ce qu'il faut toutefois faire avant 11 h 30.* *Faites-moi savoir ce que vous déciderez. »*
11 h 10	La trésorière municipale adresse la réponse suivante au présumé fraudeur, après avoir reçu des renseignements supplémentaires de la part de la Direction de la trésorerie : *« On vient de me faire un compte rendu : nous avons jusqu'à 16 h 30 si le virement est destiné aux États-Unis. S'il faut le traiter dans une monnaie différente du dollar américain ou du dollar canadien, il faut compter deux jours ouvrables. »*
12 h 11	Le présumé fraudeur adresse à la trésorière municipale le courriel suivant : *« D'accord. Voici les coordonnées bancaires du fournisseur.* *NOM DE LA BANQUE :* [redacted] *ADRESSE DE LA BANQUE :* [redacted] *NOM DU COMPTE :* [redacted] *ADRESSE DU BÉNÉFICIAIRE .* [redacted]

Heures (HNE)	Détails
	NUMÉRO DU COMPTE : xxxx *CODE SWIFT :* xxxx *NUMÉRO D'ACHEMINEMENT :* xxxx *MONTANT ET DEVISE : 97 797,20 $ US* *Prévenez-moi quand le virement sera fait et faites-moi parvenir le bordereau de confirmation.* *[Directeur municipal]»*
12 h 16	La trésorière municipale adresse au présumé fraudeur la réponse suivante : *« Ce sera fait. »*
12 h 35	La Direction de la trésorerie crée un virement électronique pour la somme de 97 797,20 $ US (128 603,32 $ CA).
12 h 43	La Direction de la trésorerie autorise le virement électronique.
12 h 49	La Direction de la trésorerie adresse un courriel à la trésorière municipale pour lui faire savoir que la transaction a été effectuée.
12 h 50	La trésorière municipale adresse un courriel directement au directeur municipal, sans se servir de l'adresse de courriel frauduleuse, pour confirmer que la transaction a été effectuée. (Pendant l'entrevue menée avec le directeur municipal, ce dernier a confirmé qu'il avait bien reçu ce courriel et qu'il s'était mis une note pour faire un suivi auprès de la trésorière municipale à une date ultérieure afin d'en discuter. Cette discussion n'a pas eu lieu avant le 11 juillet 2018, après la demande ultérieure de fonds supplémentaires du présumé fraudeur.)
13 h 55	Le présumé fraudeur adresse le courriel suivant à la trésorière municipale : *« Pourriez-vous confirmer que le virement a été traité?* *Merci.* *[Directeur municipal] »*

Heures (HNE)	**Détails**
13 h 58	La trésorière municipale adresse la réponse suivante au présumé fraudeur : *« Je vous ai fait parvenir la confirmation à 12 h 50. Vous ne l'avez pas reçue? »*
14 h 05	Le présumé fraudeur adresse à la trésorière municipale le courriel suivant : *« Non, je ne l'ai pas reçue. Pourriez-vous m'en faire parvenir une copie?* *Merci.* *[Directeur municipal] »*
14 h 21	Le présumé fraudeur adresse à la trésorière municipale le courriel suivant : *« [Nom de la trésorière municipale],* *Ce virement est toujours en attente à la banque. Veuillez me prévenir quand ce paiement aura été effectué par la banque.* *Merci.* *[Directeur municipal] »*
14 h 29	La trésorière municipale joint au courriel qu'elle adresse au présumé fraudeur une copie du rapport détaillé sur le virement et lui répond : *« Le paiement est maintenant effectué. »*
14 h 34	Le présumé fraudeur adresse à la trésorière municipale le courriel suivant : *« Merci.* *[Directeur municipal] »*

2. Dépistage de la manœuvre frauduleuse : la « fraude du faux PDG »

Dans les deux dernières années, la cybercriminalité est devenue le crime économique le plus souvent dénoncé par les entreprises et les organismes au Canada.[12]

Les cybercriminels s'en prennent mondialement aux entreprises et aux organismes en faisant appel à une manœuvre frauduleuse répandue, appelée la « fraude du faux PDG ».[13] Voici ce qui se produit dans ces attentats, dont la Ville a été victime dans cet incident de virement frauduleux :

- les fraudeurs ont accès au compte de courriel d'un cadre supérieur ou créent une adresse de courriel comparable et ciblent les employés titulaires de fonctions financières qui sont habilités à transférer des fonds dans l'entreprise ou l'organisme;
- les fraudeurs font parvenir des courriels d'aspect réaliste, en demandant des virements électroniques urgents pour des motifs professionnels en apparence légitime, par exemple pour « obtenir un contrat important », « réaliser une transaction confidentielle » ou « mettre à jour l'information sur les paiements d'un fournisseur »;
- les fraudeurs adressent souvent des courriels frauduleux ciblés lorsque les cadres supérieurs se déplacent à l'étranger ou sont normalement difficiles à joindre;
- en croyant que la demande est authentique, l'employé fait virer les fonds, pour constater, au retour de son supérieur hiérarchique, que le courriel était un subterfuge et que les fonds se sont volatilisés.

Dans ce type de subterfuge, les pertes sont généralement comprises entre des dizaines de milliers et des millions de dollars. La fraude du faux PDG est une menace mondiale grandissante pour les entreprises et les organismes de plus ou moins grande envergure.

