Resolution
LEGAL PARTNERS

NEWSLETTER – Juillet 2020 – Droit bancaire

Ordres de virements donnés par e-mail : le Tribunal fédéral durcit drastiquement sa jurisprudence pour le client (arrêt 4A_9/2020 du 9 juillet 2020)

I. Faits

En automne 2014, X. a décidé de transférer une partie de ses avoirs à une société de négoce en valeurs mobilières. X. a dès lors signé les documents d'ouverture de compte, une convention de banque restante, ainsi qu'une décharge pour la communication par téléphone, télécopie et e-mail (ci-après « la décharge ») et a accepté les Conditions générales de la banque.

L'art. 5 des Conditions générales de la banque prévoyait que le dommage provenant de l'emploi notamment de la poste, du télégraphe, du téléphone, du fax, du courrier électronique ou de tout autre moyen de transmission, était à la charge du client, sauf en cas de faute grave de la société de négoce.

Depuis le début du mois de décembre 2015, des *hackers* ont pris le contrôle de l'adresse e-mail de X. utilisée pour communiquer avec la société de négoce, ce qui leur a permis de lire les e-mails qui avaient déjà été adressés à la banque précédemment et d'en envoyer de nouveaux. C'est ainsi qu'entre le 1er décembre 2015 et le 4 janvier 2016 (soit environ un mois), ces pirates informatiques ont envoyé huit ordres de virement à la banque pour un montant de EUR 34'000 et GBP 357'000, lesquels ont tous été exécutés et débités du compte de X., à son insu.

Il est précisé qu'entre novembre 2014, date de l'ouverture du compte, et début décembre 2015, X. n'avait donné que deux ordres de virement au moyen de l'adresse e-mail qu'il avait communiquée à la banque.

Par ailleurs, la majorité des virements requis par les escrocs étaient tous à destination d'une banque au Royaume-Uni en faveur de trois sociétés différentes. La banque n'a toutefois pas suspecté une quelconque fraude à ce stade.

Ce n'est qu'en janvier 2016, après avoir reçu des ordres de virement de X. provenant d'une adresse électronique légèrement différente, que la banque a émis certaines suspicions et suspendu tout paiement, priant son client de confirmer sa nouvelle adresse, exigeant une confirmation de l'identité du donneur d'ordre et le priant de prendre contact par téléphone. Après avoir été en contact avec X. quelques jours plus tard, ce dernier a contesté les transferts frauduleux effectués.

Une société d'expertise mandatée par X. n'a détecté aucun *fishing* e-mail sur son ordinateur, ni aucune trace de mauvaise utilisation de celui-ci.

Dans ces circonstances, X. a réclamé à la société de négoce le remboursement des montants indûment débités de son compte, lui reprochant des manquements à son devoir de diligence. Après avoir été débouté de ses prétentions en première instance, l'appel de X. a été entièrement admis par la Chambre civile de la Cour de justice du canton de Genève, qui a condamné la banque à lui rembourser les montants litigieux au motif qu'elle avait commis une faute grave dans l'exécution des ordres.

La société de négoce a dès lors interjeté un recours en matière civile au Tribunal fédéral, concluant au rejet de la demande en paiement de X.

II. Considérations juridiques du Tribunal fédéral

Le Tribunal fédéral a été amené à déterminer si la société de négoce a commis une faute grave dans l'exécution des ordres litigieux, auquel cas elle ne pourrait opposer la clause impliquant le report sur X. du préjudice qu'il subit du fait de cette exécution.

Pour ce faire, le Tribunal fédéral a notamment examiné la validité et les conditions de la clause de transfert de risque (« la décharge ») conclue par les parties.

À cet égard, notre Haute Cour a rappelé, d'une part, que lorsque les parties sont convenues d'habiliter le client à transmettre des ordres par e-mail, la banque n'a pas à prendre des mesures extraordinaires, incompatibles avec une liquidation rapide des opérations. D'autre part, elle n'a pas à systématiquement présumer que le message qui lui est communiqué depuis l'adresse e-mail du client ne provient pas de celui-ci.

Le Tribunal fédéral a surtout ajouté qu'il appartient au client de prendre toutes les mesures de précaution nécessaires pour éviter des interventions illicites de tiers dans son système informatique, la responsabilité du client s'étendant même aux cas fortuits.

