Prétention en dommages-intérêts pour des paiements par e-banking déclenchés par des inconnus

Sujet: **Abus et escroquerie** Numéro de cas: **2020/12**

> En l'espèce, la cliente a été vraisemblablement victime d'un hameçonnage (phishing). Des escrocs inconnus ont réussi à l'attirer sur un site internet ressemblant à celui de la banque, où elle a saisi ses données d'accès e-banking. Après avoir mis la main sur celles-ci, les escrocs ont effectué une douzaine de paiements au débit de ses comptes, pour un montant total d'environ 150 000 CHF. La banque a proposé de lui verser 39 000 CHF à titre de dédommagement, une somme toutefois jugée insuffisante par la cliente, qui comptait sur une indemnisation intégrale. La cliente a alors soumis son cas à l'Ombudsman. Dans le cadre de la procédure de médiation, la banque a revu à la hausse son offre et s'est dite prête à payer 75 000 CHF, soit la moitié du dommage. La cliente a accepté cette solution à l'amiable.

En l'espace de plusieurs jours, des escrocs inconnus ont effectué une douzaine de transactions dans le système e-banking, débitant ainsi deux comptes de la cliente d'un montant total de 150 000 CHF. Ces transactions lui semblant inhabituelles, la banque a finalement bloqué les comptes en question après cinq jours. De l'avis de la cliente, le système e-banking de la banque présentait des lacunes de sécurité, et la banque aurait dû se rendre compte bien plus tôt de l'infiltration des escrocs et des ordres de débit frauduleux.

Dans sa réponse écrite à la réclamation de la cliente, la banque a émis l'hypothèse suivante: l'ordinateur que la cliente utilisait notamment pour ses opérations e-banking a été infecté par un «cheval de Troie», ce qui a permis à des auteurs inconnus d'effectuer les transactions dommageables. Tout en contestant une éventuelle responsabilité de sa part, la banque a proposé à la cliente de lui verser 39 000 CHF pour solde de tout compte, à titre de geste commercial et sans reconnaissance d'une obligation juridique. Ce montant, qui représentait environ un quart du dommage, n'était toutefois pas suffisant aux yeux de la cliente.

La question de savoir quand une banque répond des transactions non autorisées effectuées par des tiers dans une telle situation est généralement réglée contractuellement. La plupart des contrats dont l'Ombudsman a connaissance s'appuient sur la théorie dite de la «sphère des risques», selon laquelle chaque partie répond en principe des dommages qui relèvent de sa propre sphère de contrôle, sur laquelle elle peut influer en faisant preuve de la diligence requise. Ainsi, une banque est notamment responsable de l'application de normes de sécurité actuelles dans son système e-banking. En revanche, la responsabilité relative à la sécurité des appareils qu'un client utilise pour accéder à l'e-banking incombe généralement à ce client.

Saisi de l'affaire, l'Ombudsman a tout d'abord demandé à la banque de décrire précisément la façon dont chaque transaction avait été déclenchée, ainsi que de lui expliquer les grandes lignes du concept de sécurité applicable à son système e-banking. Il n'était plus possible d'établir ce qui s'était passé sur les appareils de la cliente, car ceux-ci n'avaient été examinés ni par la banque, ni par l'autorité pénale auprès de laquelle la cliente avait déposé plainte. De même, il n'était plus possible de déterminer les adresses IP avec lesquelles la cliente s'était connectée à l'e-banking avant l'incident. La banque recourt à un processus d'authentification à deux facteurs avec numéro de

transaction (mTAN) pour la connexion au système e-banking, pour le déclenchement de certaines transactions (telles que les paiements en faveur de nouveaux destinataires), ainsi que pour la modification des coordonnées ou du numéro de téléphone. En d'autres termes, les clients doivent confirmer de telles opérations au moyen d'un code qu'ils reçoivent par SMS sur un second appareil préalablement enregistré, généralement un téléphone portable. En l'espèce, la banque a pu prouver que la cliente s'était connectée à l'e-banking en saisissant un code envoyé au numéro de téléphone qu'elle avait enregistré. Par la suite, un second numéro de téléphone a été enregistré. Cette opération a été elle aussi exécutée au moyen d'un code envoyé au premier numéro de téléphone de la cliente, auquel la banque a ensuite également envoyé la confirmation de changement de numéro. Puis, les premières transactions non autorisées par la cliente ont été déclenchées peu après au moyen du code que la banque a envoyé au nouveau numéro de téléphone, qui appartenait probablement aux escrocs inconnus. L'adresse IP avec laquelle les ordres de débit ont été passés a été enregistrée par la banque, remplaçant ainsi les adresses IP utilisées antérieurement par la cliente.

Au vu de ce qui précède, il semblerait que la cliente ait été victime de ce que l'on appelle un hameçonnage (phishing), l'escroquerie la plus répandue dans le domaine de l'e-banking. Dans un tel schéma, des escrocs attirent le client sur un site internet ressemblant à celui de la banque. Si le client essaie alors de se connecter en saisissant les données requises à cette fin, les escrocs interceptent celles-ci, puis s'en servent pour accéder au compte du client sur le véritable site de la banque. Dans d'autres cas, les escrocs parviennent à installer un logiciel malveillant (par exemple un «cheval de Troie») sur l'appareil du client et, de cette façon, à voler des données ou à prendre le contrôle de l'appareil.

Il va de soi que la banque ne pouvait pas contrôler ce qui se passait sur l'appareil de la cliente, respectivement si celui-ci avait été infecté par un «cheval de Troie». De plus, la cliente a de toute évidence saisi les données de connexion ainsi que le code SMS ayant permis le changement de numéro de téléphone. De l'avis de l'Ombudsman, un élément primordial à cet égard était le fait que le libellé du code reçu par SMS en vue de la modification du numéro de téléphone enregistré auprès de la banque était clairement différent de celui du code SMS reçu pour se connecter à l'e-banking, et qu'il était reconnaissable comme tel en faisant preuve de la diligence requise. L'Ombudsman reconnaissait en outre que le recours à un processus d'authentification par code donne en principe autorisation à la banque d'exécuter les transactions e-banking. En revanche, il estimait qu'un dispositif de sécurité supplémentaire aurait vraisemblablement permis de reconnaître le schéma d'escroquerie, qui se distingue souvent par l'utilisation d'une nouvelle adresse IP peu de temps après une modification du numéro de téléphone enregistré.

La banque a informé l'Ombudsman qu'elle avait entre-temps adapté son système e-banking dans ce sens. Elle s'est en outre proposée de faire un geste commercial plus généreux en indemnisant la cliente à hauteur de 50 % du dommage subi. Au regard des circonstances générales de l'affaire, l'Ombudsman a conseillé à la cliente d'accepter cette offre, ce qu'elle a finalement fait.