COMMENT PROTÉGER VOTRE ENTREPRISE DE LA FRAUDE : EXEMPLES COURANTS ET MEILLEURES PRATIQUES

Montréal, le 3 décembre 2019

Ronald Audette
Associé | Chef national, Groupe de litiges bancaires

Jeanne Morency | Conseillère juridique principale, Litige, RBC Groupe Juridique

GOWLING WLG

I. LES TYPES DE FRAUDES BANCAIRES LES PLUS FRÉQUENTES

1. La fraude du président (cyberfraude)

1.1. Description

Il s'agit d'un stratagème frauduleux où le fraudeur se fait passer pour le président ou un haut dirigeant d'une entreprise par courriel adressé à un employé de l'entreprise (souvent une personne du département de comptabilité) pour demander un virement bancaire à l'étranger. Le fraudeur exige normalement de sa victime qu'elle effectue un virement international urgent pour une transaction confidentielle. Un soi-disant avocat, conseiller ou autres tiers identifié dans le courriel frauduleux prend ensuite le relai pour donner des instructions supplémentaires à sa victime.

GOWLING WLG

1.2. Caractéristiques

Les caractéristiques de cette cyberfraude aidant à l'identifier sont :

i. Demande de virement international adressée par le président ou un haut dirigeant de l'entreprise à un employé du département de comptabilité ou autre personne autorisée à faire des virements à l'étranger;

ii. Demande de traiter le transfert et le virement bancaire de façon confidentielle;

iii. Demande de traiter la demande de virement bancaire de façon urgente;

iv. Le président ou le haut dirigeant n'est pas au bureau lorsque la demande est reçue;

v. La requête du fraudeur est dirigée à un employé autorisé à s'occuper des transferts bancaires/contrôleur de l'entreprise.

1.3. Exemples réels

a. La Coop fédérée, fraude de 5,5 millions $

https://www.lapresse.ca/actualites/201701/19/01-5061353-comment-un-escroc-a-vole-5,5-millions-a-la-coop-federee.php

- La Coop fédérée est propriétaire des quincailleries BMR et des marques de viandes Olymel. Un géant du monde agricole dont le chiffre d'affaires avoisine les 10 milliards de dollars annuels.

- La Coop avait une comptable professionnelle agréée, Mme Cadieux, avec beaucoup d’expérience. Elle avait travaillé au Vérificateur général du Canada avant de se joindre à la Coop. Elle avait ensuite gravi les échelons à La Coop, où elle est devenue contrôleuse des finances.

- Elle occupait le poste depuis 10 ans lorsque les fraudeurs ont frappé, le 21 août 2014.

- C’était un jeudi matin à 9 h 32, elle reçoit un courriel de Gaétan Desroches, chef de la direction de La Coop, qui n'est pas physiquement au bureau ce jour-là.

- Il lui explique que l'entreprise va procéder à une offre publique d'achat (OPA). L'opération est rigoureusement surveillée par l'Autorité des marchés financiers du Québec (AMF) et doit être tenue strictement confidentielle jusqu'à sa conclusion. Il lui demande de prendre contact avec un avocat externe, « Maître Deschamps », pour préparer un virement de fonds.
- Des escrocs ont envoyé le courriel qui semble provenir de M. Desroches.
- Ils savent que Mme Cadieux est en mesure d'autoriser des virements bancaires. Ils savent probablement aussi que le chef de la direction n'est pas au bureau en ce moment.
- Le modus operandi des fraudeurs est adapté au Québec : il est question d'une OPA, de l'AMF, d'un avocat externe.
- À La Coop fédérée, Mme Cadieux a plusieurs conversations téléphoniques avec le mystérieux « Maître Deschamps ». Il demande des copies de documents, notamment des exemples de transferts de fonds passés. Il sait que la signature d'une autre employée, Johanne Gauthier, est nécessaire pour le virement, mais il assure qu'il va la contacter lui-même.
- Mme Cadieux prépare un bordereau, inscrit les codes d'autorisation appropriés et l'envoie à l'avocat. Celui-ci le lui retourne avec la signature de Johanne Gauthier. En fait, cette dernière n'a jamais été contactée. Les fraudeurs ont copié sa signature dans un des anciens documents envoyés par Mme Cadieux.

- La contrôleuse des finances envoie la demande de transfert à la Banque Nationale, où La Coop fédérée a son compte. Cinq millions US (5,5 millions CA selon le taux de change de l'époque) doivent être acheminés à une banque chinoise, au bénéfice d'une entreprise nommée Acceleration Trade, dont le siège social serait au 1, Road Street, à Hong Kong (une adresse bidon). La banque s'exécute.