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

[13] https://www.canada.ca/fr/bureau-concurrence/nouvelles/2017/06/montrez-leur_quiestlepatronmettezfinalarnaquedufauxpdg.html

3. Impossibilité de connaître l'identité de l'auteur véritable du courriel (origine interne ou externe)

À la date à laquelle s'est produit l'incident de virement frauduleux, les courriels transmis par les employés de la Ville ne permettaient pas de savoir s'il s'agissait d'un courriel interne de la Ville ou d'un courriel externe. Cette précision permet de mieux attirer l'attention du destinataire sur les pourriels ou les autres courriels suspects, qui pourraient servir à l'hameçonnage[14] ou comprendre des maliciels dangereux.

Dans nos entrevues, le personnel des Services de sécurité de la TI a déclaré qu'en réaction à l'incident de virement frauduleux, on a demandé aux groupes responsables du serveur d'échange de courriels dans l'exploitation des réseaux et en nuagique de mettre en œuvre un mécanisme pour permettre de dépister visuellement tous les courriels d'origine externe.

Recommandation nº 1

> Que la Ville mette en œuvre un processus pour dépister les courriels externes adressés au personnel et pour les afficher de manière évidente sur l'écran des postes de travail des destinataires.

Réponse de la direction

> La direction est d'accord avec cette recommandation.
>
> Les Services de sécurité de la TI des Services de technologie de l'information (STI) mettent actuellement à l'essai des solutions potentielles qui devraient être mises en œuvre au troisième trimestre de 2019.

4. Intervention louable des Services de sécurité de la TI

Comme nous l'avons mentionné, le 11 juillet 2018, l'incident de virement frauduleux a été signalé aux Services de sécurité de la TI, qui ont aussitôt lancé leur intervention conformément au Plan d'intervention en cas d'incident informatique (le « Plan »).

[14] Il s'agit d'une tentative de fraude destinée à obtenir des renseignements confidentiels comme des noms d'utilisateur, des mots de passe et des détails sur des cartes de crédit, en faisant croire que le message électronique provient d'une entité digne de confiance.

L’objectif du Plan, tel qu’il est exposé dans de document, consiste à :

- dépister et analyser :
  - la menace;
  - l’ampleur de l’incident;
  - les répercussions de l’incident sur la Ville;
- circonscrire l’incident :
  - recenser les contrôles à exercer et les mesures à prendre pour éviter que l’incident cause d’autres préjudices;
- maîtriser l’incident :
  - supprimer la menace dans les systèmes ou le réseau et rétablir l’environnement pour qu’il soit de nouveau « digne de confiance »;
- reprendre les activités normales après l’incident :
  - remettre en service les systèmes de traitement des données touchés selon un ordre de priorités pour permettre de reprendre les opérations professionnelles normales;
- tirer les leçons de l’incident :
  - établir un rapport d’événement précisant les constatations sur l’incident, ainsi que les lacunes relevées et que l’on peut corriger pour réduire la probabilité que l’incident se reproduise.

Voici les procédures adoptées entre autres par les Services de sécurité de la TI :

- ils ont programmé et tenu une téléconférence avec les Services juridiques de la Ville pour discuter de l’incident;
- ils ont nommé une personne-ressource principale comme responsable de l’incident;
- ils ont confirmé que l’adresse de courriel du directeur municipal n’avait pas été piratée et qu’une adresse de courriel frauduleuse avait été utilisée pour commettre la fraude;
- pour éviter que d’autres courriels frauduleux soient transmis à des employés, ils ont mis en œuvre un processus selon lequel tous les courriels comportant le suffixe @e-officenq.com dans l’adresse de courriel du présumé fraudeur soient

versés dans un dossier sécurisé auquel seuls pourraient avoir accès certains employés des Services de sécurité de la TI;

- ils ont procédé à des recherches et confirmé qu'il n'y avait pas eu d'autres communications passées depuis des adresses de courriel inconnues à d'autres employés de la Ville et comportant l'adresse de courriel du présumé fraudeur (info@e-officenq.com) depuis le 1er mars 201815;
- ils ont conservé toute la correspondance échangée par courriel entre le présumé fraudeur et la trésorière municipale;
- ils ont interviewé la trésorière municipale pour réunir les détails sur le paiement frauduleux;
- après s'être mis en rapport avec l'avocat général adjoint et le Bureau du vérificateur général et leur avoir demandé des directives, ils ont communiqué et se sont réunis avec le SPO pour déposer un rapport16 sur l'incident de virement frauduleux et sur la tentative de fraude ultérieure du présumé fraudeur;
- ils ont confirmé, auprès de la Direction de la trésorerie, que l'institution financière (RBC) avait lancé un avertissement spécial sur toutes les transactions éventuelles, puisque le présumé fraudeur pouvait connaître une partie des coordonnées bancaires;
- ils ont consigné par écrit toutes les mesures adoptées;
- ils ont donné une formation sur la lutte contre la fraude aux employés de la Direction de la trésorerie.

Les Services de sécurité de la TI ont apporté leur entière collaboration au BVG dans le cadre de cette enquête et ont fourni au BVG tous les documents recueillis à la suite de leur intervention dan. En sachant que les Services de sécurité de la TI ont d'abord pris la responsabilité du dossier avant que le BVG prenne en charge l'enquête, il faut les féliciter de leur intervention rapide, puisqu'ils ont montré qu'ils étaient prêts à intervenir en cas d'incident informatique regrettable.

[15] Courriels accessibles sur le serveur de la Ville.

[16] Numéro du dossier (18-169146).

5. Non-conformité à la *Politique sur le paiement des fournisseurs* et aux *Procédures relatives au paiement des fournisseurs* de la Ville

Dans le cadre de l'enquête, nous avons évalué le paiement frauduleux pour savoir s'il respectait la *Politique sur le paiement des fournisseurs*[17] (la « politique ») et les *Procédures relatives au paiement des fournisseurs* (les « procédures ») de la Ville. Nous avons constaté que les procédures pertinentes n'ont pas été respectées.

