1. Résumé de la plainte

Un consommateur a été victime d'une arnaque sur ses comptes bancaires à la suite de la réception d'un mail de phishing « Itsme ». Il a reçu un prétendu sms de Itsme, reprenant un lien sur lequel il a cliqué et suivi les étapes d'une procédure d'identification via sa banque. Il a recopié un code qui lui a été transmis et a utilisé son digipass.

A la suite de cet incident, il a été contacté par Atos pour l'aviser de mouvements suspects sur ses comptes et il a immédiatement bloqué ses cartes.

Il réclame à sa banque le remboursement intégral de son préjudice.

2. Position de la banque

L'analyse des opérations contestées montre qu'elles ont été validées au moyen de l'application Mobile de la banque. La banque constate que cette application a été installée le 12 mars 2022 sur le profil client une première fois à 10h38, une seconde fois à 10h56 et enfin, une troisième fois à 12h42

L'installation de cette application est protégée par la technologie 3D-Secure. Pour l'installer, il faut disposer des 3 éléments suivants : être en possession physique de la carte de débit; disposer du code secret, dont seul le titulaire de la carte a connaissance et disposer du code-autorisation provenant du lecteur de carte (après y avoir introduit la carte et le code secret).

Le système « 3D-secure » est un mécanisme permettant de sécuriser les paiements en ligne via une triple authentification de l'utilisateur de l'instrument de paiement : en combinant (1) la carte de débit et (2) l'introduction du code pin connu seulement de l'utilisateur (3) dans le lecteur de cartes, un code sécurisé est généré. Il n'existe à ce jour pas de moyen d'authentification plus solide ou plus sécurisé.
A l'exception d'une installation de l'application effectuée par le titulaire de la carte de débit, il n'existe ainsi que 2 cas de figure pour qu'une tierce personne puisse le faire :

- soit le titulaire de la carte lui a donné sa carte de débit et lui a communiqué son code secret ;
- soit le titulaire de la carte lui a communiqué son numéro de carte et le code confidentiel sécurisé délivré par le lecteur de carte.

Pendant cette installation, la banque a envoyé, à chaque installation, 2 SMS, sur le numéro de téléphone connu dans la base de données de la banque :

- « Info Banque. Vous venez d'installer l'app de la Banque ! Ce n'est pas vous? Bloquez vite vos cartes via Card Stop au 078 170 170 et appelez-nous au …. »
- «Info Banque. Vous venez d'installer l'app de la Banque. Votre code d'activation est xxxx. Valide pendant 10 minutes. Ne le partagez avec personne!"

Le client a donc reçu 6 sms au total.

Après avoir effectué l'installation au moyen du numéro de carte et d'un code généré par le digipass, l'activation finale de l'application ne peut se faire qu'au moyen du code confidentiel qui est personnellement envoyé par SMS.

La banque observe que le client n'a pas réagi à ces SMS d'information concernant une installation de l'application Mobile et n'a pas contesté ou bloqué celle-ci immédiatement. Pourtant, les opérations ayant eu lieu plusieurs heures après, une réaction rapide aurait permis de les éviter.

Le client explique avoir utilisé son digipass mais n'explique pas comment le fraudeur a pu entrer en possession des codes générés par le digipass. Or, il est démontré que le numéro de carte et les codes digipass, ainsi qu'un code secret envoyé par SMS, étaient indispensables pour installer l'application Mobile.

La loi sur les instruments de paiement (code de droit économique) définit les droits et obligations du détenteur d'un moyen de paiement. L'article VII 44 mentionne *« le payeur ne supporte aucune perte si la perte, le vol ou le détournement d'un instrument de paiement n'a pu être détecté par le payeur avant qu'un paiement ne soit effectué (…)* »

Ce caractère détectable s'apprécie suivant les circonstances de faits. La banque estime qu'il existait de nombreux indices qui auraient pu attirer l'attention du client :

- être contacté d'abord par sms;
- devoir cliquer sur un lien dans un sms ;
- être contacté par sms par un tiers inconnu, qui demande des données personnelles ; puis devoir utiliser le digipass et la carte de débit ;
- des demandes répétées pour introduire des chiffres dans le digipass
- ces manipulations ne font pas sens pour « valider » son identité
- recevoir au total 6 sms de la part de la banque l'informant qu'une installation venait d'être effectuée et que si ce n'était pas vous, de bloquer votre carte

L'article VII 44 du code de droit économique mentionne : « *le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent soit d'un agissement frauduleux de sa part, soit du fait qu'il n'a pas satisfait intentionnellement ou à la suite d'une négligence grave a une ou plusieurs des obligations qui lui incombent en vertu de l'article VII 38*. »

L'article VII 38 mentionne: « l'utilisateur de services de paiement prend, en particulier, dès qu'il reçoit un instrument de paiement, toutes les mesures raisonnables afin de préserver la sécurité de l'instrument de paiement et de ses données de sécurité personnalisées.».

Cette sécurité ne peut être assurée que si le client n'introduit pas des données strictement personnelles comme les codes uniques générés par le lecteur de cartes dans un environnement autre que l'environnement sécurisé de la banque.

L'analyse technique fait la preuve que l'installation Mobile aurait été impossible sans le concours du client.

Le client omet d'indiquer ce qu'il a fait de ces codes. Or introduire sa carte et son code secret dans le digipass pour générer un code secret, sans rien en faire ensuite, ne peut pas avoir de conséquences financières. En l'espèce, le fraudeur a bien été en mesure d'intercepter ces codes générés, ainsi que le code secret qui a personnellement été envoyé par SMS.