- Le surlendemain, en échangeant avec son patron, Mme Cadieux découvre l'arnaque. La Coop fédérée avise la Banque Nationale, qui déclenche un branle-bas de combat, rappelle d'urgence des employés au travail, tente des appels à New York et en Chine, dans l'espoir de récupérer les fonds. Mais nous sommes maintenant samedi. Pas la meilleure journée pour des opérations bancaires complexes sur deux continents.

- Les fonds n'ont pas été récupérés. La Coop avait 2 couvertures d'assurance (une spécifique pour la fraude et une générale) et a soumis une réclamation à ses assureurs. L'assureur spécifique a couvert et l'autre a nié couverture.

- Un litige entre la Coop et ses assureurs est monté jusqu'en Cour d'appel. La banque a été appelée en garantie par les assureurs. En gros, la Cour d'appel s'est prononcée sur le partage entre les assureurs et non pas la responsabilité de la banque.

b. Dossier Alfagomma, fraude de 1,8 millions $

- Les faits suivants viennent des procédures judicaires publiques déposées au dossier de la Cour supérieure dans un litige impliquant Alfgomma Canada et sa banque la HSBC, qui viendra à procès devant la Cour en Juin 2020.

- Alfagomma Canada est un fabricant, producteur et distributeur de tuyaux hydrauliques industriels. Alfagomma Canada fait partie d'un groupe multinational de sociétés privées dont le bureau est situé à Milan, en Italie.

- Les propriétaires du groupe Alfagomma en Italie étaient deux frères, Enrico Gennasio et Guido Gennasio. Enrico qui réside en Italie, était président de Groupe Alfagomma. Guido était président et administrateur de sa filiale canadienne, Alfagomma Canada.

- Alfagomma Canada avait 2 autres administrateurs: M. Dino Sacchetti,VP Finance et M. Ignazio Blanco, DG.

- Au moment des faits, le nom, la fonction, le numéro de téléphone et l'adresse électronique de M. Bianco adresse n'ont pas été divulgués sur le site Web d'Alfagomma.

- Le 25 juin 2015, vers 12 h 10, M. Blanco a reçu un appel téléphonique d'un individu s'identifiant comme étant M. Paolo Rossetti, prétendant être un avocat italien engagé par le groupe Alfagomma. L'appel a été acheminé vers le téléphone portable de M. Bianco à partir de son bureau d'Alfagomma Canada.

- À l'époque, cet appel téléphonique n’a pas soulevé de soupçons auprès de M. Blanco, car il savait que le groupe Alfagomma Italie, devait engager un avocat. Le fraudeur prétendant être l'avocat Paolo Rossetti avait un parfait accent italien et toutes ses communications verbales et écrites étaient impeccables.

- Le fraudeur a demandé à M. Blanco s’il avait des détails d’une transaction qui, selon le fraudeur, le groupe Alfagomma allait faire. M. Blanco a répondu qu’il n’était pas au courant. Cependant, la notion d’une transaction imminente n’était pas inhabituelle, car Alfagomma Group avait des antécédents de croissance internationale par acquisitions. En outre, à l'époque, M. Blanco était au courant que Alfagomma a été impliquée dans une acquisition potentielle, à Toronto.

- M. Blanco a informé le fraudeur qu’il aurait besoin d’un mandat de Enrico. Le fraudeur a répondu que cela ne poserait aucun problème et a également indiqué à M. Blanco que les choses devraient aller vite parce que Enrico était pressé.

- À 12 h 38, le même jour, M. Blanco a reçu un courriel de « Enrico Gennasio <enrico.gennasio@alfagomma.com> mailphone@mail.com ». L’adresse électronique légitime de M. Gennasio étant enrico.gennasio@alfagomma.com. M. Blanco a estimé qu'il s'agissait d'un courriel légitime envoyé par M. Gennasio à partir d'un iPhone.