Voici ce que précise la politique :

- Énoncé

  « Tous les paiements dus aux fournisseurs doivent être effectués au moyen du mode le plus efficient disponible, en s'assurant que l'autorisation adéquate a été obtenue et que toutes les conditions de paiement ont été satisfaites. »

- Conditions de paiement et traitement des factures

  « … Les factures sont traitées au moyen de MarkvVew (le système automatisé de traitement des factures de la Ville) ou d'un autre système, selon le cas. Le mode privilégié est MarkView; »
  « Les paiements peuvent être effectués au moyen d'un système autre que MarkView dans les cas suivants :
  - *Lorsque le respect de la présente politique ne s'applique pas ou n'est pas adopté (p. ex. conseils locaux et représentants élus);*
  - *Lorsqu'il faut tenir compte de la confidentialité;*
  - *Lorsqu'il n'y a aucune facture (un formulaire de paiement sans référence doit être rempli);*
  - *Lorsque la pièce justificative de paiement est traitée par enregistrement direct (voir les Procédures relatives au paiement des fournisseurs). »*

Voici ce que précisent les procédures :

- Application

  « Elles ne s'appliquent ni aux conseils locaux de la Ville ni aux représentants élus. Les présentes procédures ne portent pas sur les remboursements et les demandes de remboursement des employés. »

- Traitement des factures sans bon de commande

[17] Date de la révision : le 9 mars 2017.

Le tableau ci-après fait état du processus qui se déroule entre la facturation sans bon de commande et le paiement.

Origine de la facture	Processus
Sans faire appel à MarkView	• L'utilisateur opérationnel code la facture. • Il s'assure que le fondé de pouvoir compétent a approuvé la facture. • Il joint à la facture le Formulaire de paiement sans référence (FPSR) (annexe A) et les pièces justificatives, le cas échéant. • Il fait suivre la facture, le FPSR et les copies des pièces justificatives à la DSF[18] pour examen. • La DSF passe en revue la facture et le FPSR et, le cas échéant, les estampille et les signe pour confirmer qu'elle en a pris connaissance. • La DSF enregistre les données sur le paiement dans le système SAP. • Elle note le numéro du document sur la facture, la numérise et la fait suivre par courriel (AP-Attachments@ottawa.ca).

D'après les constatations de l'enquête, nous avons relevé ce qui suit :

- le paiement frauduleux n'a pas été traité dans le système MarkView;
- la DSF n'est pas intervenue dans cette transaction;
- on n'a pas établi le Formulaire de paiement sans référence;
- l'approbation selon les pouvoirs délégués a été délivrée d'après la teneur des courriels présumément envoyés par le directeur municipal;
- on n'a pas fourni de pièce justificative à la Direction de la trésorerie pour traiter le paiement. La teneur du courriel du présumé fraudeur, transmis le 6 juillet 2018 à 12 h 11 et qui fait état des coordonnées bancaires du présumé fraudeur est la seule information qui a été mise à la disposition de la Direction de la trésorerie;
- on n'a pas fourni de code (compte du grand-livre général, budget ou centre de coût ou de profit) à la Direction de la trésorerie pour traiter la transaction;
- la Direction de la trésorerie n'a pas de politique ni de procédure officielle approuvée pour les virements électroniques. Dans la foulée de l'incident de

[18] Direction des services financiers.

virement frauduleux, on a préparé des versions provisoires de cette politique et de ces procédures, qu'on est en train de finaliser.

Voici ce qu'a déclaré la trésorière municipale dans l'entrevue que nous avons menée auprès d'elle :

- elle a confirmé que tous les employés de la Ville doivent respecter la Politique et les Procédures pour le paiement des biens et des services;
- la Politique et les Procédures n'ont pas été respectées dans le traitement de ce paiement frauduleux parce que le directeur municipal a le pouvoir de déroger à une politique dans les cas d'urgence. Elle s'est conformée à la demande du directeur municipal d'après la teneur des courriels, qu'elle a crus légitimes.

Nous avons interrogé l'ancien directeur municipal et le directeur municipal en poste, qui ont tous deux affirmé qu'ils n'avaient jamais demandé directement qu'un paiement soit traité par les Comptes créditeurs ou qu'un virement électronique soit effectué par la Direction de la trésorerie. L'actuel directeur municipal a déclaré qu'à son avis, il est investi de certains pouvoirs permettant de demander des paiements urgents; il y a toutefois un certain nombre de critères à respecter, et il faut notamment déclarer immédiatement ces paiements au Conseil municipal.

Nous avons passé en revue le *Règlement municipal sur la délégation de pouvoirs* (le « Règlement ») et avons relevé les articles suivants en ce qui concerne les « *circonstances urgentes ou particulières* » :

> *« 5 – En cas d'urgence ou de circonstances particulières exigeant une intervention dans le cadre du mandat normal d'une direction générale, le directeur général peut prendre les mesures jugées nécessaires pour rectifier la situation, même si ces mesures excèdent le pouvoir délégué.*
>
> *6 – Toute mesure prise en vertu de l'article 5 doit être signalée immédiatement au comité permanent concerné.*
>
> *7 – En cas d'urgence ou de circonstances particulières exigeant une intervention qui excède le mandat normal d'une direction générale, le directeur municipal peut prendre les mesures jugées nécessaires pour rectifier la situation.*
>
> *8 – Toute mesure prise en vertu de l'article 7 doit être signalée immédiatement au comité permanent concerné, puis au Conseil. »*

La Politique précise clairement que toutes les conditions doivent être respectées et que les Procédures s'appliquent à tous les employés de la Ville. La trésorière municipale n'a pas respecté la Politique et les Procédures. Si la Politique et les Procédures avaient été respectées, la demande aurait été traitée par l'entremise des Comptes créditeurs ou de la Direction des services financiers. À notre avis, il est beaucoup moins probable que le paiement aurait été effectué si l'un de ces groupes avait traité la demande.

