Enregistrement frauduleux d’une carte de crédit dans un porte-monnaie électronique (tel qu’Apple Pay ou Samsung Pay)

Sujet: **Abus et escroquerie** Numéro de cas: **2020/11**

> En très peu de temps, la carte de crédit du client a été débitée de plus de 21 000 CHF, un montant dépassant sa limite de crédit de 2000 CHF. Les débits provenaient d’un pays scandinave, dans lequel le client ne se trouvait pas au moment des faits. En réponse à la réclamation du client, l’émettrice de la carte de crédit a soutenu qu’il avait transmis les données de sa carte à des tiers inconnus, leur permettant ainsi d’enregistrer celle-ci dans un porte-monnaie électronique et d’exécuter les transactions. Elle s’est donc proposée de ne lui rembourser qu’un peu moins de 75 % du dommage causé par l’utilisation abusive de la carte. Insatisfait de cette proposition, le client s’est tourné vers l’Ombudsman. Dans le cadre de la procédure de médiation, l’émettrice de la carte de crédit a accepté d’augmenter le montant de l’indemnisation à 85 %, une offre que le client a finalement acceptée à contrecœur.

Le client a expliqué à l’Ombudsman non seulement être toujours très prudent avec sa carte de crédit, qu’il utilise avant tout pour des transactions en ligne, mais aussi protéger tous ses appareils électroniques au moyen de logiciels de protection constamment mis à jour. Il affirmait n’avoir jamais transmis les données de sa carte de crédit à des tiers et ne pas comprendre comment les débits contestés avaient pu être effectués. Selon lui, de tels débits étaient très inhabituels pour lui et auraient dû attirer l’attention de l’émettrice de la carte de crédit, d’autant plus qu’ils dépassaient largement sa limite de crédit. Il avait augmenté celle-ci à 19 000 CHF dans le cadre d’un voyage aux Etats-Unis et avait malheureusement oublié de l’abaisser à nouveau à 2000 CHF, ce qu’il s’est néanmoins empressé de faire après l’incident.

Dans sa prise de position à l’attention de l’Ombudsman, l’émettrice de la carte de crédit n’a pas mis en doute le fait que les transactions contestées par le client avaient été effectuées par un tiers non autorisé. Néanmoins, l’utilisation des données de carte dans un porte-monnaie électronique équivaut à une utilisation de la carte avec un code NIP. Les tiers non autorisés ne peuvent utiliser une carte dans un porte-monnaie électronique que s’ils sont en possession des données de carte nécessaires. Or, celles-ci sont initialement toujours transmises au seul titulaire de la carte. Par conséquent, le fait qu’un tiers parvienne à se procurer ces données, y compris le code de confirmation pour l’authentification à deux facteurs, résulte d’une violation des obligations de diligence du titulaire de la carte. Etant donné que les données n’avaient de toute façon pas pu atterrir entre les mains d’un tiers autrement que par le biais du titulaire de la carte, il n’était pas déterminant de savoir comment cette transmission avait eu lieu exactement. Toujours selon les dires de l’émettrice de la carte de crédit, une carte ne peut être enregistrée dans un porte-monnaie électronique qu’au terme d’un processus d’authentification à deux facteurs. Dès lors, il y a lieu de partir du principe que les transactions effectuées avec une telle carte sont déclenchées par le titulaire de la carte ou autorisées par lui. De telles opérations ne sont donc pas surveillées selon les mêmes règles que les transactions non soumises à l’authentification à deux facteurs.

En outre, l’émettrice de la carte de crédit a rappelé que, malheureusement, il arrive souvent que des

clients se fassent abuser par des courriers électroniques ou des SMS falsifiés, qui les invitent à cliquer sur des liens et à saisir les données de leur carte de crédit. Selon elle, une telle situation s'est vraisemblablement produite en l'espèce, le client ayant divulgué toutes les données nécessaires à l'enregistrement de sa carte dans un porte-monnaie électronique, à savoir le numéro, la date d'expiration et le code de vérification (CVC) de la carte, ainsi que le numéro de transaction (mTAN) reçu pour confirmer l'enregistrement.

Etant donné que le CVC figure uniquement au dos de la carte et n'est pas généralement accessible, l'émettrice de la carte de crédit estimait que le client avait antérieurement transmis ce code à des tiers, peut-être en croyant payer pour une prestation souhaitée ou participer à un concours. De surcroît, les tiers non autorisés devaient avoir soit obtenu un accès à son téléphone portable, soit reçu le code directement du client. En effet, ce code n'était accessible que sur le téléphone portable préalablement enregistré du client.