- Selon cet e-mail frauduleux, Enrico demande à M. Blanco d'être disponible pour traiter un dossier confidentiel avec le groupe Alfagomma et son avocat, M. Paolo Rossetti. Il s'ensuit ensuite une chaine de courriels où M. Blanco, croyant correspondre avec le vrai Enrico, a confirmé qu'il s'était entretenu avec l'avocat, M. Paolo Rossetti et qu'il attendait avoir son approbation pour procéder.
- Le courriel suivant de Enrico demande à M. Blanco de faire un paiement de 660 000 $ US à une entreprise indiquée par M. Rossetti et d'écrire à M. Rossetti à son adresse électronique (Paolo.rossettilaw@gmail.com) pour lui dire que le paiement devait être effectué dans la journée même. M. Blanco a répondu qu'il s'entretiendrait avec M. Rossetti et appellerait également leur vice-président à la HSBC pour s'assurer de pouvoir procéder durant la journée.
- M. Blanco a eu plusieurs autres appels le 25 juin 2015, avec le fraudeur prétendant être l'avocat, M. Paolo Rossetti. Le fraudeur a notamment fourni un numéro de téléphone permettant de le joindre: 0039-02-5831-4742. Le chiffre fourni avait du sens pour M. Blanco, car le 0039 était le préfixe pour l'Italie et 02 était le code pour Milan, où la tête du groupe Alfagomma est située.
- Le fraudeur a envoyé un courriel à M. Blanco fournissant les coordonnées d'une banque située en Chine. Ceci n'a pas soulevé de soupçons parce à l'époque des faits, le groupe Alfagomma était implanté en Chine au travers de deux filiales.

- Plus tard dans l'après-midi, M. Blanco a appelé Mme Perreault, vice-présidente adjointe de HSBC, pour lui faire savoir qu'Alfagomma Canada aurait besoin de transférer des fonds et être sûr que cela serait possible malgré l'indisponibilité de Monsieur Sacchetti.

- Au cours de l'après-midi, M. Blanco a également appelé M. Sacchetti, qui se trouvait au bureau de Alfagomma America à Burlington (Iowa), pour l'informer du transfert de 660 000 $ US qui avait déjà été traité plus tôt dans la journée. M. Sacchetti a demandé à M. Blanco s'il avait parlé à Enrico et M. Blanco lui a répondu que le transfert avait bien été demandé et approuvé par Enrico personnellement par courriel.

- Le même jour, à 16 h 30, M. Blanco a transféré à M. Sacchetti son échange de courriels avec le fraudeur se faisant passer pour Enrico et l'avocat, Paolo Rossetti.

- Vers 17 h 17, M. Rickli de HSBC a écrit à M. Blanco pour confirmer que le virement télégraphique de 660 000 $ US avait été effectué.

- Le lendemain du premier transfert, M. Rickli de HSBC a envoyé un e-mail à M. Sacchetti indiquant que HSBC avait besoin d'obtenir sa signature sur le formulaire de virement télégraphique signé la veille par M. Blanco.

-

- Un deuxième virement de 730 000 $ US a été effectué dans des circonstances similaires, toujours en Chine. Une demande pour effectuer un troisième virement a presque réussi en prétextant vouloir transférer des fonds de Alfagomma USA vers Alfagomma Canada pour soi-disant rembourser les précédents paiements faits par Alfagomma Canada en Chine.

- M. Sacchetti a voulu valider et a envoyé un courriel à Enrico confirmant qu'il était prêt à procéder au troisième transfert de fonds requis et qu'il était en attente de la confirmation du montant. Cependant, en envoyant ce courriel, M. Sacchetti n’a pas répondu à un précédent courriel du fraudeur. Il a plutôt fait un nouveau courriel et l’adresse de Enrico a été entrée automatiquement par le IPhone de M. Sacchetti. Par conséquent, le courriel de M. Sacchetti a été envoyé à Enrico à son compte de messagerie légitime, et non pas au fraudeur.

- Toutefois, M. Sacchetti n'a pas reçu de réponse immédiate à ce dernier courrier électronique car . Enrico était en vacances.

- Le lundi 6 juillet 2015, M. Sacchetti est revenu aux bureaux d' Alfagomma Canada, mais il n'avait reçu aucune réponse de Enrico. Le mardi 7 juillet, M. Sacchetti a rencontré M. Blanco. En discutant des transactions récentes, M. Sacchetti a demandé à M. Blanco si ce dernier avait parlé à Enrico. M. Blanco a expliqué que tous ses échanges avec Enrico avaient été effectués par courriel seulement.

- Un peu plus tard, M. Sacchetti a reçu un appel de Rossetti pour changer des détails du troisième virement. Le fraudeur a expliqué que les fonds devraient être transférés de la banque d' Alfagomma America de son compte à New York à la même banque chinoise et non au compte d' Alfagomma Canada.

- Vu l’absence de communication verbale avec Enrico et les demandes successives de virements importants sur une courte période et ce changement soudain de destination de dernière minute a mis M. Sacchetti mal à l'aise face à la situation.

– M. Sacchetti a tenté de joindre Enrico sur son téléphone portable mais a été redirigé vers sa messagerie vocale. Après cet appel, M. Sacchetti a appelé M. Pietro Gargano, chef des finances du groupe Alfagomma en Italie, et c'est de cette façon que la fraude a été découverte.