Recommandation nº 2

Que la Ville finalise et approuve la politique et les procédures qui obligent les Comptes créditeurs ou l'Unité des services financiers à traiter, examiner et approuver tous les paiements par virement électronique.

Réponse de la direction

La direction est d'accord avec cette recommandation.

La Direction de la trésorerie travaille de concert avec les Comptes créditeurs (CC) pour mettre à jour la Politique et les procédures de paiement des fournisseurs, afin d'y intégrer des politiques et des procédures précises sur les paiements par virement électronique. Ce travail doit être terminé d'ici le deuxième trimestre de 2019. Entretemps, la Direction de la trésorerie s'est réunie avec les CC et l'USF pour confirmer que dorénavant, ils examineront et approuveront toutes les demandes de paiement par virement électronique avant le traitement des transactions.

Recommandation nº 3

Que la Ville adresse un communiqué à tous les membres de la direction pour préciser qu'ils ne sont pas habilités à déroger aux contrôles et qu'ils seront tenus responsables des cas de non-conformité.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services des finances municipales travailleront de concert avec les Services de l'approvisionnement afin de mettre au point un communiqué à l'intention de tous les membres de la direction pour renforcer les politiques, les procédures et les contrôles portant sur les finances et l'approvisionnement afin d'autoriser les paiements destinés aux fournisseurs. Ce communiqué sera élaboré et publié par

le Bureau du directeur municipal à l'intention de tous les gestionnaires d'ici le premier trimestre de 2019.

6. Contrôles insuffisants dans le traitement des virements électroniques

Nous avons relevé de dangereuses lacunes de contrôle en ce qui a trait au traitement des virements électroniques. Afin de savoir s'il avait pu y avoir auparavant des paiements frauduleux par virement électronique, comparables à la manœuvre de paiement frauduleux dont la Ville a été victime, nous avons mené les procédures d'enquête juricomptable ci-après :

- nous avons analysé le processus réalisé par la Direction de la trésorerie pour les paiements par virement;
- nous avons mené une analyse des pièces justificatives par rapport aux transactions de virement électronique sélectionnées, à partir des données fournies par la Direction de la trésorerie[19], pour la période comprise entre le 6 janvier 2015 et le 31 août 2018. Nous avons sélectionné 19 transactions à analyser, d'après les critères suivants :
  - absence des noms des fournisseurs;
  - noms de fournisseurs douteux;
  - possibilité de paiement en double.
- Nous avons appliqué des procédures d'analyse des données portant sur le virement électronique et fournies par la RBC par rapport au compte de banque de la Ville utilisé pour traiter les virements électroniques, pour la période comprise entre le 3 octobre 2016 et le 17 octobre 2018. Nous avons sélectionné, pour cette analyse, huit transactions d'après les résultats des procédures suivantes appliquées dans l'analyse des données :
  - nous avons procédé à l'analyse des noms du créateur et de l'approbateur ou du responsable de l'autorisation afin de savoir si le même employé avait exercé ces deux fonctions. Nous n'avons pas relevé de cas dans lesquels le même employé aurait pu exercer les deux fonctions;
  - les virements électroniques étaient initialement filtrés d'après le volume des transactions traitées pour chaque bénéficiaire pendant l'exercice financier;

[19] Données extraites du système comptable de la Ville (SAP).

- nous avons retranché de l'échantillon les bénéficiaires dont on savait qu'ils avaient des rapports professionnels légitimes avec la Ville, soit les conseils scolaires, la Commission de la capitale nationale et les cabinets d'avocats;
- pour le reliquat de l'échantillon des virements électroniques, nous avons recensé les bénéficiaires dont le volume de transaction est faible (quatre transactions ou moins), en particulier les transactions traitées dans les devises distinctes du dollar canadien. Nous avons sélectionné huit virements électroniques pour examen.

Le lecteur trouvera ci-après nos constatations en ce qui a trait aux procédures d'enquête juricomptable que nous avons appliquées et que nous venons d'évoquer ci-dessus :

- rien ne prouve que des paiements frauduleux comparables à la manœuvre de paiement frauduleux dont il est question dans ce rapport ont été émis;
- toutes les transactions que nous avons analysées étaient accompagnées de pièces justificatives suffisantes. Ces pièces comportaient les signatures de l'approbateur; toutefois, nous n'avons pas toujours pu connaître l'identité des approbateurs, puisque leur nom n'était pas reproduit en caractères d'imprimerie;
- on avait prévu une séparation des tâches entre la personne qui crée la demande de virement électronique et le personnel de la Direction de la trésorerie qui approuve et autorise le virement dans le système bancaire de la RBC (le « système de la RBC »);
- les pièces justificatives portant sur les virements électroniques sont versées au dossier pour chaque transaction. Puisque l'on ne prépare pas de rapport de synthèse des virements électroniques, la haute direction ne peut pas en prendre connaissance;
- le système de la RBC pour les virements électroniques n'est pas directement intégré dans le système SAP de la Ville. On peut traiter des paiements par virement électronique sans indiquer le numéro de compte du grand-livre général pour affecter le paiement dans le système financier ou pour y passer des écritures;
- il n'y a pas de limite formelle constatée par écrit pour les autorisations de la Ville (règles d'approbation) en ce qui a trait aux paiements par virement électronique;
- pour paramétrer un paiement par virement électronique, l'employé autorisé commence par le créer dans le système de la RBC. L'employé qui a créé le paiement fait alors suivre les pièces justificatives à l'approbateur et lui demande

