Dossier du mois : Phishing – Opérations frauduleuses entre (notamment) un compte privé d'une personne et un compte professionnel sur lequel cette personne était mandataire – Absence d'authentification forte du client

Avis rendu en néerlandais - traduction libre

1. LA PLAINTE

Vous avez introduit une plainte en votre nom propre et en qualité d'administrateur d'une société. Vous-même, la société ainsi qu'un certain nombre d'associations de copropriétaires (ACP) pour lesquelles vous étiez mandataire, êtes titulaires de compte auprès de la même banque.

Vous avez été victime d'une fraude. Vous avez déposé plainte à ce sujet auprès de la police.

Les faits suivants ressortent du procès-verbal de la plainte pénale et de la plainte que vous avez introduite auprès d'Ombudsfin:

- L'an passé, vous avez reçu sur votre ordinateur un message vous indiquant que vous deviez contacter la banque via le numéro de téléphone mentionné.
- Selon votre déclaration dans le procès-verbal, vous avez appelé ce numéro de téléphone et vous avez eu en ligne un homme qui s'est présenté comme un collaborateur de la banque. L'homme vous a indiqué que des opérations suspectes avaient lieu sur votre compte. Dans votre plainte auprès d'Ombudsfin, vous avez toutefois indiqué que vous aviez été appelé.
- Afin de vérifier que vous aviez effectivement un collaborateur bancaire en ligne, vous avez communiqué les deux derniers chiffres d'un numéro de compte bancaire et vous avez demandé le solde à une date déterminée. Votre interlocuteur a pu vous le communiquer.
- Sur instruction du prétendu collaborateur bancaire, vous deviez effectuer différentes manipulations afin de bloquer vos comptes. Vous avez commencé à avoir des soupçons lorsque vous avez également reçu des questions concernant vos comptes auprès d'une autre banque.
- Après avoir mis fin à l'appel téléphonique frauduleux, vous avez contacté l'autre banque afin de demander le blocage de votre compte.
- Vous avez également été appelé par une autre institution financière, qui vous a demandé si vous aviez effectué, via sa plateforme, un virement vers un compte étranger. Vous avez répondu par la négative et demandé que ce virement soit bloqué.
- Vous vous êtes ensuite rendu à l'agence bancaire locale de la banque contre laquelle vous avez introduit la présente plainte. Vos comptes y ont été bloqués (probablement, selon vous, suite à un appel à un service interne de la banque). Il

vous a également été conseillé de déposer plainte auprès de la police. Aucun extrait de compte relatif aux opérations frauduleuses ne vous a été remis.

- Quelques jours plus tard, vous vous êtes à nouveau rendu à votre agence bancaire locale et vous avez reçu une impression du compte de la société dont vous êtes administrateur. Vous avez constaté qu'un montant de 25.015 euros avait été viré depuis le compte de la société vers un compte étranger. Aucun bénéficiaire n'était mentionné. Votre collaborateur bancaire a ensuite inscrit à la main le nom du bénéficiaire sur l'extrait. Il s'agissait d'un bénéficiaire disposant d'un numéro de compte en dehors de la zone SEPA. Vous avez également constaté que, préalablement au virement étranger, plusieurs virements avaient été effectués vers le compte de la société: un montant total de 39.350 euros avait été viré depuis les comptes d'ACP (pour lesquelles vous étiez mandataire) et un montant de 11.250 euros avait été viré depuis votre compte personnel vers le compte de la société.
- Le même jour, vous vous êtes à nouveau rendu à la police afin de faire établir un procès-verbal. Vous avez évoqué avec le policier la possibilité que l'argent viré vers un compte étranger en dehors de la zone SEPA se trouvait encore sur un compte d'attente et pouvait éventuellement être récupéré (sans garantie toutefois).
- Au cours de la période de juillet à septembre 2025, vous avez dû vous rendre à plusieurs reprises à votre agence bancaire locale afin de faire payer des factures et de vous informer au sujet de nouvelles cartes bancaires. Vous n'avez reçu de nouvelles cartes bancaires qu'au début du mois d'octobre 2025, soit plus de trois mois après la fraude.

