Assurance
responsabilité
professionnelle
Barreau

PRÆVENTIO

Juillet 2015 | Volume 16 | nº 3

© « Brise d'été », Claude Théberge

Où que vous alliez, quelle que soit la température, apportez toujours votre propre soleil. Tout est dans l'attitude.

Anthony J. D'Angelo

SOLLICITATION DE SERVICES PAR COURRIER ÉLECTRONIQUE – UN RAPPEL À LA PRUDENCE

Le Fonds d'assurance rappelle à ses assurés d'être prudents à l'approche des vacances face à la sollicitation suspecte par courrier électronique de fraudeurs opérant à distance et souhaitant retenir vos services afin de finaliser une affaire découlant de perception de comptes, conventions de divorce ou transactions. On vous sollicite pour disposer de sommes en fidéicommis suite au dépôt de chèques, traites bancaires ou transferts électroniques falsifiés.

Nous vous rappelons que la protection offerte par la police du Fonds ne s'applique pas à ces situations. Le permis d'assureur du Barreau est restreint à l'assurance responsabilité et ne couvre pas les délits dont peuvent être victimes les avocats.

Signes précurseurs

Voici quelques signes précurseurs qui vous aideront à être vigilants :

- L'utilisation du mot « avocat » ou « conseiller juridique » dans la ligne objet ou dans le corps du message;
- La personne vous contacte en utilisant un compte courriel personnel pour représenter sa société ou son entreprise, **sans utiliser l'adresse de messagerie de l'entreprise**. Cette personne peut même utiliser des noms réels de personnes et d'entreprises trouvés sur des sites Web;
- Le client réside à l'extérieur du Canada et **insiste sur le moyen de communication du courriel** en raison des différences de fuseau horaire;
- Le client, sans hésitation aucune, est disposé à payer votre taux horaire ou tarif forfaitaire;
- Le débiteur semble trop anxieux et empressé d'acquitter sa dette;
- La mise de fonds provient d'une tierce personne (même pas du débiteur);
- Par virement, par la poste ou par messager, le soi-disant chèque ou la traite bancaire arrive d'une adresse insensée, dont l'enveloppe est adressée manuellement ou même, sans lettre d'accompagnement;
- Le paiement reçu est différent de l'entente convenue ou ce n'est pas une traite bancaire ni un chèque certifié – attention, même les chèques certifiés et les traites bancaires peuvent s'avérer être des faux;
- L'effet bancaire ou tout document l'accompagnant contient souvent des erreurs d'écriture (par exemple : des noms mal orthographiés);
- Le client insiste pour savoir si l'effet bancaire a été déposé dans votre compte en fidéicommis;
- Le client réclame que les fonds soient déboursés rapidement **une fois que vous avez reçu et déposé le chèque** ou la traite bancaire **(sans provision) dans votre compte en fidéicommis**.

SOMMAIRE

suite à la page 2

Mesures préventives

Afin de réduire les risques d'être victime de ce type de fraude, nous vous suggérons ce qui suit :

- Vérifiez auprès de sources externes l'identité de votre nouveau client et la validité des pièces d'identité soumises;
- Assurez-vous que l'effet de commerce (chèque, traite ou autres) que vous recevez émane d'une institution financière canadienne;
- Examinez et déposez vous-même l'effet de commerce ou faites procéder au dépôt par l'un de vos associés ou de vos employés;
- Attendez **au moins** 8 jours **ouvrables** suivant le dépôt de l'effet de commerce dans votre compte en fidéicommis avant de débourser les sommes;
- Obtenez confirmation de l'institution financière qu'elle a vérifié **la validité de l'effet de commerce**, et non seulement que les sommes sont disponibles, puis confirmez par écrit cette information à l'institution;
- Envisagez la possibilité d'exiger de recevoir les transferts électroniques irrévocables des sommes par le biais du *Système de transfert de paiements de grande valeur* (STPGV);
- Révisez régulièrement votre portefeuille d'assurances multirisques d'entreprise avec votre courtier d'assurance.

Vous vous demandez si l'affaire est légitime ou vous n'êtes pas à l'aise dans le traitement d'un dossier, mieux vaut renoncer au mandat!

OÙ SE CACHENT RÉELLEMENT LES CYBERCRIMINELS?

Par *Me Andrew Penhale*
Directeur du Service des sinistres

De nos jours, de plus en plus d'avocats s'appuient sur les technologies de l'information pour gérer leurs activités quotidiennes de même que les infrastructures de leur cabinet. Toutefois, bien que les technologies de l'information puissent grandement améliorer votre efficacité et faciliter votre travail, il n'en demeure pas moins qu'elles vous exposent également aux risques liés à la cybercriminalité, quels qu'ils soient. D'ailleurs, plusieurs études effectuées au Canada et aux États-Unis démontrent que la cybercriminalité compte maintenant parmi les plus grandes menaces pour les entreprises.