d'approuver le paiement dans le système de la RBC. Si la transaction est inférieure à 25 millions de dollars, le paiement est autorisé dès qu'il est approuvé. Si la transaction est supérieure à 25 millions de dollars, le paiement doit être approuvé par un deuxième responsable. Le créateur du paiement fait alors suivre les pièces justificatives au deuxième approbateur et lui demande d'approuver la transaction dans le système de la RBC. Dès que la deuxième approbation est délivrée, la transaction est automatiquement autorisée;

- les limites d'autorisation sont fixées dans le système de la RBC et peuvent être modifiées n'importe quand par un employé de la Direction de la trésorerie qui a des droits d'accès administratifs. Le lecteur pourra prendre connaissance, ci-après, des limites d'autorisation qui étaient en vigueur au moment de notre enquête;
- sont autorisés à créer, dans le système de la RBC, les coordonnées des nouveaux bénéficiaires des paiements :

    1. les agents principaux de placement (deux);
    2. l'analyste des activités de trésorerie;
    3. l'analyste de la Direction de la trésorerie;
    4. le gestionnaire de la Direction de la trésorerie;
    5. la trésorière municipale adjointe;
    6. la trésorière municipale;

- sont autorisés à approuver les nouveaux bénéficiaires des paiements (deux des responsables ci-après doivent donner leur approbation) :

    1. les agents principaux de placement (deux);
    2. le gestionnaire de la Direction de la trésorerie;
    3. la trésorière municipale adjointe;
    4. la trésorière municipale (qui est également autorisée à approuver les nouveaux fournisseurs qu'elle a elle-même créés dans le système);

- sont autorisés à créer des virements électroniques :

    1. les agents principaux de placement (deux);
    2. l'analyste des activités de trésorerie;
    3. l'analyste de la Direction de la trésorerie;
    4. le gestionnaire de la Direction de la trésorerie;
    5. la trésorière municipale adjointe;
    6. la trésorière municipale;

- sont autorisés à approuver les virements électroniques :
    1. les agents principaux de placement (deux);
    2. le gestionnaire de la Direction de la trésorerie;
    3. la trésorière municipale adjointe;
    4. la trésorière municipale;
- les virements électroniques de moins de 25 millions de dollars peuvent être approuvés et autorisés par l'un quelconque des responsables visés ci-dessus et autorisés à approuver les transactions;
- les virements électroniques de plus de 25 millions de dollars doivent être approuvés par deux des responsables visés ci-dessus et autorisés à approuver les transactions;
- les droits d'accès administratifs sont attribués :
    - à l'agent principal de placement (un agent seulement);
    - au gestionnaire de la Direction de la trésorerie;
    - à la trésorière municipale adjointe;
    - à la trésorière municipale;
- le personnel de la Direction de la trésorerie nous a appris que les contrôles institués pour la séparation des tâches dans le système de la RBC empêchaient le même utilisateur de créer et d'approuver à la fois un virement électronique. Nous avons quand même demandé à la Direction de la trésorerie de procéder à un sondage pour confirmer que cette éventualité ne pouvait pas se produire dans le système de la RBC. Or, il s'est révélé que cette éventualité pouvait effectivement se produire. Par conséquent, ces contrôles n'existent pas dans le système de la RBC. N'importe lequel des cinq employés autorisés pourrait à lui seul créer et autoriser un virement électronique à concurrence de 25 millions de dollars. Il s'agit d'une lacune de contrôle dangereuse. Pour donner suite à cette constatation, les dirigeants de la Direction de la trésorerie ont fait savoir qu'ils avaient apporté les changements nécessaires pour maîtriser ce risque.

Recommandation nº 4

Que la Ville s'assure que les approbations matérielles sont consignées en bonne et due forme pour consultation ultérieure; il s'agit de la confirmation selon laquelle les signatures matérielles sont légitimes (par rapport à la fiche de modèle de signature) et que les noms sont transcrits en caractères d'imprimerie.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le personnel de la Direction de la trésorerie responsable du traitement des opérations de virement électronique a désormais accès à la plateforme des pouvoirs de signature de SAP pour pouvoir vérifier et faire concorder tous les modèles de signature lorsqu'il s'agit d'approuver un paiement par virement électronique.

La Direction de la trésorerie travaille de concert avec les Comptes créditeurs afin de mettre au point la Politique et les procédures de paiement des fournisseurs pour y intégrer des politiques et des procédures précises pour les paiements par virement électronique afin de s'assurer que les signatures matérielles sont légitimes et qu'elles sont consignées en bonne et due forme, et qu'il existe un processus de vérification pour assurer la conformité. Ce travail sera terminé d'ici le deuxième trimestre de 2019.

Recommandation nº 5

Que la Ville prépare les rapports récapitulatifs mensuels se rapportant aux virements électroniques créés et autorisés. Un cadre supérieur des Finances doit passer en revue et signer ces rapports, qui doivent être versés au dossier pour consultation ultérieure. Toutes les anomalies recensées doivent être signalées immédiatement au Bureau du vérificateur général.