Vous estimez que la banque n'a pas correctement donné suite à votre signalement de fraude et a omis d'empêcher le virement dommageable du compte de la société vers un compte étranger en dehors de la zone SEPA. Vous renvoyez à cet égard à des communications de la banque indiquant que, pour les virements non SEPA, il peut s'écouler jusqu'à cinq jours avant que les fonds soient disponibles pour le bénéficiaire.

Vous demandez que la banque indemnise votre préjudice financier de 25.015 euros. Il s'agit du montant qui a été viré depuis le compte de la société vers un numéro de compte étranger en dehors de la zone SEPA (frais inclus). Ce virement a été précédé d'un virement depuis votre compte personnel (pour un montant de 11.250 euros) et de virements depuis les comptes des ACP (pour un montant total de 39.350 euros), chaque fois vers le compte de la société.

2. POSITION INITIALE DE L'INSTITUTION FINANCIÈRE

L'institution financière nous a communiqué la position initiale suivante :

« (...) Le client conteste neuf virements qui ont tous été exécutés à la même date à partir de différents comptes dont le client est mandataire ou titulaire. Le client ne peut lui-

même fournir aucune explication quant à la manière dont les virements ont pu être exécutés.

L'analyse des opérations montre que celles-ci ont été exécutées via la banque en ligne, à savoir :

Transferts internes : (...)

Virement sortant : (...)

La connexion pour l'utilisation de la banque en ligne a été effectuée au moyen de la carte bancaire personnelle du client. La carte n'a par ailleurs jamais été déclarée perdue ou volée. Une manipulation supplémentaire avec la carte et le lecteur de carte a également été utilisée.

Étant donné que cette connexion s'est déroulée au moyen d'une authentification forte, les opérations contestées sont autorisées conformément à l'article VII.32, §§ 1er et 2, du CDE. Dans ce cas, la banque n'est pas tenue d'en indemniser le dommage.

Même si le client estime ne pas avoir donné son consentement à ces transactions, celles-ci ont soit été exécutées par un tiers qui a temporairement eu accès à la carte bancaire et connaissait le code secret y afférent, soit le client a permis à un tiers de prendre connaissance ou de disposer de sa procédure de signature en communiquant des données bancaires, ce qui constitue une négligence de la part du client.

Le non-respect des mesures de précaution reprises dans les conditions générales bancaires est considéré comme un élément de négligence grave.

La notion de « négligence grave » est une notion juridique et n'implique aucun jugement de valeur de la part de la banque.

Après la notification de la fraude, une demande de récupération a été transmise le (date). La banque correspondante s'est toutefois référée à la législation du pays du bénéficiaire, qui prévoit que le bénéficiaire doit confirmer son accord pour un éventuel remboursement. Aucun remboursement n'a été possible dès lors que le correspondant n'a pas pu établir de contact.

Conclusion

Sur la base de tous les éléments du dossier exposés ci-dessus, nous devons confirmer que nous ne pouvons pas accéder à la demande d'indemnisation du dommage subi.

Les opérations se sont déroulées au moyen d'une authentification forte et la banque a également transmis une demande de récupération ; la banque correspondante n'a toutefois pas voulu y donner suite. »

3. NOTRE AVIS

A. Déroulement de la fraude : vishing

Vous avez malheureusement été victime d'une fraude connue sous le nom de vishing (voice + phishing). Un fraudeur est parvenu à vous convaincre par téléphone d'effectuer des manipulations avec votre carte bancaire, votre code PIN et votre lecteur de carte afin de mettre en échec une prétendue tentative de fraude.