En 2014, il y aurait eu plus de sept millions de victimes de la cybercriminalité au Canada. Il ne se passe plus une semaine sans que les médias ne traitent d'une nouvelle histoire abracadabrante de piratage. Par ailleurs, et bien que nous n'entendions pas régulièrement parler de cabinets d'avocats qui auraient été victimes de piratage, il n'en demeure pas moins que plusieurs cyberattaques visant un ou des cabinets d'avocats comptent parmi les dix plus importants cas de cyberattaques de l'histoire du Canada.

Les avocats sont et demeureront des cibles de choix pour les cybercriminels pour plusieurs raisons, dont trois, en particulier :

- Les avocats détiennent des informations confidentielles de grande valeur;
- Les avocats détiennent des sommes d'argent considérables en fidéicommis;
- Les avocats sont reconnus pour la faiblesse de leurs systèmes de sécurité informatique.

Cela dit, plusieurs croient à tort que les menaces proviennent principalement de l'extérieur du cabinet. Pourtant, les statistiques démontrent que plus de 65 % des incidents impliquant la destruction ou la perte de données découleraient plutôt des agissements d'un employé de l'entreprise et tous s'entendent pour dire que les menaces internes continueront à figurer parmi les principaux facteurs de risques de pertes de données tant du fait d'erreurs que d'actions malveillantes d'employés de votre entreprise.

Pensons à l'employé en colère suivant son congédiement ou encore à l'employé qui quitte pour se joindre à un compétiteur et qui utilise ou partage délibérément des informations confidentielles par vengeance personnelle ou afin d'en tirer un avantage pécuniaire. Après tout, peu de gens en connaissent autant sur les systèmes informatiques de votre entreprise que vos employés; et peu de gens sont dans une meilleure position pour causer des dommages importants.

Toutefois, les menaces internes ne sont pas toutes volontaires, mais sont plutôt induites par la maladresse des utilisateurs ou par leur méconnaissance des outils qu'ils utilisent. Il se pourrait qu'un employé, sans le savoir ou sans le vouloir, facilite l'accès à votre système informatique à des pirates. Par exemple, vos employés peuvent être amenés, à l'aide de méthodes d'ingénierie sociale, à ouvrir des courriels malveillants ou à visiter des sites Web compromis. Il peut également s'agir d'un employé qui efface involontairement les données emmagasinées sur votre système informatique ou encore, un employé qui perd son ordinateur portable.

Cela dit, si les erreurs humaines ou la malveillance d'un employé sont à l'origine de plus de 65 % des incidents, les agressions externes ne sauraient être sous-estimées. Bien que moins fréquentes, les menaces externes sont malgré tout redoutables du fait de la diversité des acteurs impliqués et de leur évolution constante.

Les logiciels malveillants (maliciels) sont parmi les moyens les plus fréquemment utilisés par les cybercriminels pour infiltrer les ordinateurs et les systèmes informatiques d'une entreprise.

L'intention malveillante derrière de tels logiciels implique généralement l'accès non autorisé à des ordinateurs ou des réseaux informatiques avec comme objectif de voler de l'argent, des mots de passe ou des informations confidentielles et sensibles ou encore, de perturber votre réseau informatique ou détruire des données.

Les logiciels malveillants peuvent affecter autant les ordinateurs des avocats que votre réseau informatique ou même, le fonctionnement de l'Internet.

Le profil des cybercriminels a évolué au cours des dernières années. Ceux-ci exploitent toutes les avancées technologiques. Leurs techniques et leurs méthodes sont de plus en plus sophistiquées et difficiles à contrer. Les avocats devront ainsi faire face à de nouveaux types d'attaques et il nous sera donc essentiel de bien cerner les risques internes et externes auxquels nous sommes exposés pour bien nous protéger contre les cybercriminels.

À défaut d'échapper au phénomène grandissant de la cybercriminalité, il demeure essentiel de vous assurer que vous détenez une protection d'assurance adéquate contre la cybercriminalité. Cela dit, aucune forme de protection d'assurance ne doit être considérée comme une réponse adéquate à la cybercriminalité. En effet, bien qu'une garantie d'assurance puisse représenter un certain réconfort, vous commettriez une grosse erreur en demeurant complaisant face à la cybercriminalité. Après tout, les organisations qui apporteront le plus d'importance à l'intégrité de leurs systèmes informatiques et qui mettront en place des systèmes de sécurité complets et bien communiqués seront moins susceptibles d'être la prochaine victime des cybercriminels.

QUELLE PROTECTION AVEZ-VOUS PENDANT VOS VACANCES?

Vous pensez sûrement à la meilleure protection solaire qui protège des UVA, des UVB, efficace, pas trop chère, contre le cancer de la peau et résistante à l'eau? Nombreuses elles sont sur le marché et malgré que plusieurs s'en sortent bien, une condition demeure : c'est que vous en mettiez suffisamment!

