

Ordre de paiement frauduleux

Sujet: **Trafic des paiements** Numéro de cas: **2013/10**

Un fraudeur, qui n'avait pas froid aux yeux, était parvenu à subtiliser 50 000 USD à un client d'une banque suisse qui vivait à l'autre bout du monde. Il avait fait virer ce montant dans une banque en Chine. Selon le client, la banque aurait pu éviter ce problème en se montrant plus sourcilleuse. Mais le client lui-même n'avait manifestement pas fait preuve de toute la diligence requise, puisque l'escroc disposait d'informations très détaillées sur la relation d'affaires. La banque et le client finirent par convenir d'un dédommagement à hauteur de 80 % du préjudice.

Le client considérait que les circonstances dans lesquelles l'ordre litigieux avait été passé auraient dû éveiller les soupçons de la banque, qui aurait dû prendre contact avec lui avant toute exécution. Ainsi, jamais auparavant il n'avait passé de tels ordres, les instructions du fraudeur étaient criblées de fautes d'orthographe et, pour pouvoir exécuter l'ordre, on avait même dû vendre des titres au préalable. Le client exigea donc de la banque un dédommagement intégral.

La banque décrivit la méthode sophistiquée employée par le fraudeur. Tout d'abord, en empruntant le nom du client, il avait demandé par écrit à la banque de modifier ses numéros de téléphone et son adresse électronique, ainsi que de remplacer le mot de passe convenu avec elle pour les ordres de virement par celui qu'il lui indiquait. La signature avait été soigneusement vérifiée et jugée valable. Ensuite, toujours sous le nom du client, le fraudeur avait téléphoné à la banque et, en se référant aux modifications effectuées, il avait annoncé qu'il aurait bientôt besoin d'un montant en dollars. Peu après, il avait rappelé, s'était identifié à l'aide du nouveau mot de passe et du numéro de compte, puis avait passé l'ordre de virement. Suite à cet appel téléphonique, la banque avait demandé un ordre écrit signé. Celui-ci, assorti du nouveau mot de passe, était arrivé peu après par coursier. La signature avait été vérifiée par deux collaborateurs de la banque et jugée authentique. Dès lors, on avait vendu la quantité de titres nécessaire et procédé au virement. La banque considérait globalement avoir fait preuve de la diligence que l'on était en droit d'attendre d'elle. Le paiement de 50 % qu'elle proposait n'était donc pas un dû, mais un simple geste commercial.

L'Ombudsman ne put se ranger à l'avis de la banque. Certes, graphiquement, la falsification de la signature du client était indétectable. Mais le fraudeur avait signé chaque fois en ajoutant le prénom du client, ce qui n'était conforme ni aux documents de base, ni à la pratique antérieure. Pour l'Ombudsman, il était en outre incompréhensible que la banque ait accepté l'ordre de modifier le mot de passe sans demander l'ancien mot de passe. Enfin, de l'avis de l'Ombudsman, la banque ne peut prétendre faire preuve de la diligence requise en se bornant à vérifier la signature: elle doit prendre dûment en compte d'autres aspects (p. ex. des modèles d'ordres antérieurs). Globalement, l'Ombudsman parvint à la conclusion que si le fraudeur avait déployé une énergie criminelle remarquable et disposait sans conteste de certaines données essentielles concernant le client (coordonnées bancaires, numéro de compte, signature, existence d'un mot de passe), la banque n'en devait pas moins relever son offre pour les raisons susmentionnées. Après quelques discussions, elle se déclara disposée à dédommager le client à hauteur de 80 %, ce que l'avocat du client accepta.