– Après avoir découvert la fraude, M. Blanco a immédiatement appelé le 911 pour alerter les autorités policières.

– M. Blanco a également immédiatement appelé M. Rickli de HSBC pour rappeler les virements télégraphiques. Le 8 juillet 2015, M. Blanco a reçu un appel de Mme Perreault de HSBC qui l'a informé que les virements télégraphiques étaient non réversibles.

1.4. Question : Qu'auriez-vous fait pour prévenir la fraude dans ces deux cas?

Discussion.

1.5. Mesures préventives générales

Quelles sont les mesures préventives que l'entreprise peut mettre en place pour éviter de tomber dans le piège de ce type de fraude?

En voici quelques-unes :

a) Chaque entreprise devrait adopter des mesures de contrôle interne visant à prévenir la fraude au niveau des sorties de fonds (virements bancaires et chèques);

b) Ces mesures de contrôle interne devraient prévoir au minimum ceci :

i. Limiter le nombre de personnes au sein de l'entreprise qui sont autorisées à initier des virements bancaires et à faire émettre et signer des chèques;

ii. Éduquer les employés responsables des comptes payables, des virements bancaires et des émissions des chèques des divers types de fraude possible (commis aux comptes payables, signataires de chèques, personne responsable des virements bancaires, contrôleur, vice-président, CFO);

iii. Limiter la communication d'information sur l'organisation de l'entreprise, son organigramme, sur le site internet de l'entreprise et les médias sociaux afin de ne pas rendre accessible aux fraudeurs le nom de ces personnes et le fonctionnement interne de l'entreprise;

iv. Vous pourriez aussi exiger que tout virement à l'international soit préalablement approuvé à l'interne par un minimum de deux personnes;

v. Vous pourriez mettre un « flag » dans votre système à l'égard de tout virement international avec des pays avec lesquels l'entreprise ne fait affaires exemple, la Chine, Dubaï, pays d'Afrique, etc., si c'est le cas, puisque plusieurs fraudes internationales proviennent de ces pays.

1.6. Mesures préventives plus spécifiques afin de prévenir la fraude du président

Voici certaines mesures de contrôle pour prévenir la fraude du président :

i. **Confirmation verbale** : La mesure de contrôle doit prévoir l'obligation pour la personne responsable d'effectuer un virement bancaire suite à la réception d'un courriel ou d'une autre correspondance de communiquer directement, par téléphone, avec le demandeur du virement en utilisant les coordonnés dont dispose l'entreprise et non pas celles indiquées dans le courriel ou la correspondance du fraudeur. Il faut donc confirmer verbalement avec le haut dirigeant qui a fait la demande de virement l'authenticité de sa demande de virement et consigner au dossier cet appel téléphonique;

ii. Vérifier l'adresse courriel du demandeur du virement. Généralement, le courriel frauduleux est similaire à celui du haut dirigeant de l'entreprise qui a fait la demande de virement mais comporte une lettre, un point, un chiffre ou un caractère de plus ou différent. Cependant, ceci n'est qu'un indice et n'est pas toujours le cas car le fraudeur peut avoir « hacké » l'ordinateur du président;

2. La fraude nigériane - paiement en trop

2.1. Description

Plusieurs de ces fraudes ont été faites à partir du Nigéria mais ce type de fraude est utilisé partout dans le monde. Il est à la hausse depuis 1995.

Cette fraude consiste à un stratagème frauduleux par lequel le fraudeur achète des biens ou des services d'une entreprise et fait parvenir un paiement en trop par rapport au prix du bien ou du service et demande à l'entreprise de retourner rapidement le trop payé.

Le fraudeur demandera les coordonnés bancaires de l'entreprise pour y effectuer un dépôt, soit un chèque ou une traite bancaire frauduleux et demandera à l'entreprise de retourner rapidement le montant excédentaire. Fréquemment, le fraudeur laissera croire qu'il a effectué un virement bancaire au compte de l'entreprise alors que tel n'est pas le cas. Souvent, le chèque ou la traite déposé au compte sera une fausse traite tirée sur une banque US.

Les caractéristiques qui aident à détecter cette fraude sont les suivantes :

2.2. Caractéristiques

i. Achat de biens ou de services souvent par internet sur le site Web de l'entreprise ou par courriel adressé à l'entreprise;

ii. Le fraudeur demande les coordonnées bancaires de l'entreprise pour y effectuer un prétendu dépôt;

iii. Le fraudeur prétend que son comptable ou lui-même ont effectué une erreur en transmettant à l'entreprise un montant supérieur au prix des biens ou des services vendus par l'entreprise;

iv. Le fraudeur demande le retour rapide des fonds « excédentaires » et exerce de la pression sur la victime pour qu'elle s'exécute.

