Assurance responsabilité professionnelle Barreau

Maîtres@droits

Service de prévention

Guylaine LeBrun, avocate
Coordonnateur aux activités de prévention

Judith Guérin, avocate
aux activités de prévention

1er juin 2020

Fraude, blanchiment d'argent et cybercriminalité : Demeurez vigilant

Récemment, nous avons publié des articles portant sur les mesures préventives contribuant à limiter les risques d'être victime de cybercriminalité ou de fraude[1]. Dans cette ligne de pensée, nous avons cru opportun de traiter de divers stratagèmes utilisés par les criminels en lien avec la COVID-19 afin de tromper les avocats ou leurs clients. Par ailleurs, nous discuterons des signaux d'alarme qui facilitent la détection d'une fraude, d'une tentative de blanchiment d'argent ou d'un cybercrime. Pour conclure, nous aborderons quelques mesures préventives en lien avec ces types de crimes.

Quelques stratagèmes utilisés par les criminels

La période d'incertitude engendrée par la pandémie a intensifié les opportunités de certains individus dotés d'intentions malveillantes. Le Groupe d'action financière[2] (ci-après « GAFI ») ainsi que le Centre canadien pour la cybersécurité[3] (ci-après « CCC ») ont publié des rapports ou articles faisant état de stratagèmes utilisés par les criminels pour arnaquer les contribuables en lien avec la pandémie. Nous avons décidé de traiter de ceux susceptibles de se manifester dans la profession juridique.

Tout d'abord, les deux organisations attirent notre attention sur les tentatives d'hameçonnage qui sont en hausse que ce soit par messages textes ou par courriels. Selon le CCC, l' « hameçonnage consiste à envoyer des courriels de masse qui semblent provenir d'une source légitime, mais qui contiennent une pièce jointe infectée ou un lien malveillant »[4]. L'un des objectifs poursuivis est de s'emparer d'informations personnelles telles que le nom d'utilisateur, les mots de passe et les contacts. Par la suite, il n'est pas impossible que l'information collectée serve à duper collègues et partenaires d'affaires. À titre d'exemple, le GAFI rapporte une situation où les fraudeurs ont réussi à s'introduire dans le réseau d'une entreprise et à obtenir des informations sur un contact et ses transactions. Ensuite, les criminels ont usurpé l'identité du contact afin d'exiger un paiement en lien avec l'une des transactions. Ils ont également requis

---

[1] Voir entre autres : *La cybercriminalité : L'affaire de tous!*, Bulletin Praeventio, décembre 2019; *Prévenir les fraudes et les cyberrisques à l'ère du COVID-19*, Blogue *Maîtres@droits*, 20 mars 2020.
[2] Groupe d'action financière, *COVID-19-related Money Laundering and Terrorist Financing: Risks and Policy Responses*, mai 2020. Repéré à : http://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf
[3] Centre canadien pour la cybersécurité, *Pratiques exemplaires en cybersécurité pour la COVID-19,* 13 mars 2020. Repéré à : https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-cybersecurite-pour-la-covid-19; Centre canadien pour la cybersécurité, *Assurer sa sécurité en ligne pendant la pandémie de la COVID-19,* 13 mai 2020. Repéré à : https://www.cyber.gc.ca/fr/orientation/assurer-sa-securite-en-ligne-pendant-la-pandemie-de-la-covid-19; Centre canadien pour la cybersécurité, *La cybersécurité en mode télétravail*, 7 avril 2020. Repéré à : https://cyber.gc.ca/fr/la-cybersecurite-en-mode-teletravail; Centre canadien pour la cybersécurité, *La COVID-19 et les sites web malveillants*, 20 mai 2020. Repéré à : https://cyber.gc.ca/fr/orientation/la-covid-19-et-les-sites-web-malveillants-itsap00103
[4] Centre canadien pour la cybersécurité, *Pratiques exemplaires en cybersécurité pour la COVID-19, préc.,* note 3.

que le paiement soit déposé dans un compte en banque qui s'est avéré ne pas être celui du contact dont l'identité a été volée. Aussi, vu la quantité d'informations détenues par les avocats, les risques liés à l'hameçonnage sont bien réels.