Les systèmes de l'émettrice de la carte de crédit ont montré que le SMS contenant le code d'activation et le SMS de confirmation ont été tous deux envoyés au numéro de téléphone indiqué par le client. Après qu'une personne en possession des données nécessaires eut soumis une demande d'enregistrement de la carte comme moyen de paiement dans un porte-monnaie électronique pour smartphone, l'émettrice de la carte de crédit a immédiatement envoyé le code d'activation, grâce auquel le processus d'enregistrement a pu être conclu avec succès. La confirmation de l'enregistrement a été elle aussi envoyée par SMS au numéro de téléphone indiqué par le client. Le texte type des SMS («Veuillez saisir le code d'activation XXX afin d'activer votre carte de crédit se terminant par XXXX dans [Apple Pay/Samsung Pay]», ainsi que «Votre carte de crédit se terminant par XXXX a été activée avec succès dans [Apple Pay/Samsung Pay]») indiquait clairement qu'il était question de l'activation de la carte dans une application de paiement. Toujours d'après les dires de l'émettrice de la carte de crédit, l'utilisation frauduleuse de la carte, qui a eu lieu quelques jours plus tard, aurait pu être évitée si le client avait réagi en temps utile à ces SMS.

L'émettrice de la carte de crédit a poursuivi son argumentation en faisant valoir que les opérations contestées sont des transactions «sans contact» telles que prévues dans les conditions applicables aux cartes, où elles sont désignées comme possibilité de remplacement de la carte. En divulguant les données de sa carte et en saisissant lui-même le code d'activation, respectivement en communiquant celui-ci à des tiers, le client a violé ses obligations de diligence. L'émettrice de la carte de crédit estimait donc avoir eu raison de refuser la prise en charge du dommage.

Enfin, l'émettrice de la carte de crédit a souligné que, selon les cas, il peut arriver qu'une limite de crédit soit dépassée en raison d'une conversion ou d'une utilisation de la carte à l'étranger. De plus, les limites des clients de longue date sont gérées avec une certaine flexibilité. En définitive, en raison de leur longue relation d'affaires, l'émettrice de la carte de crédit s'est dite prête, à bien plaire et sans reconnaissance de quelque obligation juridique que ce soit, à indemniser le client à hauteur de 85 % du dommage subi.

L'Ombudsman a transmis au client cette nouvelle offre en lui faisant aussi part de ses propres remarques. En règle générale, ainsi que le prévoient la plupart des contrats correspondants, les transactions effectuées par carte de crédit sont attribuées au client dès lors qu'elles sont déclenchées par le biais des moyens de légitimation convenus. Les émetteurs de carte de crédit ne supportent les dommages résultant d'une utilisation abusive de la carte que si les transactions ont été effectuées par des tiers non autorisés sans que le client n'ait rendu possible une telle situation en violant ses obligations de diligence.

La question de savoir comment, en l'espèce, les escrocs ont réussi à prendre possession des données nécessaires pour enregistrer la carte de crédit du client dans un porte-monnaie électronique devait

être laissée ouverte dans le cadre de la procédure de médiation. Selon l'émettrice de la carte de crédit, une telle situation n'a pu se produire qu'avec la participation du client, qui a probablement été victime d'une escroquerie et a ainsi divulgué ses données. Cependant, le client contestait ces faits. En tant que médiateur neutre, l'Ombudsman n'est pas habilité à mettre en doute la crédibilité des parties. Il n'engage donc jamais de procédure d'administration des preuves qui permettrait d'établir les faits de manière contraignante, selon des règles spécifiques, lorsque les parties présentent des versions des faits contradictoires. Le but de la procédure de médiation est plutôt de régler des litiges à l'amiable, l'Ombudsman pouvant suggérer des solutions en se fondant sur les informations transmises par les parties. Il n'a toutefois pas autorité pour se prononcer de façon contraignante sur des faits ou des questions juridiques contestés, de tels aspects relevant de la compétence des tribunaux ordinaires.

Etant donné qu'il était impossible de clarifier davantage l'incident dans le cadre de la procédure de médiation et que l'émettrice de la carte de crédit avait déjà annoncé qu'elle ne consentirait pas à supporter plus de 85 % du dommage, l'Ombudsman a conseillé au client d'accepter l'offre soumise. A ses yeux, il aurait certes été souhaitable que le processus d'enregistrement d'une carte dans un porte-monnaie électronique soit régi contractuellement de façon plus claire, de sorte qu'un client soit au moins informé dans les grandes lignes sur le produit et son fonctionnement et puisse, par exemple, refuser de l'utiliser. L'Ombudsman se demandait aussi dans quelle mesure la base contractuelle invoquée à cet égard par l'émettrice de la carte de crédit était suffisante. En effet, cette base semblait davantage adaptée aux transactions individuelles avec la fonction «sans contact» qu'à l'enregistrement d'une carte dans un porte-monnaie électronique. Cependant, de l'avis de l'émettrice de la carte de crédit, il ressortait suffisamment clairement du SMS reçu dans le cadre de l'authentification à deux facteurs que le client, en saisissant le code, consentait à l'enregistrement d'une carte dans un tel porte-monnaie électronique. Compte tenu du processus mis en œuvre, les dispositions contractuelles détaillées applicables au porte-monnaie électronique étaient uniquement visibles par les malfaiteurs, sur l'appareil à partir duquel la carte a été enregistrée, ce que l'Ombudsman jugeait toutefois peu optimal.

Après avoir pesé le pour et le contre de l'arrangement proposé, le client a finalement accepté celui-ci, non sans exprimer son mécontentement quant à l'attitude adoptée par l'émettrice de la carte de crédit face à sa réclamation.