2.3. Exemple réel :

- La présidente d'une galerie d'art de Montréal reçoit par courriel une demande d'un individu situé à Dubaï indiquant être intéressé à l'achat de différents tableaux car ce dernier prétend agir pour un riche homme d'affaires intéressé à acheter des œuvres d'art québécoises.
- Le fraudeur transmet une demande de prix pour plusieurs tableaux qui totalise environ 35 000 $.
- Le fraudeur demande par la suite à la galerie d'art de lui transmettre les coordonnés bancaires de l'entreprise en lui disant que son client désire acheter les œuvres d'art et qu'il transmettra un virement bancaire au compte de l'entreprise.

- Quelques mois plus tard, un dépôt est effectué au compte bancaire de l'entreprise et le fraudeur communique avec la présidente de la galerie d'art pour lui indiquer que son comptable a fait une erreur et lui a transmis un virement destiné à un autre client. Le fraudeur affirme qu'il a transmis un paiement en trop qui aurait dû être acheminé à un autre fournisseur et demande le retour rapide des fonds.
- Le montant déposé au compte était de 135 000 $ US.
- La petite galerie d'art qui n'est pas habituée à recevoir des montants aussi importants dans son compte ressent l'urgence de retourner rapidement les fonds déposés à son compte.

- La galerie d'art vérifie auprès de sa banque si un virement bancaire est sécuritaire et se fait rassurer par sa banque croyant erronément avoir reçu un virement bancaire car le fraudeur lui avait dit qu'il ferait un virement à son compte. Cependant, elle ne demande pas à sa banque et ne fait aucune vérification pour déterminer si le dépôt spécifique provenant de l'acheteur de Dubaï était véritablement un virement bancaire ou un chèque.
- Elle demande à sa banque si les fonds sont « disponibles » à son compte sans plus de détails.
- La banque confirme que les fonds sont « disponibles » parce qu'elle ne gèle pas les dépôts effectués au compte de l'entreprise en raison de son bon crédit et non parce qu'il s'agit d'un virement bancaire effectué au compte. La galerie d'art donne instruction à sa banque de retourner l'excédent, soit 100 000 $ US. Malheureusement, ce n'est pas un virement qui avait été déposé dans son compte mais bien une fausse traite bancaire tirée sur une banque US et la fausse traite bancaire a été retournée par la banque US et le compte bancaire est devenu à découvert de 100 000 $ US.

2.4. Question: Qu'auriez-vous fait pour prévenir cette fraude?

Discussion.

2.5 Mesures préventives générales

Avant de retourner les fonds supposément reçus en trop, il est primordial de vous assurer auprès de votre institution financière que vous avez reçu un virement bancaire dans votre compte d'entreprise et non un chèque ou une traite. De plus, il est recommandé de communiquer avec votre institution financière afin de :

i. Expliquer tous les faits pertinents à votre banquier et ne vous limitez pas à poser des questions précises sans donner le contexte factuel; parler à votre directeur de compte si possible;

ii. Obtenir une copie du virement déposé à votre compte et demander à votre institution financière de valider l'authenticité s'il s'agit d'un virement en vous assurant que votre entreprise est le bénéficiaire désigné sur le virement et ce, pour éviter tout rappel du virement;

iii. S'il s'agit d'un chèque ou d'une traite bancaire, obtenez une copie et demandez à votre institution financière de valider l'authenticité du chèque ou de la traite bancaire auprès de l'institution financière sur laquelle le chèque ou la traite est tiré;

iv. Dans le cas où cela est encore possible, demandez à votre banque de faire remplacer par la banque US le chèque par une traite tirée sur la banque US ou retournez le chèque à l'acheteur et demandez un virement bancaire;

v. Attendre l'expiration des délais de compensation avant de retourner les fonds et demander une confirmation écrite à votre banque que l'item a été compensé et qu'elle a reçu paiement de la banque tirée;

vi. Vérifiez si l'émetteur du chèque correspond à votre acheteur;

vii. S'assurer que la traite ou le chèque est fait à l'ordre de votre entreprise et non pas qu'il a été endossé par le bénéficiaire et déposé à votre compte;

viii. Vérifiez s'il y a un « match » entre le nom de votre acheteur et le nom de la personne à qui on vous demande de retourner les fonds « excédentaires » et s'il n'y a pas de « match », cela devrait soulever des doutes;

ix. Ne pas céder à la pression de retourner les fonds rapidement;

x. Restez prudent et diligent et exercez votre bon jugement.