En lien avec ce qui précède, le GAFI et le CCC révèlent une augmentation de l'usurpation du vol d'identité de fonctionnaires ou d'organisations gouvernementales ou médicales. En raison de la pandémie, les deux paliers de gouvernement offrent des subventions et aides financières de toute sorte. Il a été constaté que certains fraudeurs ont transmis des courriels en se faisant passer pour un fonctionnaire du gouvernement. Ils ont requis des informations personnelles, notamment des informations bancaires afin que, soi-disant, l'aide financière soit déposée dans le compte en banque de la victime. Aussi, de faux sites Internet d'établissements de santé ou d'organismes gouvernementaux sont progressivement apparus. Une fois sur ces sites, les victimes ont dû fournir des informations personnelles pour finaliser leur demande d'aide financière ou obtenir leur matériel médical. À cela s'ajoutent de faux sites de transactions financières. En effet, les criminels profitent de nos changements d'habitude de consommation et du fait que certaines institutions financières ont réduit ou modifié leurs offres de services pour tromper les justiciables. Ainsi, dans la mesure où vous ou certains de vos clients avez requis une aide financière, il n'est pas futile d'être sensibilisé à ce type d'arnaque. Les transactions en ligne méritent aussi une attention particulière.

Le GAFI souligne également l'existence d'attaques de type rançongiciel. Dans un tel cas de figure, les criminels utilisent différentes méthodes, dont des sites Internet malveillants et des applications mobiles, pour s'insérer dans les appareils technologiques de leurs victimes, les verrouiller ou les infecter puis demander une somme d'argent en échange de l'accès à l'appareil technologique.

Enfin, vu le ralentissement économique, le GAFI affirme qu'il n'est pas impossible que certains criminels cherchent à investir dans l'immobilier ou dans des entreprises en difficulté afin de faciliter le blanchiment d'argent. Aussi, nous pouvons penser à la création de structures corporatives facilitant ces investissements. Également, les procédures de faillite peuvent entraîner la libération de fonds initialement illicites. En terminant, il est plausible que certains contribuables ou compagnies tentent d'alléger leurs charges fiscales en raison de la situation économique actuelle, et ce, par des moyens douteux. Les avocats en droit des affaires et en droit fiscal doivent donc être particulièrement vigilants.

Quelques signaux d'alarme

En 2013, le GAFI publiait un rapport intitulé *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*. Non seulement ce document rapporte plusieurs situations de blanchiment d'argent et de fraude auxquelles ont été confrontés les avocats, mais il révèle de nombreux signes précurseurs de transactions illicites. Dans le contexte actuel, nous avons cru opportun d'aborder certains d'entre eux.

Signaux concernant le client ou les parties à une transaction :

- Le client sollicite vos services par courriel ou téléphone;
- L'objet du courriel indique uniquement « avocat » ou « conseiller juridique »;
- Les raisons amenant le client à vous confier le mandat sont nébuleuses ou inusitées. À titre d'exemples, la personne n'est pas recommandée par un autre de vos clients ou elle a trouvé votre nom sur Internet;

- Le client évite sans raison apparente les rencontres en personne et il insiste pour l'utilisation du courriel;

- Le client est réticent à vous fournir des pièces prouvant son identité et celles des parties impliquées dans la transaction ou s'il en fournit, elles sont fausses;

- Il néglige de fournir l'information usuelle vous permettant d'effectuer le mandat;

- Le client est reconnu pour être impliqué dans des affaires illicites ou pour fréquenter des personnes impliquées dans ce type d'affaires;

- Le client est anxieux ou pressé de clore l'affaire;

- Le débiteur acquiesce avec empressement au paiement de la dette;

- Des personnes ou des entreprises sont impliquées sans raison apparente dans une transaction;

- Votre interlocuteur tente de vous dissimuler le véritable client ou le véritable bénéficiaire de vos services juridiques (ex : prête-nom);

- Vous éprouvez des difficultés à trouver de l'information sur les entreprises impliquées dans la transaction. À titre d'exemple, l'entreprise n'a pas de site Internet;

- Le soi-disant client utilise une adresse personnelle alors qu'il affirme agir à titre de représentant de l'entreprise impliquée dans la transaction. Également, l'utilisation de messageries telle que Hotmail, Gmail, Yahoo comme adresse courriel de la compagnie devrait attirer votre attention;

- Le client est disposé à payer vos honoraires sans aucune question;

- Le client a changé régulièrement d'avocats dans une courte période de temps, et ce, sans raison apparente;

- D'autres avocats ont refusé le mandat ou ont terminé abruptement ce dernier. Les explications fournies par le client quant à la fin de la relation professionnelle sont vagues. En outre, il refuse que vous communiquiez avec votre prédécesseur dans le dossier.