De la même façon, vous devez suffisamment vous protéger professionnellement afin de prendre cette pause estivale bien méritée. Le meilleur moyen, c'est de bien planifier votre absence. Comment? Voici un bref rappel des mesures à prendre pour vous assurer un retour au travail en toute quiétude :

- Assurez-vous **qu'aucun rendez-vous n'a été fixé** pendant votre absence;
- Enregistrez vos **messages d'absence**, tant dans votre boîte vocale, que dans votre logiciel de messagerie, sans oublier d'indiquer votre date de retour et une personne ressource en cas d'urgence;
- Assurez-vous qu'aucun **délai** ne viendra à échéance pendant votre absence;
- **Informez vos clients** et vos **collègues** de votre absence;
- Si vous pratiquez **seul**, il est important qu'un membre de votre personnel de bureau soit présent pendant votre absence et prenne connaissance de votre courrier et puisse réagir aux urgences, le cas échéant, ou demandez à un collègue de s'occuper de votre bureau;
- Si on vous **consulte** avant votre départ, n'acceptez aucun nouveau mandat si vous n'avez pas le temps de vérifier les diverses échéances possibles. Référez le client à un collègue ou encore, si cela s'avère impossible, refusez le mandat et informez le client par écrit.

Bref, lorsque vous serez au bord de la piscine ou de la mer, vous serez heureux d'avoir planifié votre absence pour mieux vous protéger et vous éviter de mauvaises surprises...

Bonnes vacances!

CAP SUR LE NOUVEAU *CODE DE PROCÉDURE CIVILE*

Le 1er janvier 2016, date prévue pour l'entrée en vigueur du nouveau *Code de procédure civile* (*C.p.c.*), marquera une réforme majeure en matière de procédure civile. Avec 777 articles et une disposition préliminaire, sans compter les dispositions modificatives et finales énoncées dans la loi l'instituant (articles 778 à 836), nous devrons faire face à plusieurs nouveautés importantes. Aussi bien jeter un regard immédiat sur certaines nouveautés, principalement sur la procédure contentieuse (Livre II), afin de se mettre au parfum de ce qui touche les praticiens, confrontés à s'adresser aux tribunaux pour défendre les droits de leurs clients.

Nous aborderons donc ces nouveautés à travers cette rubrique que vous trouverez dans chaque édition du bulletin, sous forme de capsules, certaines plus longues, d'autres se voulant de simples alertes, question de s'adapter aux changements sans trop de difficultés.

Nous traiterons donc de certains articles sur la procédure contentieuse qui regroupe les articles 141 à 301 du nouveau *C.p.c.*, sans exclure quelques autres dispositions que nous jugerons pertinentes d'aborder.

Encore une fois, il s'agira de capsules se voulant un outil d'information et leur contenu ne saurait être interprété comme une étude exhaustive des sujets traités, ni comme avis juridique et encore moins comme suggérant des standards de conduite professionnelle.

Gestion d'instance, collaboration des parties et modes privés de prévention et de règlement des différends

Débutons cette première rubrique en précisant que le nouveau *C.p.c.* est principalement centré sur la gestion d'instance ainsi que sur la collaboration des parties dans la mise en état des dossiers. Les parties doivent considérer avant tout les modes privés de prévention et de règlement des différends (articles 1 à 7), que ce soit la négociation, la médiation, l'arbitrage ou tout autre mode.

Principes directeurs

Le nouveau *C.p.c.* introduit des principes directeurs, entre autres, le principe de la contradiction (article 17), la proportionnalité (article 18) qui s'étend dorénavant aux moyens de preuve, la coopération (les parties se doivent, selon l'article 20, de coopérer notamment en s'informant mutuellement, en tout temps, des faits et des éléments susceptibles de favoriser un débat loyal et en s'assurant de préserver les éléments de preuve qu'elles entendent produire).

Autre principe directeur qui existait avant cette réforme, mais codifié par l'article 22, est que l'expert dont les services ont été retenus par l'une des parties ou qui leur est commun ou qui est commis par le tribunal, a pour mission d'éclairer le tribunal dans sa prise de décision, bien avant les intérêts des parties.

Finalement, les personnes physiques qui agissent pour elles-mêmes devant les tribunaux sans être représentées doivent le faire dans le respect de la procédure établie par le *C.p.c.* et les règlements pris en son application (article 23).

Seuils de compétence

Terminons aujourd'hui avec l'augmentation des seuils de compétence :

Cour d'appel : Le seuil de compétence pour les appels de plein droit est porté à 60 000 $ (articles 29 et 30);

Cour supérieure et Cour du Québec : Le seuil de compétence est porté à 85 000 $, sans égard aux intérêts (Cour du Québec – seuil inférieur à 85 000 $), avec indexations ponctuelles suivant l'indice des prix à la consommation pour le Québec, déterminé par Statistique Canada (article 35).

AVIS

Service de prévention

Me Guylaine LeBrun, Coordonnateur aux activités de prévention
Fonds d'assurance responsabilité professionnelle du Barreau du Québec
445, boulevard Saint-Laurent, bureau 300
Montréal (Québec) H2Y 3T8
Téléphone : 514 954-3452
Télécopieur : 514 954-3454
Courriel : guylaine.lebrun@farpbq.ca
Visitez notre site Internet : www.farpbq.ca

Assurance responsabilité professionnelle Barreau

Une version anglaise est aussi disponible sur demande. / An English version is available upon request.
Tous les bulletins Praeventio antérieurs sont disponibles à l'adresse suivante : www.farpbq.ca/fr/bulletin.html