Dans le procès-verbal de votre plainte pénale, nous avons lu qu'après avoir reçu sur votre ordinateur un message qui semblait provenir de la banque, vous avez appelé le numéro mentionné dans ce message et vous pensiez avoir un collaborateur de la banque en ligne. Au cours de notre médiation, vous n'avez pas pu nous transmettre le message concerné. Vous n'avez pas non plus pu retrouver le numéro de téléphone que vous deviez appeler. Vous nous avez également indiqué que, dans votre souvenir, vous aviez été appelé par un numéro inconnu plutôt que d'avoir appelé vous-même. Vous avez pris contact avec votre opérateur télécom afin de vérifier les heures de cet ou ces appels, mais vous ne les avez pas reçues.

Au cours de notre médiation, vous avez indiqué que vous deviez communiquer votre numéro de carte bancaire afin que le prétendu collaborateur bancaire puisse obtenir un aperçu de tous les comptes sur lesquels vous disposiez d'une procuration.

Le prétendu collaborateur bancaire a gagné votre confiance en pouvant vous communiquer les soldes corrects de vos comptes. Nous ne pouvons malheureusement pas expliquer comment cela a été possible. Les escrocs recourent souvent à des techniques de manipulation psychologique pour vous donner l'impression qu'ils disposent de vos informations. Les fraudeurs utilisent également des données bancaires précédemment interceptées au moyen d'un phishing classique afin de convaincre leur victime, de manière crédible, de la légitimité de l'appel. Lorsque les escrocs ont déjà obtenu, par un phishing préalable, l'accès à l'environnement bancaire en ligne de leur victime — ce qui leur permet de voir les comptes de la victime et déjà d'effectuer des opérations entre les différents comptes de celle-ci — ils parviennent souvent à présenter un récit très crédible. Nous ne pouvons toutefois pas déterminer si tel a bien été le cas dans le présent dossier.

Vous nous avez en outre expliqué qu'après que le prétendu collaborateur bancaire eut gagné votre confiance, vous deviez introduire un certain nombre de chiffres par compte, soi-disant afin de bloquer ceux-ci. Vous nous avez aussi indiqué que vous deviez, au moyen de votre carte bancaire, de votre code PIN et de votre lecteur de carte, générer des codes et les communiquer via votre ordinateur, qui était sous le contrôle du fraudeur. Cela était nécessaire, selon lui, pour empêcher de prétendues opérations frauduleuses sur les comptes et pour bloquer ceux-ci. Vous ne vous souvenez pas d'autres détails concernant les manipulations exactes que vous deviez effectuer.

Il ressort des données techniques de la banque qu'au moins deux codes de réponse ont dû être générés et interceptés par le fraudeur. Celui-ci est ainsi parvenu, au moyen d'un premier code de réponse intercepté, à se connecter à votre banque en ligne et à approuver des virements entre les comptes sur lesquels vous disposiez d'une procuration. Au moyen d'un second code de réponse intercepté, le virement dommageable de 25.000 euros, majoré de 15 euros de frais, a été approuvé. La carte bancaire et le code PIN utilisés pour générer ces codes de réponse étaient ceux de la carte bancaire liée à votre compte personnel.

Au cours de la médiation, vous avez indiqué ne disposer d'aucun élément laissant penser que votre ordinateur aurait été pris en main à distance (par exemple au moyen d'applications telles qu'Anydesk ou TeamViewer). Le fait que, selon votre déclaration dans le procès-verbal de votre plainte pénale, vous ayez vu un message sur l'écran de votre ordinateur laisse toutefois supposer le contraire. La banque nous a également communiqué, au cours de la médiation, que les actions effectuées dans votre banque en ligne provenaient d'une adresse IP connue de la banque comme vous étant associée et qui avait déjà été utilisée auparavant pour votre banque en ligne. Le fait que votre banque en ligne ait été utilisée depuis une localisation connue de la banque comme étant la vôtre, alors que vous contestez avoir vous-même exécuté les différentes opérations, laisse supposer qu'un fraudeur est effectivement parvenu à prendre le contrôle de votre ordinateur.