Réponse de la direction

La direction est d'accord avec cette recommandation.

On peut actuellement consulter les rapports mensuels sur les activités produits dans les systèmes existants, notamment les rapports sur les activités relatives aux paiements par virement, aux transferts de compte et à l'administration. Les nouveaux rôles et les nouvelles responsabilités dans le cadre de ce processus seront mis en œuvre au premier trimestre de 2019. La documentation de ce

processus sera intégrée dans la nouvelle section consacrée aux paiements par virement électronique de la version à jour des Procédures sur le paiement des fournisseurs, qui sera terminée d'ici le deuxième trimestre de 2019.

Recommandation nº 6

Que la Ville passe en revue ses pratiques actuelles et établisse les limites d'autorisation et les règles d'approbation en bonne et due forme en ce qui a trait à l'émission des paiements par virement électronique. Que la Ville délègue, au responsable compétent de ces règles, l'obligation de s'assurer qu'elles seront établies et respectées en bonne et due forme dans le système de l'institution financière.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les limites d'autorisation et les règles d'approbation en bonne et due forme en ce qui a trait à l'émission des paiements par virement électronique et aux rôles et responsabilités dans le respect de ces règles feront partie de la nouvelle section consacrée aux paiements par virement électronique de la version à jour des Procédures de paiement des fournisseurs, qui sera terminée d'ici le deuxième trimestre de 2019.

Recommandation nº 7

Que la Ville se concerte avec son institution financière pour désactiver la fonction qui permet, aux employés de la Direction de la trésorerie auxquels on a attribué des droits administratifs, de modifier les droits d'accès et l'autorisation. Tous les changements à apporter aux droits d'accès et d'autorisation doivent l'être par l'institution financière uniquement après avoir reçu par écrit les instructions d'un fondé de pouvoir supérieur de la Ville.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Le personnel de la Direction de la trésorerie a discuté de cette recommandation avec l'institution financière, qui a fait savoir qu'elle n'est pas prête à prendre cette responsabilité. Elle insiste pour dire qu'il appartient au client de désigner les administrateurs internes compétents pour gérer ces pouvoirs.

Les Services des finances municipales passeront en revue la séparation des tâches et les droits administratifs de la Direction de la trésorerie, déterminera les pratiques exemplaires et mettra en œuvre les contrôles, la séparation des tâches et les rôles et responsabilités clairs dont il faut s'acquitter pour attribuer les droits administratifs d'ici le deuxième trimestre de 2019.

Recommandation nº 8

Que la Ville apporte des modifications à ses profils d'autorisation dans le système de l'institution financière pour éviter qu'un même employé de la Ville puisse à la fois créer et approuver la même transaction de virement électronique et vérifie que ces modifications sont en vigueur.

Réponse de la direction

La direction est d'accord avec cette recommandation.

La fonction qui permet au même employé de créer et d'approuver à la fois un virement électronique dans le système de l'institution financière a été supprimée, sauf à l'intention des employés qui ont des droits administratifs, selon le mode de fonctionnement du système de l'institution bancaire. L'application de la recommandation nº 7 permettra de s'assurer que la séparation des tâches est appropriée et qu'il existe des contrôles permettant de s'assurer que les employés titulaires de droits administratifs ne peuvent pas créer ou approuver de virements électroniques. Ces modifications des rôles, des responsabilités et des procédures seront mises en œuvre et seront intégrées dans la nouvelle section consacrée aux paiements par virement électronique de la version à jour des Procédures de paiement des fournisseurs, qui sera terminée d'ici le deuxième trimestre de 2019.

7. Tentative antérieure de virement électronique frauduleux

Dans le cadre de l'enquête, nous avons constaté que la Ville avait été la cible d'une tentative de manœuvre frauduleuse, comparable à cet incident de virement frauduleux. En voici les détails :

- au printemps de 2018, un courriel frauduleux, censément envoyé par la directrice générale de la Bibliothèque publique d'Ottawa, a été adressé à la trésorière municipale (la trésorière municipale) pour demander un virement électronique de fonds;
- la trésorière municipale a fait suivre le courriel à la trésorière adjointe pour lui demander de s'en occuper;

- la trésorière adjointe a fait suivre le courriel à la Direction de la trésorerie;
- le personnel de la Direction de la trésorerie a pris connaissance du courriel et a demandé de plus amples renseignements à la trésorière adjointe à propos de la demande de virement électronique, puisque le courriel ne comprenait pas les coordonnées bancaires nécessaires;
- la trésorière adjointe a envoyé un courriel à la directrice générale de la Bibliothèque publique d'Ottawa pour obtenir les détails bancaires supplémentaires; la directrice générale lui a fait savoir qu'elle n'avait pas adressé le courriel d'origine;
- le virement électronique n'a pas été effectué;
- la question n'a pas été signalée aux Services de la sécurité de la TI ni au BVG.

Recommandation nº 9

Que la Ville déclare au Bureau du vérificateur général toutes les tentatives de fraude contre la Ville dans les cas où des employés municipaux auraient établi une correspondance avec les fraudeurs ou déjà entrepris les mesures requises.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services de sécurité de la TI des Services de technologie de l'information (STI) mettent actuellement au point un programme de formation sur la sensibilisation à la cybersécurité obligatoire dans l'ensemble de l'administration municipale. On a publié une demande de propositions et attribué un contrat pour mettre au point ce programme, qui prévoit l'obligation de déclarer les tentatives de fraude. On s'attend à ce que cette recommandation soit mise en œuvre d'ici le deuxième trimestre de 2019.

