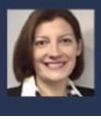
Février 2024

Judith Guérin
Avocate aux activités de prévention
judith.guerin@farpbq.ca



Aurélie Lompré, LL.M.
Avocate aux activités de prévention
aurelie.lompre@farpbq.ca

Transfert de fonds frauduleux : Êtes-vous couvert?

Ce matin, vous découvrez un étrange courriel de votre client Jay Lafortune dans votre boîte de messagerie.

Jay Lafortune est un auteur de romans policiers à succès, que vous avez représenté dans un litige l'opposant à Ella Plagiet, qui a repris des passages du dernier roman de Jay Lafortune dans son film d'action.

Le litige est maintenant réglé et Ella Plagiet doit verser la somme de 150 000 $ en dommages à Jay Lafortune.

Partant en expédition au pôle Sud pour son prochain roman, Jay Lafortune vous a transmis ses coordonnées bancaires pour lui transférer cette somme quand vous l'aurez reçu dans le compte en fidéicommis.

Ce matin, un courriel signé de Jay Lafortune demande plutôt de transférer cette somme de 150 000 $ sur un compte bancaire à l'étranger, car il prévoit prolonger de plusieurs semaines son expédition.

Que faire? Avant tout transfert de fonds, il est primordial de valider de vive voix avec le client les instructions relatives au virement bancaire.

Sans prétendre à l'exhaustivité, voici quelques suggestions :

- ❑ Ne répondez pas au courriel modifiant les instructions de transfert, car le compte de messagerie courriel peut être compromis! Vérifiez les instructions en contactant votre client par un autre moyen de communication. Par exemple, appelez le client en utilisant son numéro de téléphone inscrit dans le dossier et non celui figurant dans le courriel suspect.

- ❑ Examinez l'adresse courriel du message. Il peut s'agir d'une fausse adresse courriel qui imite la véritable adresse du client. Par exemple la lettre « l » (L minuscule) et « I » (i majuscule) peuvent sembler identiques selon la police d'écriture utilisée.

- ❑ Si l'adresse courriel du message reçu est une contrefaçon de celle utilisée par votre client, informez immédiatement ce dernier ainsi que tous les membres de votre cabinet de l'existence de cette fausse adresse courriel.

- ❑ Souscrivez à une assurance Cyberrisque et à toutes autres assurances appropriées à cet effet. À titre informatif, voir le site Web de la Corporation de services du Barreau du Québec sur ce sujet. Également, nous vous invitons à visionner une courte capsule vidéo du blogue *Maîtres@droits!* du Fonds d'assurance *Cybercriminalité : L'importance de souscrire une assurance cyberrisques et d'adopter des mesures préventives*.

Que faire si le virement frauduleux a été initié?

- ❑ Contactez sans délai la banque émettrice du virement bancaire pour demander qu'il soit interrompu, si cela est possible. Demandez également à cette dernière qu'elle contacte la banque devant réceptionner les fonds, le cas échéant.

- ❑ Avisez votre client, le plus rapidement possible, de cette fraude afin qu'il examine si son système informatique, messagerie, etc. est compromis, ainsi il pourra mettre en place des mesures.

- ❑ Prévenez les autorités policières et le Centre antifraude du Canada.

- ❑ Communiquez avec votre équipe TI pour déterminer si votre système informatique a été piraté et comment y parer.

- ❑ Avisez vos assureurs cyberrisques. Nous vous rappelons que la police d'assurance responsabilité professionnelle du Barreau du Québec n'offre aucune couverture dans une telle situation.

Que faire par la suite? À moins que cela ne soit déjà fait :

- ❑ Mettez en place des protocoles et systèmes informatiques pour bloquer les tentatives de fraudes électroniques et maintenez-les à jour.

- ❑ Protégez votre boîte de messagerie, votre ordinateur, etc. en utilisant un système d'authentification à deux facteurs.

- ❑ Suivez des formations en Cybersécurité. Il est primordial que les avocats et les employés du bureau suivent régulièrement ces formations pour demeurer vigilants.

- ❑ Mettez en place un politique au bureau concernant les transferts de fonds électroniques et avisez vos clients de celle-ci.

La vigilance est de mise puisque les avocats sont une cible de choix pour les fraudeurs considérant l'importance des sommes détenues dans les comptes en fidéicommis. De plus, avec le développement de l'intelligence artificielle, de nouveaux types de piratage des systèmes technologiques pourraient émerger prochainement.

Références :

"You transferred funds to the wrong account – what now?", LAWPRO Lawyers' Professional Indemnity Company, 1er juin 2022, https://www.practicepro.ca/2022/06/you-transferred-funds-to-the-wrong-account-what-now/

"Wire Fraud Fraud Watch", LAWPRO Lawyers' Professional Indemnity Company, 2023, https://www.practicepro.ca/wp-content/uploads/2023/06/Wire-Fraudwatch-Factsheet-June-2023-AODA.pdf

Melanie Hodges Neufeld, "Fraud Detection in a World of Deepfakes", Slaw Canada's online legal magazine, 29 août 2023, https://www.slaw.ca/2023/08/29/fraud-detection-in-a-world-of-deepfakes/

Centre antifraude du Canada, https://www.antifraudcentre-centreantifraude.ca/index-fra.htm