Paiements frauduleux effectues par e-banking

Sujet: **Abus et escroquerie** Numéro de cas: **2017/09**

> Le client a été victime d'escrocs qui sont parvenus à intercepter ses données de connexion au système e-banking et à effectuer des versements en faveur d'une entreprise détenant un compte auprès d'une banque anglaise. La banque n'est disposée à le dédommager qu'à hauteur de la moitié du montant viré, ce que le client juge insuffisant. Elle a catégoriquement décliné toute obligation d'indemnisation dans le cadre de la procédure de médiation, mais a accepté de payer 50 % du dommage à titre de geste commercial. Sur conseil de l'Ombudsman, le client a finalement accepté la proposition de la banque.

Le client a reçu un appel téléphonique d'un interlocuteur qui s'est présenté comme un ingénieur en logiciel travaillant pour son fournisseur d'Internet. Le prétendu ingénieur lui a expliqué qu'il devait éliminer un logiciel malveillant introduit dans le système à la suite d'une cyberattaque, susceptible notamment d'agir sur l'accès aux systèmes e-banking de certaines banques. Il a ensuite demandé au client de lui communiquer ses coordonnées bancaires. Le client s'est exécuté. Son interlocuteur lui a alors enjoint de n'accéder au site Internet des banques en question qu'après avoir saisi un code spécifique. Le client a suivi cette instruction, et, à chaque fois, le site Internet a disparu brièvement avant de réapparaître à l'écran. Enfin, le prétendu ingénieur lui a expliqué que lui et ses collaborateurs pouvaient dès lors éliminer le logiciel malveillant. Par la suite, le client s'est connecté au système e-banking de ses banques en suivant les procédures d'accès habituelles et n'a rien remarqué de particulier. Quelques jours plus tard, alors qu'il s'était à nouveau connecté au système e-banking de la banque, il a constaté qu'un paiement, qu'il n'avait pas ordonné lui-même, avait été effectué depuis son compte en faveur d'un compte en banque anglais, dont le titulaire était une entreprise qu'il ne connaissait pas. Il en a immédiatement informé la banque, qui lui a assuré qu'elle prendrait les mesures nécessaires. Il s'est finalement avéré que l'argent avait déjà été retiré du compte auprès de la banque destinataire lorsque la banque a informé celle-ci de l'escroquerie.

De l'avis du client, qui a déposé une dénonciation contre inconnu, la banque est tenue de rembourser le paiement qui a été effectué sans qu'il en ait donné l'ordre. Il soutient que les autres banques auprès desquelles il détenait des comptes ont été victimes du même type d'escroquerie, et que soit elles n'ont pas exécuté les paiements, soit elles sont parvenues, en réagissant en temps opportun auprès des banques destinataires, à obtenir le remboursement des paiements effectués contre son gré, si bien qu'il n'a subi aucun dommage auprès de ces banques-là. Le client fait valoir qu'il s'est connecté au système e-banking en suivant la procédure d'accès prévue et qu'il n'est pas responsable du fait que des tiers ont, à cette occasion, pu disposer de ses comptes. Par ailleurs, la banque aurait dû reconnaître le caractère inhabituel du paiement, étant donné qu'il n'avait encore jamais effectué de versements à des tiers depuis ce compte. Toujours d'après le client, la banque a attendu trop longtemps après le signalement de l'incident pour contacter la banque destinataire, ce qui a permis aux escrocs de disposer de l'argent. Enfin, elle lui avait initialement confirmé par téléphone que le montant avait pu être bloqué auprès de la banque destinataire. De son côté, la banque a cependant décliné toute obligation d'indemnisation et s'est uniquement déclarée prête à lui rembourser 50 % du montant viré, à titre de geste commercial. Le client s'est alors tourné vers l'Ombudsman afin que celui-ci entame une procédure de médiation.

La banque a expliqué plus en détail à l'Ombudsman la position qu'elle avait déjà communiquée directement au client. Elle affirme que le paiement en question a été exécuté après la saisie des données d'accès au système e-banking requises, sans que des tiers aient agi sur les systèmes de la banque. Elle se dit autorisée, en vertu des accords contractuels relatifs à l'e-banking, à exécuter de telles transactions. La banque rappelle en outre que le client est tenu de conserver soigneusement les moyens d'accès et de ne les fournir à des tiers sous aucun prétexte. De surcroît, aucune obligation contractuelle n'engage la banque à examiner également la plausibilité de chaque paiement ordonné via e-banking. De toute évidence, en l'espèce, les déclarations du client laissent entendre que des tiers ont intercepté ses données d'accès en contaminant son appareil de saisie avec un logiciel malveillant, méfait qui s'est produit en dehors de la sphère d'influence de la banque. Celle-ci ne comprend pas pourquoi le client ne l'a pas contactée après sa conversation téléphonique avec le prétendu ingénieur afin de lui demander si l'accès à son système e-banking était bel et bien perturbé. D'après la banque, aux termes de l'accord contractuel conclu, les risques liés au système e-banking qui ne relèvent pas de sa sphère d'influence doivent être supportés par le client. Par ailleurs, la banque a pu prouver qu'elle avait informé la banque destinataire de l'incident sans délai, le matin même où elle en avait eu connaissance, et qu'elle avait réclamé le remboursement du montant viré. La banque destinataire n'ayant malheureusement pas réagi, un rappel a dû lui être adressé. Or, le client a considéré que le rappel constituait la première intervention et a dès lors conclu, à tort, à une réaction tardive de la banque. Enfin, la déclaration de la banque selon laquelle le montant avait pu être bloqué concernait un second cas contesté par le client, pour lequel l'argent avait effectivement pu être bloqué à temps et restitué au client.

La banque a décliné toute obligation d'indemnisation face à l'Ombudsman également, mais a proposé une nouvelle fois de rembourser 50 % du montant du paiement en guise de geste commercial. Après avoir procédé à un examen attentif des arguments des deux parties, l'Ombudsman a conseillé au client d'accepter l'offre de la banque. En effet, au vu de la description de l'incident, il lui semblait plausible que les escrocs aient agi sur les systèmes du client et qu'un tel acte ne relève de fait nullement de la sphère d'influence de la banque. Or, il était convenu contractuellement que de tels risques devaient être supportés par le client, ce qui correspond à une règle habituelle dans la branche. De plus, la description de l'incident permet bel et bien de douter que le client se soit montré suffisamment prudent lors de la conversation téléphonique décrite. En outre, l'Ombudsman n'a connaissance d'aucune décision judiciaire qui contraindrait une banque à vérifier la plausibilité des ordres exécutés automatiquement via e-banking. D'après lui, la jurisprudence développée en lien avec les ordres exécutés frauduleusement qui parviennent à la banque par d'autres canaux et sont examinés par des collaborateurs ne s'applique pas nécessairement à la situation du cas d'espèce. Par ailleurs, même à la lumière de la jurisprudence susmentionnée, le fait qu'aucun ordre à l'intention d'un tiers n'a jamais été effectué depuis le compte en question ne constitue pas un critère suffisant pour qualifier l'ordre d'inhabituel. Enfin, la banque a été en mesure de démontrer qu'après avoir été elle-même informée de l'escroquerie, elle l'a signalée en temps utile à la banque destinataire. Pour toutes ces raisons, l'offre de la banque semblait appropriée aux yeux de l'Ombudsman. Le client a finalement accepté la proposition de la banque.