Vous avez en outre évoqué, au cours de notre médiation, l'utilisation d'un lecteur de carte eID. Nous n'avons toutefois pas de visibilité sur l'éventuelle utilisation abusive que le fraudeur aurait faite de vos données eID.

B. Régime légal de responsabilité en cas d'opérations de paiement non autorisées pour les consommateurs et les non-consommateurs

Ombudsfin estime que vous démontrez de manière suffisamment vraisemblable que vous n'avez pas consenti aux opérations contestées. Vous avez été contacté par téléphone par un fraudeur qui s'est fait passer pour un collaborateur bancaire. Vous avez été entièrement trompé et avez suivi les instructions du fraudeur. Vous pensiez prévenir une fraude par vos actions. Vous ignoriez que, par vos manipulations, vous généreriez des codes réponse permettant au fraudeur d'accéder à votre banque en ligne, d'effectuer des virements entre les comptes sur lesquels vous disposiez d'une procuration et, finalement, d'approuver le virement dommageable vers un compte étranger en dehors de la zone SEPA.

Étant donné que vous n'avez pas consenti à l'exécution des opérations contestées, il est question, dans ce dossier, d'opérations de paiement non autorisées au sens de l'article VII.32 du Code de droit économique (ci-après « CDE »).

Par conséquent, les dispositions du CDE relatives à la répartition des responsabilités en cas d'opérations de paiement non autorisées (articles VII.43 et VII.44 CDE) sont applicables. Ce régime de responsabilité s'applique en principe tant aux consommateurs qu'aux non-consommateurs. Le CDE permet toutefois aux banques de convenir avec les clients qui ne sont pas des consommateurs que le régime de responsabilité objective en cas d'opérations de paiement non autorisées ne s'applique pas, en tout ou en partie.

L'article VII.29 CDE dispose comme suit :

> « ***Lorsque l'utilisateur de services de paiement n'est pas un consommateur**, **les parties peuvent convenir** que les articles VII.30, § 1er, VII.32, § 3, VII.33, VII.42, **VII.44**, VII.46 et VII.47, VII.50, VII.55/3 à VII.55/7, **ne s'appliquent pas, en tout ou en partie***. *Les parties peuvent également convenir d'un autre délai que celui prévu à l'article VII.41*. » **(mise en évidence par nos soins)**

La banque a fait usage de cette possibilité par le biais de ses conditions générales bancaires : (...)

Dans le présent dossier, vous êtes, en tant que personne privée, titulaire de votre compte personnel et vous êtes qualifié de consommateur pour ce compte. La société ne peut en revanche être qualifiée de consommateur. Enfin, selon nous, les ACP ne peuvent pas non plus être qualifiées de consommateurs pour l'application des articles VII.43 et VII.44 CDE. Bien que le CDE prévoie, dans certains domaines, que certaines ACP bénéficient de la même protection que les consommateurs (voir par exemple l'article VI.81/1 CDE en matière de clauses abusives dans les contrats conclus avec des consommateurs), le CDE ne prévoit pas une telle protection pour l'application des articles VII.43 et VII.44 CDE.

Étant donné que, dans le cadre de la fraude dont vous avez été victime, une opération a été effectuée depuis votre compte privé vers le compte professionnel de la société, suivie d'une opération depuis ce dernier compte vers un tiers, la question se pose de savoir pour quelles opérations la banque peut se prévaloir de la limitation du régime légal de responsabilité en cas d'opérations de paiement non autorisées pour les non-consommateurs prévue dans ses conditions générales.

Au cours du traitement du dossier, Ombudsfin a spécifiquement consulté son collège d'experts à ce sujet.