<u>Signaux concernant la nature du mandat</u> :

- Votre mandat consiste à élaborer une structure corporative inutilement complexe et sans raison économique apparente;

- Dans le cadre d'une transaction, le client vous demande de décaisser des fonds en faveur d'entreprises qui ne semblent pas avoir de liens entre elles ou avec lui et sont situées dans plusieurs pays;

- La présence de plusieurs transactions entre personnes ou compagnies liées, et ce, dans une courte période de temps et sans raison apparente. Parfois, le prix payé ne reflète pas celui du marché ou encore, il y a augmentation de la valeur du bien ou de l'entreprise de manière inexplicable;

- La transaction est abandonnée à la dernière minute et vos instructions sont de remettre les sommes détenues dans votre compte en fidéicommis à une personne ou entreprise n'ayant aucun lien avec la transaction;

- Les instructions changent à la dernière minute, notamment les instructions de paiement.

Signaux concernant la provenance des fonds :

- La transaction implique d'importantes sommes en argent comptant ou de faux effets de commerce;

- Le client utilise des fonds provenant de multiples comptes en banque;

- Le paiement reçu est différent de l'entente convenue ou ce n'est pas une traite bancaire ni un chèque certifié;

- Dans le cas de l'utilisation d'effet bancaire ou tout document l'accompagnant, vous constatez la présence d'erreurs d'écriture. À titre d'exemple, le nom du bénéficiaire est mal orthographié.

Mesures préventives

Une fois sensibilisé aux différents signaux d'alarme indiquant la présence d'une fraude, d'un cybercrime ou d'une tentative de blanchiment d'argent, une question demeure : comment diminuer les risques d'en être victime ou d'être impliqué? À cet égard, voici quelques mesures préventives :

Dans le cadre d'un mandat :

- Posez des questions au futur client sur les raisons justifiant l'octroi du mandat. Obtenez des clarifications si la situation vous paraît inusitée;

- Effectuez des démarches pour valider l'identité de votre futur client et de toute personne impliquée dans le mandat;

- Méfiez-vous si le client est anxieux ou utilise un ton urgent;

- Assurez-vous que l'effet de commerce que vous recevez émane d'une institution financière canadienne;

- Obtenez confirmation de l'institution financière qu'elle a vérifié la validité de l'effet de commerce, et non seulement que les fonds sont disponibles, puis confirmez par écrit cette information à l'institution avant de débourser les sommes;

Dans le cadre de l'utilisation des technologies de l'information (prévenir le cybercrime)[5] :

- Utilisez des mots de passe sécuritaires. À titre d'exemple, le CCC suggère d'utiliser une phrase unique et complexe;

[5] Plusieurs des suggestions de cette section proviennent du Centre Canadien pour la cybersécurité, notamment leur article intitulé *Pratiques exemplaires en cybersécurité pour la COVID-19*. Repéré à : https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-cybersecurite-pour-la-covid-19

- Considérant que plusieurs d'entre nous sont en télétravail, assurez-vous que l'accès à votre réseau soit sécurisé, notamment, faites l'usage d'une clé VPN (réseau privé virtuel);

- Pour ce qui est des courriels malveillants, utilisez des logiciels antivirus ou anti-maliciel. Également, vérifiez l'identité de l'expéditeur du courriel : Est-ce quelqu'un que vous connaissez? Est-ce qu'il y a des erreurs dans son adresse courriel?

- En ce qui concerne les pièces jointes malveillantes, le CCC conseille de vérifier que « l'adresse courriel de l'expéditeur comprend un nom d'utilisateur et un nom de domaine valides »[6]. En cas de doute, n'ouvrez pas la pièce jointe et confirmez auprès de l'expéditeur, verbalement, que cette pièce émane de lui;

- Concernant les sites Internet malveillants, assurez-vous que l'URL est correctement orthographiée. De même, il est recommandé de taper l'URL dans une fenêtre distincte au lieu de cliquer sur le lien[7]. Enfin, le CCC mentionne que « Si vous devez cliquer sur un hyperlien, pointez votre curseur sur le lien pour vérifier qu'il vous dirigera bel et bien vers le site Web indiqué »[8];

- Souscrivez à une police couvrant les cyberrisques.

En terminant, l'objectif poursuivi par ce texte était de sensibiliser les avocats aux stratagèmes frauduleux utilisés par les criminels notamment en temps de pandémie. Bien qu'il soit impossible d'éradiquer toute menace de cybercriminalité ou de fraude, il n'en demeure pas moins qu'en demeurant vigilants, nous pouvons diminuer les risques d'être victime de ce type de crime ou d'être impliqué. Ici, l'expression « Prudence est mère de sûreté » prend tout son sens!

[6] *Id.*
[7] *Id.*
[8] *Id.*