PPrétention en dommages-intérêts pour un paiement par e-banking déclenché par des inconnus

Sujet: **Abus et escroquerie** Numéro de cas: **2020/14**

> Le présent cas constitue un nouvel exemple d'hameçonnage (phishing). Un dimanche, le client a tenté, en vain, de se connecter au système e-banking de la banque afin de consulter le compte d'épargne de son épouse. A la suite de cette tentative, il a reçu un SMS faisant mention d'un montant de 3000 CHF, qu'il a pris pour le solde du compte. Le lundi matin, le client a pu à nouveau se connecter sans problème au système e-banking, où il a constaté un versement non autorisé de plus de 3000 CHF. Il a alors immédiatement signalé l'incident à la banque. Celle-ci a contacté la banque destinataire afin de réclamer la restitution du montant, mais seulement à 16h30 via SWIFT. Les fonds n'ayant pas pu être bloqués sur le compte destinataire, le client a réclamé à la banque des dommages-intérêts au nom de son épouse. Face à l'impossibilité de s'entendre avec la banque, le client s'est finalement tourné vers l'Ombudsman, mais la banque a continué d'exclure toute concession dans le cadre de la procédure de médiation.

Pour son système e-banking, la banque utilise un processus d'authentification à deux facteurs avec code de vérification (mTAN). Une fois qu'un client a saisi ses données de connexion, ce code lui est envoyé sur le téléphone portable qu'il a préalablement enregistré. Le client doit saisir ce code dans l'e-banking pour confirmer sa connexion. En l'espèce, lorsque le client a saisi ce code pour se connecter un dimanche, l'écran est devenu noir, et un message est apparu pour signaler des travaux de maintenance sur le site e-banking de la banque. Le client a alors interrompu le processus avant d'essayer de se connecter à nouveau, une fois de plus en vain. Au vu des circonstances, il y a lieu de penser que son ordinateur était vraisemblablement infecté, et que le client a saisi les données de connexion sur un site d'hameçonnage, qui ressemblait certes au site internet de la banque mais avait été créé par des escrocs pour leur permettre d'intercepter les données en question. Grâce aux données ainsi volées, les tiers inconnus se sont ensuite connectés à l'e-banking et ont débité le compte de son épouse en faveur du compte qu'une mule financière (money mule) détenait auprès d'une autre banque. La procédure pénale introduite par le client a permis de révéler que la destinataire était une étudiante, elle aussi trompée sur la véritable nature de la transaction, qui a transmis l'argent aux escrocs contre rémunération. L'identité de ceux-ci n'a en revanche pas pu être établie, ni l'argent récupéré.

Le problème majeur dans ce genre de cas est que le montant du dommage ne peut généralement pas être récupéré auprès des auteurs. Il s'agit alors de déterminer s'il incombe au client ou à la banque de supporter tout ou partie de ce dommage. Or, la réponse à cette question dépend des dispositions contractuelles applicables. Habituellement, celles-ci prévoient que la banque peut (et doit) exécuter tout ordre de paiement passé dans le système e-banking, dans la mesure où les moyens de légitimation transmis sont corrects. S'agissant de la responsabilité en cas d'abus, les contrats s'appuient généralement sur la théorie dite de la «sphère des risques», selon laquelle chaque partie répond en principe des erreurs qui relèvent de sa propre sphère de contrôle et qu'elle aurait pu éviter en faisant preuve de la diligence requise. En l'espèce, la banque s'est fondée sur ces dispositions contractuelles pour exclure toute responsabilité, arguant que ses systèmes fonctionnaient parfaitement bien et que le client était seul responsable de la sécurité de son appareil, qui avait été

très probablement infecté.

Cependant, en l'espèce, il s'agissait aussi de déterminer si la banque n'aurait pas dû réagir plus rapidement auprès de la banque destinataire, de sorte que le montant transféré par les escrocs puisse encore être bloqué. Si la banque estimait être intervenue en temps utile, l'Ombudsman déplorait pour sa part le temps de réaction très long de la banque, qui n'a agi qu'en fin d'après-midi alors que le client avait signalé l'incident tôt dans la matinée. De l'expérience de l'Ombudsman, ce type d'escroquerie se caractérise souvent par le fait que les auteurs, ou les mules financières mandatés comme auxiliaires par ceux-ci, retirent l'argent immédiatement après réception sur le compte destinataire et empêchent ainsi tout blocage des fonds. Etant donné qu'une discussion sur le temps de réaction de la banque pouvait être écartée si même une intervention immédiate après notification de l'escroquerie aurait été de toute façon tardive, l'argent ayant déjà été retiré, l'Ombudsman a contacté la banque destinataire pour lui demander à quel moment le retrait a eu lieu. Invoquant le secret bancaire, celle-ci a cependant refusé de fournir des informations détaillées et s'est contentée de préciser qu'elle traitait toujours sans délai de telles notifications. L'Ombudsman n'a donc pas pu clarifier ce point comme il l'aurait souhaité, mais a fait savoir au client que les documents de l'enquête pénale pourraient s'avérer utiles à cet égard.

Si l'Ombudsman a souvent pu constater que les banques traitent de tels incidents de manière très différente les unes des autres, elles sont parfois plus généreuses que la banque concernée en l'espèce. Ici, face au refus de celle-ci de transiger en faveur du client, l'Ombudsman n'a malheureusement pas eu d'autre choix que de clore le dossier sans suite après avoir adressé son avis final au client.