Le collège d'experts a rendu l'avis suivant le 7 avril 2026 :

> *« Lorsque, dans le cadre d'une fraude unique, un fraudeur fait d'abord transférer des fonds d'un compte privé vers un compte professionnel auquel le titulaire du compte privé a accès via son environnement de banque en ligne, puis fait transférer des fonds de ce compte professionnel vers le compte d'un fraudeur, il ne peut être dérogé à l'article VII.44 CDE que pour la seconde opération de paiement non autorisée. Pour la première opération non autorisée, une dérogation*

au régime de l'article VII.44 CDE n'est pas possible, dès lors que la victime détient ce compte en qualité de consommateur. Cette interprétation garantit qu'un consommateur victime d'une fraude au paiement soit traité de la même manière, indépendamment du déroulement ultérieur de la fraude.

En l'espèce, un montant de 11.250 euros a été transféré du compte privé de la victime vers un compte professionnel d'une société auquel la victime avait accès via son environnement de banque en ligne. Ensuite, un montant de 25.000 euros a été transféré via ce compte vers un compte contrôlé par le fraudeur en Turquie. Le raisonnement qui précède implique que, pour l'opération de paiement non autorisée d'un montant de 11.250 euros, le régime de l'article VII.44 CDE est applicable. Pour la seconde opération de paiement non autorisée, il peut être dérogé au régime de l'article VII.44 CDE dans les conditions bancaires. »

Nous examinerons ci-après d'abord l'application du régime légal de responsabilité à l'opération de paiement non autorisée effectuée depuis votre compte privé à concurrence de 11.250 euros.

Nous aborderons ensuite l'opération de paiement non autorisée effectuée depuis le compte de la société à concurrence de 25.015 euros.

C. Application du régime légal de responsabilité à l'opération de paiement non autorisée effectuée depuis votre compte privé

Tout d'abord, l'article VII.43, § 1er, du CDE est applicable. Sur la base de cet article, la banque doit rembourser immédiatement à son client, à titre provisoire, le montant des opérations de paiement non autorisées, sauf si la banque a des motifs raisonnables de soupçonner une fraude dans le chef de son client et qu'elle a communiqué ces motifs par écrit au SPF Économie.

Dans le contexte de la fraude sur Internet, Ombudsfin constate que les banques procèdent très rarement à un remboursement provisoire, parce qu'elles souhaitent généralement aussi analyser l'application des règles de répartition de la responsabilité entre le client et la banque prévues à l'article VII.44 du CDE. L'application des règles de l'article VII.44 du CDE détermine définitivement dans quelle mesure la banque doit intervenir dans le dommage.

L'article VII.44, § 2, du CDE, particulièrement pertinent dans le présent dossier, dispose ce qui suit :

« § 2. ***Lorsque le prestataire de services de paiement du payeur n'exige pas une authentification forte du client, le payeur ne supporte aucune perte financière éventuelle, sauf si le payeur a agi frauduleusement.***

Lorsque l'authentification forte du client n'est pas acceptée par le bénéficiaire ou par le prestataire de services de paiement du bénéficiaire, le dommage financier

subi par le prestataire de services de paiement du payeur est indemnisé par celui-ci. » **(mise en évidence par nos soins)**

Dans le présent dossier, un fraudeur est parvenu, sur la base d'un seul code de réponse intercepté (généré au moyen de la carte bancaire, du code PIN et du lecteur de carte), à se connecter à la banque en ligne. L'accès à la banque en ligne était donc soumis à une authentification forte du client.

En règle générale, les banques doivent en outre prévoir une authentification forte du client lorsqu'un payeur :

- accède en ligne à son compte de paiement ;
- initie une opération de paiement électronique ;
- effectue, par un moyen de communication à distance, une opération susceptible de comporter un risque de fraude au paiement ou d'autres formes d'abus ou de fraude.

(voir les articles 47 et 145 de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique)

Des dérogations sont toutefois autorisées, pour autant qu'elles soient conformes au règlement délégué européen relatif à l'authentification forte du client.