2.6. Exemples

Si vous recevez un chèque de 135 000 $ pour une transaction de 35 000 $ ceci devrait éveiller votre suspicion qu'il s'agit d'une fraude.

Si un acheteur à Dubaï vous émet un chèque tiré sur une banque US et le dépose dans votre compte alors qu'il vous avait promis un virement, ceci aussi devrait soulever une suspicion.

3. FRAUDE PAR VIREMENT ÉLECTRONIQUE À UN FAUX FOURNISSEUR OU SUITE À UN CHANGEMENT DE COORDONNÉS BANCAIRES

3.1. Description

Il s'agit d'une fraude assez fréquente appelée « Change in Supplier's Account/Changement au compte du fournisseur » par laquelle un fraudeur personnifie un véritable fournisseur de l'entreprise et demande qu'un paiement lui soit effectué par virement bancaire en transmettant, préalablement ou simultanément de nouvelles coordonnés bancaires pour rediriger les fonds payables au véritable bénéficiaire.

3.2. Caractéristiques

Afin d'aider à détecter cette fraude, on peut souligner les caractéristiques suivantes :

i. La demande de paiement sera précédée ou accompagnée d'une demande de changement des coordonnés bancaires du fournisseur;

ii. Cette demande de changement des coordonnés bancaires du fournisseur sera adressée fréquemment à une personne aux comptes payables de l'entreprise, tel qu'un commis comptable;

iii. Le fraudeur utilisera une adresse courriel très semblable à celle du véritable fournisseur de l'entreprise et pourra même « hacker » l'ordinateur de votre fournisseur.

3.3. Exemples réels

a) Changement des coordonnés bancaires d'un fournisseur

Le cas d'une université en Alberta qui avait un contrat public pour la construction d'un immeuble de plusieurs millions de dollars.

Le nom du constructeur était connu du public puisque le contrat avait été octroyé et publié suite à l'appel d'offres. Les fraudeurs disposaient donc d'informations utiles pour commettre leur fraude. Les fraudeurs ont donc adressé un courriel au commis comptable de l'université pour lui transmettre les nouvelles coordonnés bancaires du supposé entrepreneur en construction qui s'appelait Clark Builders Inc. Une lettre comportant une signature frauduleuse du CFO de l'entrepreneur accompagnait le courriel et confirmait le changement de coordonnées bancaires.

L’adresse courriel utilisée par le fraudeur était très similaire à l’adresse courriel du département des comptes à recevoir du véritable entrepreneur. La bonne adresse courriel était :

accountsreceivables@clarkbuilders.com

Alors que l’adresse frauduleuse utilisée fut :

accounts.receivables@clarkbuilders.com

Donc seulement par l’insertion d’un « point », entre le mot « accounts » et « receivables », a permis de tromper la commis comptable.

Lorsque la commis comptable a reçu la demande de changement de coordonnés bancaires de Clark Builders, elle a procédé au changement sans parler directement avec un représentant de l’entrepreneur pour confirmer la demande de changement de coordonnés bancaires.

Quelque temps plus tard, le fraudeur a fait parvenir un courriel demandant paiement des factures du constructeur.

L'Université a effectué trois virements bancaires au compte bancaire des fraudeurs totalisant 11,8 millions de dollars.

Nous verrons ci-après que les procédures juridiques entreprises au Canada et à Hong Kong ont permis de récupérer environ 11 millions de dollars.

b) Changement des coordonnés bancaires du vendeur auprès d'un bureau d'avocats

Récemment, un avocat d'un grand cabinet national a reçu un courriel de son prétendu client lui transmettant de nouvelles coordonnés bancaires pour effectuer le virement de son compte en fidéicommis suite à la vente de son entreprise pour plusieurs millions de dollars.

L'avocat a trouvé suspicieuse cette demande de changement de coordonnés bancaires à la dernière minute et a donc communiqué verbalement avec son client pour valider la demande de changement de coordonnés bancaires.

Heureusement, la fraude a été détectée à temps dans ce cas-ci.

3.4. Question : Qu'auriez-vous fait pour éviter la fraude dans ces deux cas?

Discussion.