Il s'agit à notre sens d'une nouvelle restriction imposée au client. En effet, la jurisprudence retenait jusqu'alors qu'il était notoire que « *de nombreux services gouvernementaux et entreprises privées - dont on peut penser qu'ils avaient pris des précautions raisonnables pour se protéger contre une telle éventualité - ont fait l'objet d'attaques informatiques parfois couronnées de succès de la part de tiers mal intentionnés. [...] Ainsi, la situation d'un client à qui l'on ne peut reprocher d'avoir pris des précautions insuffisantes pour empêcher l'accès à sa messagerie électronique - protégé par un mot de passe - n'est en rien comparable à celle d'un client qui laisse ses documents bancaires librement accessibles dans le bureau de sa maison fréquentée par des visiteurs dont le client n'a pas la maîtrise, et dont il se méfie* » (ATF 4A_386/2016 consid. 4.4.).

Or, à la lecture de ce nouvel arrêt 4A_9/2020, objet de la présente contribution, il semble désormais que le simple fait de protéger sa messagerie à l'aide d'un mot de passe ne soit plus suffisant.

Les Juges fédéraux ont également précisé qu'il ne peut y avoir de faute grave de la banque et, partant, de responsabilité de celle-ci que si l'examen auquel elle procède, nécessairement rapidement pour ce type d'opérations bancaires, fait apparaître des indices sérieux d'une usurpation d'adresse et donc d'identité.

Tel serait le cas s'il devait « *sauter aux yeux* » de toute personne raisonnable que l'ordre transmis, de par son adresse, son texte, son contenu ou un lieu de virement exotique, et compte tenu de la situation du client, ne pourrait émaner de celui-ci.

Là encore, on constate que le Tribunal fédéral serre la vis s'agissant de la preuve de la faute grave de la banque, qui devient de plus en plus difficile à apporter.

Le Tribunal fédéral s'est encore référé à sa jurisprudence citée ci-dessus (4A_386/2016), rendue dans le cadre d'un complexe de faits plus ou moins identique, dans laquelle il avait été retenu que la banque

avait commis une faute grave parce que les ordres de virement avaient été rédigés dans un anglais présentant des erreurs de syntaxe, des fautes d'orthographe et un vocabulaire approximatif alors que le client en question était un avocat de langue anglaise, qui s'était toujours exprimé en bon anglais, avec une syntaxe correcte et une variété de termes adéquats et précis. La qualification de la faute grave avait également été retenue au motif que les ordres de virement effectués par les escrocs étaient en contradiction avec la volonté du client, bien connue de la banque, qui était la conservation à long terme de ses avoirs.

En l'espèce, notre Haute Cour a donc rejeté le recours de X., et ce notamment pour les motifs suivants :

- Les éléments retenus par la Cour cantonale n'ont pas permis de retenir l'existence d'indices sérieux d'abus de la messagerie et donc de fraude, de sorte que la société de négoce n'avait pas à suspecter l'authenticité des ordres de transfert donnés depuis l'adresse e-mail de X.
- Bien que les e-mails aient été échangés dans un anglais approximatif, cela ne permettait pas à la société de négoce de suspecter des faux, dès lors que X. n'était pas de langue maternelle anglaise, qu'il avait déjà fait des fautes dans ses précédents e-mails et que les *hackers* avaient pu consulter les e-mails qui avaient déjà été échangés précédemment et s'en inspirer.
- Le destinataire des ordres de paiement frauduleux était une banque connue du Royaume-Uni, et non de pays lointains ou exotiques.
- La fréquence et les montants élevés des ordres de paiement ne suffisent pas à déduire une faute grave de la société de négoce.
- Considérant que la décharge englobe également les cas fortuits, le dommage est à la charge de X. même s'il n'a commis aucune faute en lien avec la prise de contrôle de sa messagerie par les pirates informatiques.

Au vu de ce qui précède, la signature d'une décharge en cas de transmission par e-mail est clairement défavorable au client compte tenu du durcissement de la jurisprudence en la matière. Si une telle décharge facilite la communication entre la banque et son client, ce dernier doit être rendu attentif au risque de ne pas être dédommagé en cas d'hacking de sa messagerie électronique. Il conviendrait tout au plus d'utiliser les plateformes de messagerie sécurisées de la banque ou de veiller à disposer d'une messagerie cryptée (p. ex. ProtonMail).

Ce mode de communication est d'autant plus risqué si le client ne maîtrise pas parfaitement la langue dans laquelle il échange avec la banque, car il est plus difficile pour celle-ci de distinguer les écrits de son client de ceux de potentiels pirates informatiques.

Pascal de Preux
Associé | Partner
depreux@resolution-lp.ch

Marc-Henri Fragnière
Associé | Partner
fragniere@resolution-lp.ch

Julien Gafner
Associé | Partner
gafner@resolution-lp.ch

Françoise Martin Antipas
Associée | Partner
martinantipas@resolution-lp.ch

Resolution
LEGAL PARTNERS

Av. de l'Avant-Poste 4
CP 5747 | 1002 Lausanne
T. +41 21 312 59 40 | F. +41 21 312 59 41