8. Réponse du SPO

Le 11 juillet 2018, les Services de sécurité de la TI se sont réunis avec un agent du SPO pour établir un rapport de police[20] en ce qui a trait à l'incident de virement frauduleux et au courriel ultérieur du présumé fraudeur qui demandait le versement d'un supplément de 154 238 $ US. Au moment où nous rédigions le présent rapport, le présumé fraudeur continuait de correspondre avec la trésorière municipale, et les Services de sécurité de la TI ont suggéré au SPO de jouer un rôle proactif en

[20] Numéro du dossier (18-169146).

continuant de communiquer avec le présumé fraudeur afin d'identifier le responsable de la fraude. L'agent du SPO auquel le dossier a été confié a fait savoir qu'il n'avait aucune expérience de la cybersécurité. Il a communiqué avec ses collègues pour leur faire savoir qu'il s'agissait d'une fraude en cours de perpétration. Les Services de sécurité de la TI nous ont fait savoir que les collègues de cet agent lui avaient répondu que parce que le virement électronique avait été effectué, il n'y avait rien qu'ils puissent faire. C'est pourquoi la Ville a cessé de communiquer avec le présumé fraudeur.

Le personnel des Services de sécurité de la TI a précisé que le SPO n'avait pas fait de suivi relativement à cette question.

9. Procédures de recouvrement

Le bénéficiaire du virement frauduleux est le titulaire d'un compte bancaire suspect domicilié dans une banque aux États-Unis (le « premier compte américain »). La plus grande partie des fonds déposés dans le premier compte américain a été virée dans un autre compte bancaire ouvert au nom du même titulaire auprès d'une banque différente, elle aussi située aux États-Unis (le « deuxième compte américain »). La Ville ne savait pas que le deuxième compte américain était surveillé par l'United States Secret Service (l'« USSS »), puisqu'il était lié à des virements frauduleux se rapportant à d'autres comptes bancaires américains.

Le 3 août 2018 ou aux environs de cette date, l'USSS a communiqué avec la Ville puisque les fonds du deuxième compte américain avaient été saisis. L'USSS a fait savoir que les fonds déposés dans le deuxième compte américain correspondent au virement frauduleux; toutefois, les fonds virés par la Ville n'ont pas été déposés intégralement dans ce compte. L'USSS a estimé qu'environ 88 000 $ US ont été récupérés dans le deuxième compte américain, en faisant toutefois observer que ces fonds étaient regroupés avec les fonds obtenus frauduleusement auprès d'une autre victime d'un incident comparable à celui de la Ville.

L'avocat général a pris en charge le dossier et a déposé, auprès de l'USSS, la demande obligatoire de restitution ou d'atténuation des mesures de confiscation (la « demande »), pour faire valoir les prétentions de la Ville sur les fonds déposés dans le deuxième compte américain. Le 5 novembre 2018, l'USSS à Ottawa a fait savoir à l'avocat général que l'administration américaine compétente rendrait, dans cette demande, une décision à la fin de l'enquête et de l'examen.

La Ville a beaucoup de chance, puisqu'il est extrêmement rare que les victimes de ces manœuvres frauduleuses puissent récupérer leurs fonds.

10. Absence de formation sur la sensibilisation à la fraude

La sensibilisation à la fraude permet de prévenir, de détecter et de dénoncer les fraudes. Tous les employés interviewés ont fait savoir que la formation sur la sensibilisation à la fraude serait utile et qu'elle aurait pu empêcher que l'incident de virement frauduleux se produise. Le personnel des Services de sécurité de la TI avait fait preuve de clairvoyance en offrant des séances de sensibilisation discrétionnaires sur la question avant que cet incident se produise; or, le personnel des Services de sécurité de la TI a fait savoir qu'il faut adopter un programme de sensibilisation obligatoire.

En janvier 2018, les Services de sécurité de la TI ont mené un test d'hameçonnage[21], dans le cadre duquel 200 utilisateurs de la Ville ont été sélectionnés au hasard. Selon le résultat de ce test, 53 utilisateurs ont cliqué sur le lien du courriel d'hameçonnage, ce qui donne un taux d'échec de 26,5 pour cent. Le personnel des Services de sécurité de la TI a fait savoir que la moyenne sectorielle est de 15 pour cent et qu'à son avis, les résultats confirment qu'il faut donner une formation obligatoire sur la sensibilisation à la cybercriminalité et à la fraude. Le personnel des services de sécurité de la TI a en outre fait savoir que la Ville de Toronto est en train de déployer, auprès de ses employés, un programme obligatoire de formation sur la sensibilisation à la fraude.

Recommandation nº 10

> Que la Ville crée et mette en œuvre un programme de formation pour la sensibilisation à la fraude, qui s'étendrait au Code de conduite, aux risques de fraude, ainsi qu'au rôle des employés dans la prévention et la déclaration des fraudes.

[21] Dans un test d'hameçonnage, un organisme envoie des courriels trompeurs, comparables à des courriels malveillants, à son propre personnel afin de prendre la mesure de leur réaction à l'hameçonnage et aux attentats par courriel comparables.