3.5. Mesures préventives spécifiques pour prévenir ce type de fraude

Les mesures de contrôle internes devraient prévoir spécifiquement qu'aucun changement de coordonnés bancaires d'un fournisseur ne peut être effectué à moins que certaines vérifications soient effectuées, dont les suivantes :

i. Toujours détenir le nom d'une personne responsable du fournisseur dans le dossier « fournisseurs » avec ses coordonnés;

ii. Communiquer avec cette personne par téléphone et confirmer verbalement la demande de changement de coordonnés bancaires;

iii. Exiger une lettre signée par le contrôleur ou le vice-président Finances du fournisseur pour confirmer la demande de changement de coordonnés bancaires;

iv. Communiquer avec ce contrôleur ou vice-président Finances du fournisseur par téléphone afin de confirmer verbalement la demande de changement de coordonnés bancaires;

v. Utiliser les coordonnés téléphoniques que vous avez au dossier pour votre véritable fournisseur et non pas celles apparaissant sur l'adresse courriel du fraudeur;

vi. Garder à jour vos listes de fournisseurs et de personnes contacts chez vos fournisseurs ainsi que leurs coordonnés;

vii. Vérifier l'adresse courriel provenant de toute demande de changement de coordonnés bancaires pour vous assurer qu'elle correspond à celle de votre véritable fournisseur mais ceci n'est parfois qu'un indice de fraude et ne garantit pas l'absence de fraude lorsque le fraudeur a « hacké » l'ordinateur de votre véritable fournisseur;

viii. Limiter autant que possible la divulgation sur des sites publics d'informations permettant à des tiers de connaitre les contrats que vous octroyez ainsi que le nom de vos fournisseurs.

4. FRAUDE PAR INTERCEPTION DE CHÈQUE

4.1. Description

Il s’agit d’une fraude assez fréquente par laquelle un employé de l’entreprise obtient possession des chèques payables à des fournisseurs de l’entreprise en prétextant différentes raisons pour les obtenir et les dépose par la suite à son propre compte bancaire.

4.2. Caractéristiques

Les caractéristiques de cette fraude sont les suivantes :

i. L’employé de l’entreprise demande que le chèque payable à un fournisseur lui soit remis directement prétextant qu’il veut remettre lui-même le chèque au fournisseur pour une variété de raisons;

ii. Le chèque est déposé par guichet automatique au compte de l’employé ou d’une raison sociale semblable à celle du véritable fournisseur plutôt qu’être remis au fournisseur;

iii. L’employé a généralement un lien avec les fournisseurs, soit qu’il s’agit de ses clients au sein de l’entreprise ou c’est lui qui a retenu les services du fournisseur, ainsi de suite.

4.3. Exemples réels

a) Le dossier d'une entreprise agroalimentaire

Un vice-président Approvisionnement qui était en relation étroite avec les éleveurs et fournisseurs de porc et de volaille demandait que les chèques de « loyauté » ou ristourne remis aux fournisseurs lui soient remis parce qu'il désirait leur remettre directement et s'assurer de l'approvisionnement en volaille pour l'entreprise.

Pendant plusieurs années, la fraude est passée inaperçue puisque ces paiements n'étaient pas pour l'achat proprement dit de produits des éleveurs mais plutôt une forme de paiements effectués par l'entreprise agroalimentaire pour s'assurer de la loyauté des fournisseurs et donc, il n'y avait pas de véritables montants dus aux fournisseurs, ce qui a permis au vice-président Approvisionnement de détourner les chèques sans qu'il n'y ait de plaintes des éleveurs/fournisseurs.

Le vice-président Approvisionnement apposait de faux endossements sur les chèques et les déposait à son compte bancaire pendant plusieurs mois, voire années, jusqu'à ce que la fraude soit découverte à l'interne chez le producteur et représentait plusieurs centaines de milliers de dollars.

b) Le directeur de l'informatique d'un syndicat

Un autre exemple est celui d'un directeur de l'informatique d'un syndicat d'employés qui transigeait directement avec certains fournisseurs de services informatiques. Il recevait directement les factures des fournisseurs en informatique.

Il a commis une fraude en modifiant le montant des factures qu'il recevait directement des fournisseurs pour les augmenter et exigeait du département de comptabilité que les chèques lui soient remis directement en prétextant qu'il les remettrait directement au fournisseurs.

Il a reçu plus de 27 chèques qui étaient généralement pour des montants supérieurs aux montants réels des factures qu'il avait trafiquées à la hausse. Il encaissait les chèques faits au nom du fournisseur dans son compte bancaire et transmettait au fournisseur une traite bancaire pour le paiement du montant réel de la facture. Pour le montant excédentaire, il le conservait dans son compte et a pu empocher une somme de l'ordre de 125 000 $ avec ce stratagème frauduleux jusqu'à ce que la fraude soit découverte.

Le fait qu'il payait les véritables fournisseurs par traites bancaires a permis de continuer la fraude pendant plusieurs mois car les fournisseurs ne se plaignaient pas qu'ils n'étaient pas payés.

c) L’adjointe au vice-président

Dans un dossier, une adjointe au vice-président préparait des demandes de paiement pour des fausses factures de fournisseurs relatives à des événements corporatifs auxquels elle prétendait que des employés de l’entreprise avaient participé (ex. participation à une conférence organisée par la Chambre de commerce de Montréal).