La banque relève que, depuis de nombreux mois, de multiples et régulières communications sont faites par les autorités belges, les médias et les banques afin d'informer les utilisateurs de services de paiement de ce type de fraudes et de leur prodiguer des conseils en matière de sécurité.

Il appartient à l'utilisateur de services de paiement d'être prudent et diligent lors de la lecture de messages et/ou courriels surtout lorsqu'il est demandé de cliquer sur un lien. Si l'utilisateur de services de paiement clique sur un lien sollicitant la communication de codes sécurisés (délivrés par le lecteur de cartes), il est de sa responsabilité de ne pas communiquer ces codes.

La banque refuse dès lors d'intervenir.

3. L'avis d'Ombudsfin

Il ressort des éléments du dossier que le plaignant a été victime de phishing via un SMS « Itsme ». Au cours de la présente médiation et des divers échanges pour tenter de déterminer les circonstances qui ont entouré cet incident, le plaignant n'a pas contesté pas avoir reçu un sms qui provenait prétendument d'Itsme. Selon ce SMS, il devait réactiver son compte Itsme. Pour cela, il a cliqué sur un lien dans le message et ainsi accédé à un site web où il devait effectuer des actions avec sa carte bancaire et le digipass, et ensuite saisir des codes sur son écran.

Le plaignant ne savait pas qu'en cliquant sur le lien, il était arrivé sur un faux site web contrôlé par un fraudeur. En saisissant les données du client et les codes générés par sa carte bancaire et son digipass, le fraudeur a réussi à les intercepter puis à les utiliser pour installer l'application Mobile de la banque, liée aux comptes du plaignant, sur son propre appareil. Le fraudeur a utilisé cette application pour effectuer les transactions litigieuses quelques temps après cette activation. Elles ont été ainsi validées selon une authentification forte (signature 3DSecure exécutée via l'introduction d'une signature, obtenue au moyen de la carte en question et d'un lecteur de carte). Suivant l'expérience d'Ombudsfin, ces prétendues procédures sont habilement amenées et effectuées avec des logos similaires à ceux officiellement utilisés.

Étant donné que le plaignant n'a en aucune manière consenti à l'exécution des opérations litigieuses, il s'agit, selon l'analyse d'Ombudsfin, d'opérations de paiement non autorisées au sens de l'article VII.32, §2, alinéa 4 du Code économique belge (ci-après " CDE "). L'utilisation de la carte et du code PIN ne constitue pas nécessairement une preuve du caractère autorisé de la transaction ou d'une négligence grave de la part du client, comme le prévoit également l'article VII.42 CDE.

Par conséquent, les dispositions du CDE sur l'attribution de la responsabilité pour les opérations de paiement non autorisées s'appliquent.

L'article VII.44, §1, alinéa 2, 1° CDE prévoit ce qui suit :

"Par dérogation à l'alinéa 1er, le payeur ne supporte aucune perte si la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf si le payeur a agi frauduleusement."

Cet article de la loi s'applique lorsque la victime d'une fraude n'a pas pu détecter à l'avance le détournement de son instrument de paiement. Les travaux préparatoires de la loi indiquent que cet article peut être appliqué, par exemple, dans certains cas de phishing. La question de savoir si la fraude pouvait être détectée à l'avance ou non dépend de l'analyse de tous les faits. Dans son avis, la banque fait référence aux

six SMS que le client a reçus concernant l'installation frauduleuse de l'application Mobile. Ombudsfin a interrogé le plaignant à deux reprises sur la réception de ces sms du 12 mars, en lui demandant un screenshot de son gsm mais le plaignant n'a pas répondu avec précision à cette demande 9 mars. Dans ce dossier, il subsiste donc un doute quant à la réception de ces sms sur votre gsm alors que vous tentiez de réactiver une application « Itsme ». Ombudsfin iestime dès lors que la preuve de la non-détectabilité de la fraude n'est pas rapportée à suffisance.

Dans l'hypothèse où l'article VII.44, §1, alinéa 2, 1° CDE n'est pas applicable, la règle de base de l'article VII.44 CDE doit être suivie : la banque doit supporter la perte, après déduction d'une franchise de 50 euros, sauf si la banque peut apporter la preuve que le payeur a manqué à certaines obligations par négligence grave.

L'article VII.44, §4, paragraphe 3 du CDE prévoit en outre que pour l'évaluation de la négligence grave, toutes les circonstances factuelles doivent être prises en considération. Selon Ombudsfin, le plaignant ne savait pas que le lien menait à un faux site web contrôlé par le fraudeur et que ses données avaient ainsi été hameçonnées à son insu. À aucun moment, il n'a communiqué ses données directement au fraudeur. Par ailleurs, le contexte de la vérification de son identité pour son application Itsme via son lecteur de carte pouvait sembler vraisemblable compte tenu du fait que le digipass de la banque peut servir à lire les données d'identité et les données bancaires.

Ombudsfin estime donc que le comportement du plaignant est constitutif d'une imprudence mais pas d'une négligence grave.

En ce qui concerne l'éventuel blocage ou la récupération des sommes frauduleusement prélevées sur les comptes du plaignant, Ombudsfin rappelle qu'il s'agit d'achats –paiements- sur internet et qu'ils ne peuvent pas être arrêtés par la banque lorsqu'ils ont été initiés et approuvés car il s'agit d'opérations instantanées. Un recouvrement de ces paiements frauduleux n'est donc pas possible, sous réserve de la collaboration active du commerçant, mais il n'appartient pas à la banque de récupérer ces fonds chez le commerçant.