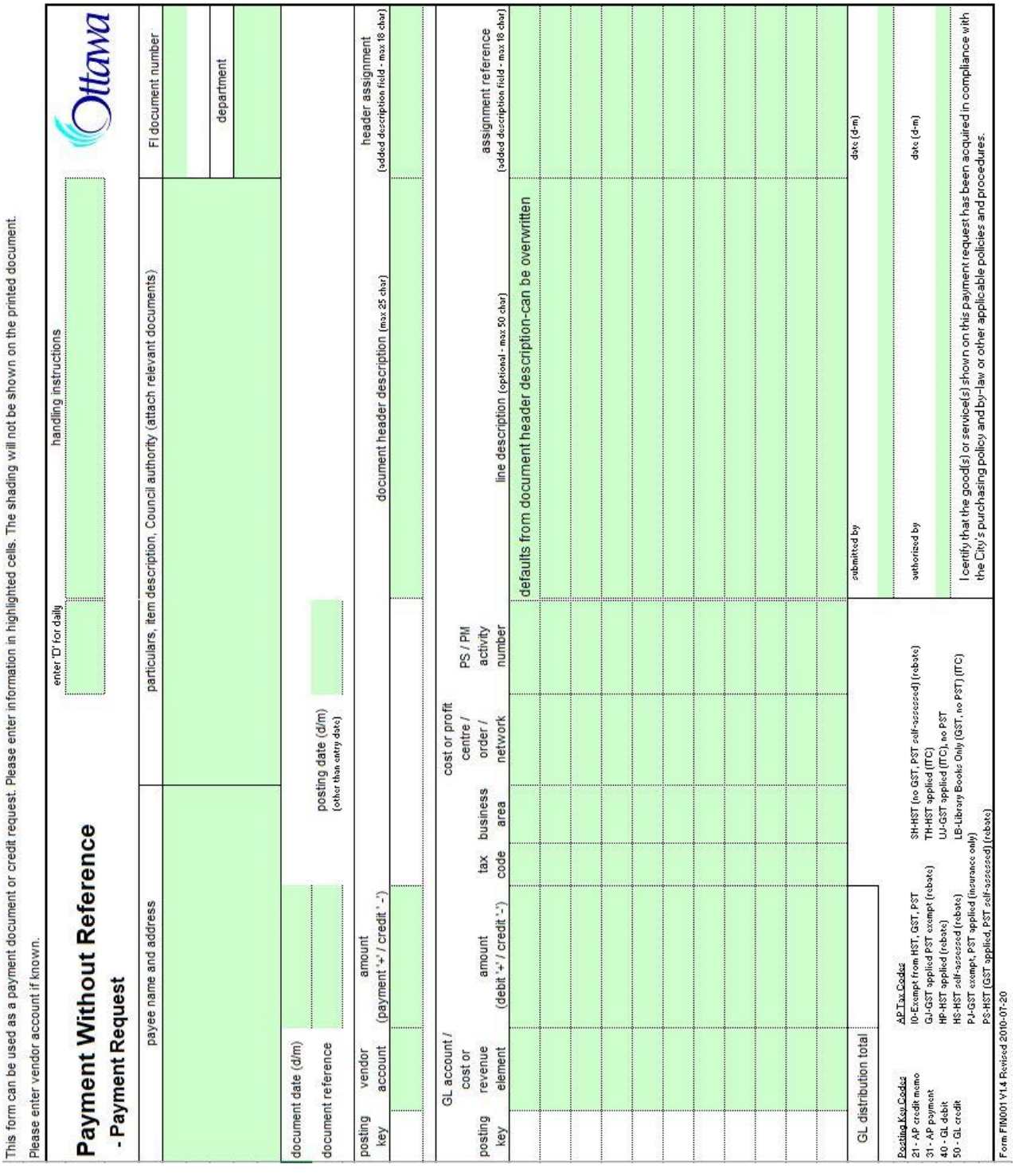
Réponse de la direction

La direction est d'accord avec cette recommandation.

Comme l'indique la réponse apportée à la recommandation nº 9, les Services de sécurité de la TI des Services de technologie de l'information (STI) mettent actuellement au point, pour toute l'administration municipale, un programme obligatoire de sensibilisation à la cybersécurité qui sera mis en œuvre d'ici le deuxième trimestre de 2019. Ce programme s'étendra au Code de conduite, aux risques de fraude et au rôle de l'employé dans la prévention et la déclaration des fraudes.

Dans l'intervalle, les STI ont mis au point, à l'intention du personnel, un message pour lui permettre de dépister les risques d'hameçonnage et les autres risques de sécurité auxquels il pourrait être soumis et de supprimer les courriels d'hameçonnage. Le 4 octobre 2018, on a adressé un courriel à tous les membres du personnel qui ont accès au réseau pour les informer de ces risques. En outre, des articles ont été publiés dans l'ensemble de l'administration municipale, dans l'infolettre de la Ville (*Au courant*) le 24 juillet 2018 et l'information a été publiée sur le site intranet de la Ville (Ozone), que les employés sont obligés de lire avant d'avoir accès à la page de renvoi. Dans le cadre du programme de sensibilisation à la cybersécurité, les STI adresseront chaque trimestre aux employés des messages se rapportant aux risques auxquels la Ville est soumise.

Annexe A – Formulaire de paiement sans référence



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 '-')					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
21 - AP credit memo
31 - AP payment
40 - GL debit
50 - GL credit

AP Tax Codes
I0-Exempt from HST, GST, PST
GJ-GST applied PST exempt (rebate)
HP-HST applied (rebate)
HS-HST self-assessed (rebate)
PJ-GST exempt, PST applied (insurance only)
PS-HST (GST applied, PST self-assessed) (rebate)
SH-HST (no GST, PST self-assessed) (rebate)
TH-HST applied (ITC)
UJ-GST applied (ITC), no PST
LB-Library Books Only (GST, no PST) (ITC)

authorized by — date (d-m)

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.

Form FIN001 V1.4 Revised 2010-07-20