Elle transmettait de fausses factures de fournisseurs qu’elle faisait approuver par son patron et les chèques qui étaient émis par l’entreprise à Vancouver lui étaient acheminés directement à Montréal pour qu’elle les achemine elle-même aux faux fournisseurs qui, en fait, était le compte qu’elle avait ouvert sous une raison sociale dans laquelle elle déposait les chèques.

Comme les employés de l’entreprise ne participaient pas réellement aux événements corporatifs, il n’y avait pas réellement de sommes dues à quiconque pour la participation aux événements et donc, il n’y avait pas de véritables fournisseurs qui pouvaient se plaindre de ne pas avoir été payés par l’entreprise.

4.4. Question: Qu'auriez-vous fait pour prévenir ces fraudes?

Discussion.

4.5. Mesures de prévention

i. Toute entreprise doit adopter des mesures de contrôle visant à prévenir la fraude. Dans ce cas, l'une de ces mesures préventives aurait dû être de ne jamais remettre les chèques payables à des fournisseurs à des employés de l'entreprise;

ii. Deux (2) signatures sont requises pour approuver une réquisition de chèque;

iii. Toute demande pour qu'un chèque soit transmis à un employé doit être faite par le contrôleur de l'unité, par courriel, en détaillant les raisons de la demande et, par la suite, une personne en autorité doit approuver cette demande;

iv. L'endos de tous les chèques doit être vérifié par la personne qui fait la conciliation bancaire et en cas de double endossement, le commis-comptable doit rapporter la situation à son superviseur pour que des vérifications additionnelles soient effectuées;

v. Dès qu'un chèque est signé, il doit être posté directement au fournisseur;

vi. Éviter de payer par chèque et payer par virement bancaire;

vii. Une confirmation de paiement est envoyée aux fournisseurs par courriel ou télécopie;

viii. Mettre en place des cloisons et adopter le principe de la séparation des tâches au sein du département de comptabilité pour que la personne autorisée à ouvrir un nouveau compte fournisseur ne soit jamais la même qui est autorisée à effectuer les paiements à ce compte fournisseur;

ix. Exiger que les factures des fournisseurs soient transmises directement au département de comptabilité.

II. LES MESURES URGENTES À PRENDRE UNE FOIS LA FRAUDE DÉCOUVERTE

Quelles-sont les mesures urgentes à prendre une fois que vous découvrez que votre entreprise a fait l'objet d'une fraude bancaire?

Discussion.

1. **Time is of the essence**

Il est essentiel d'agir rapidement pour récupérer les fonds.

2. **Communiquer immédiatement avec votre banque**

Il faut communiquer immédiatement avec votre banque et demander d'être transféré au département de sécurité de la banque pour qu'un enquêteur puisse immédiatement entreprendre des démarches pour tenter de localiser les fonds.

Entente BCPIF (Bank Crime Prevention and Investigation Framework) :

Échange d'information entre les banques en conformité avec 7 (3) (d.1) et 7 (3) (d.2) de PIPEDA (The Personal Information Protection and Electronic Documents Act et lois provinciales similaires). Les enquêteurs des banques sont très efficaces pour localiser les fonds avant même que des procédures judiciaires puissent être intentées.

Gel administratif des fonds :

Il arrive fréquemment que les banques vont accepter de geler administrativement les fonds pour donner suffisamment de temps à l'entreprise d'aller chercher une saisie avant jugement ou une ordonnance de la cour pour geler officiellement les fonds qui se trouvent dans un compte bancaire face à des allégations de fraude.

3. Communiquer avec vos conseillers juridiques externes

Il est important de communiquer immédiatement avec vos conseillers juridiques externes qui ont une expertise dans le domaine de la fraude pour que ceux-ci puisse entreprendre les procédures judiciaires nécessaires afin de récupérer les fonds.

4. Aviser vos assureurs

Il est possible que vous ayez une couverture d'assurance contre la fraude et donc aviser vos assureurs de la fraude dès que possible après la découverte de la fraude.

III. LES RECOURS POSSIBLES

1. La saisie avant jugement
2. L'injonction de type Norwich
3. L'injonction de type Anton Piller
4. L'injonction de type Mareva

Exemple :

Dans le recours de l'université d'Alberta, les procédures judiciaires canadiennes et internationales (à Hong Kong) ont permis de récupérer environ 11 millions $ sur 11,8 millions $ alors que la fraude avait été effectuée dix jours avant sa découverte.

QUESTIONS?

GOWLING WLG


GOWLING WLG