La banque nous a expliqué, au cours du traitement du dossier, qu'en ce qui concerne le virement de votre compte privé vers le compte de la société, aucune authentification forte du client n'était requise :

« Lorsqu'un client souhaite effectuer des virements internes entre ses propres comptes et/ou des comptes pour lesquels il est connu comme mandataire, ces virements ne doivent pas être signés séparément. Dès lors qu'il s'agit de transferts internes, il n'y a pas non plus de perte pour le client. »

Ombudsfin estime que cette pratique est sujette à interprétation. Au cours du traitement du dossier, Ombudsfin a donc spécifiquement consulté son collège d'experts à ce sujet.

Le collège d'experts a rendu l'avis suivant :

« En ce qui concerne l'opération de 11.250 euros, il est constaté qu'elle a eu lieu sans authentification forte du client. Le virement de ce montant a en effet pu être effectué sans qu'un code secret doive être introduit. Le seul fait qu'une authentification forte du client ait été utilisée préalablement à l'exécution de l'opération afin d'accéder à l'environnement de banque en ligne ne suffit pas à considérer que l'opération de paiement elle-même a fait l'objet d'une authentification forte du client. Une session préalablement authentifiée peut certes fournir un élément de la SCA, mais il faut alors encore que l'autre élément soit présent lors du paiement lui-même et, pour les opérations de paiement à

distance, qu'il y ait un lien dynamique avec le montant concret et le bénéficiaire (https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4141). Si l'opération n'a pu être exécutée que parce que l'utilisateur se trouvait déjà dans l'environnement de banque en ligne, sans authentification supplémentaire propre à l'opération (comme le collège d'experts le déduit des données disponibles dans le dossier), le paiement a été exécuté sans authentification forte du client.

Dans ce cas, le payeur ne supporte, sur la base de l'article VII.44, § 2, CDE, aucune responsabilité pour cette opération non autorisée qui a eu lieu sans authentification forte du client. Cette règle particulière s'applique non seulement lorsque l'authentification forte du client est obligatoire en vertu du règlement délégué, mais également lorsque le règlement délégué relatif à l'authentification forte du client permet de ne pas recourir à une authentification forte du client. Nous relevons également à cet égard que l'exception prévue à l'article 15 pour les opérations entre comptes détenus par la même personne physique ou morale ne s'applique pas lorsque le titulaire du compte débité ne dispose que d'une procuration sur le compte bénéficiaire et n'en est pas le titulaire.

Dans le cas où l'exonération de responsabilité s'applique en raison de l'absence d'authentification forte du client, une éventuelle négligence grave dans le chef du payeur ne joue aucun rôle. Le prestataire de services de paiement doit dès lors, en l'espèce, créditer le compte privé du montant de 11.250 euros.

Compte tenu de la dérogation à l'article VII.44 CDE prévue dans les conditions bancaires en ce qui concerne le compte professionnel (compte au nom de la société), aucune responsabilité ne pèse sur le prestataire de services de paiement pour l'opération de 25.000 euros (qui a d'ailleurs bien fait l'objet d'une authentification forte du client). Ce montant ne doit donc pas être recrédité sur le compte professionnel. »

Sur la base de cet avis, nous avons demandé à la banque de revoir sa position initiale et de vous indemniser à concurrence de 11.250 euros.

La banque nous a communiqué qu'elle acceptait de procéder à l'indemnisation demandée à concurrence de 11.250 euros.

Afin de pouvoir procéder au remboursement, la banque vous soumettra une quittance. La banque prendra directement contact avec vous à ce sujet.

D. En ce qui concerne l'opération de paiement non autorisée effectuée depuis le compte de la société

Comme expliqué ci-dessus, les conditions générales bancaires de la banque prévoient que les titulaires de comptes qui ne sont pas des consommateurs ne peuvent pas se

prévaloir de certaines règles du régime de responsabilité objective en cas d'opérations de paiement non autorisées prévu à l'article VII.44 du CDE (en particulier les §§ 1er et 2).

Une exclusion du régime de responsabilité est en principe autorisée (voir l'article VII.29 du CDE), étant entendu que les clauses qui créent un déséquilibre manifeste entre les droits et obligations des parties pourraient être considérées comme abusives conformément à l'article 5.52 du nouveau Code civil, qui dispose comme suit :

> *« Toute clause non négociable qui crée un déséquilibre manifeste entre les droits et obligations des parties est abusive et réputée non écrite.*
>
> *Lors de l'appréciation du déséquilibre manifeste, il est tenu compte de toutes les circonstances entourant la conclusion du contrat.*
>
> *Le premier alinéa n'est applicable ni à la définition des prestations principales du contrat, ni à l'équivalence de ces prestations principales. »*

Cela implique qu'en ce qui concerne le préjudice financier résultant d'opérations contestées effectuées depuis un compte professionnel, Ombudsfin ne peut en principe pas appliquer le régime de responsabilité objective prévu par le CDE et doit se fonder sur le régime général de responsabilité applicable entre les parties. En résumé, cela signifie qu'une faute ou une négligence dans le chef de la banque doit être démontrée pour obtenir l'indemnisation du préjudice financier découlant de cette faute ou négligence. Nous relevons également à cet égard que la banque limite contractuellement sa responsabilité au dol ou à une faute lourde commise par la banque ou son personnel dans le cadre de ses activités professionnelles.

Dans ce contexte, nous avons examiné plus avant les obligations de la banque en matière (i) d'application de l'authentification forte du client, (ii) de détection de la fraude (la banque aurait-elle dû détecter elle-même la fraude plus rapidement ?) et (iii) de récupération (la banque a-t-elle, après que vous lui avez signalé la fraude, fait le nécessaire pour tenter de récupérer les fonds ?).

(i) En ce qui concerne l'authentification forte du client

Le virement effectué depuis le compte de la société vers le compte étranger en dehors de la zone SEPA à concurrence de 25.015 euros a été approuvé au moyen d'un code de réponse généré avec la carte bancaire, le code PIN et le lecteur de carte, et était donc soumis à une authentification forte du client.

Nous relevons toutefois, dans le présent dossier, qu'aucune authentification forte du client n'a été demandée pour les virements effectués depuis les comptes des ACP vers le compte de la société (tout comme pour le virement effectué depuis votre compte privé).

Or, la banque est tenue d'appliquer une authentification forte du client lors de l'initiation d'opérations de paiement ou lors de l'exécution, par un moyen de communication à

distance, d'une opération susceptible de comporter un risque de fraude au paiement ou d'autres formes d'abus ou de fraude (voir le cadre légal précité relatif à l'authentification forte du client).

Compte tenu de l'obligation légale d'appliquer une authentification forte du client, nous estimons que des questions peuvent être soulevées quant à la licéité de l'exclusion de l'article VII.44, § 2, du CDE dans les conditions générales bancaires de la banque.

Nous avons dès lors demandé à la banque si elle était disposée à formuler également une proposition d'intervention pour le préjudice financier restant résultant des opérations effectuées depuis les comptes des ACP. La banque n'a toutefois pas souhaité donner suite à cette demande.

(ii) En ce qui concerne l'obligation de détection de la fraude

Les banques doivent disposer de systèmes performants de prévention et de détection de la fraude afin de prévenir et d'arrêter les fraudes. Les transactions suspectes doivent être détectées et bloquées autant que possible. Cette obligation découle du règlement délégué européen 2018/389 relatif à l'authentification forte du client et s'inscrit dans la norme générale de prudence qui s'impose à chacun, et plus spécifiquement dans le devoir général de diligence de la banque à l'égard de ses clients.

Cette obligation de détection de la fraude dans le chef de la banque est une obligation de moyens. Cela signifie que la banque ne peut être tenue à un résultat consistant à détecter toute fraude dans chaque dossier individuel. Lors de la mise en place de systèmes de détection, les banques définissent des paramètres généraux afin de détecter autant que possible les fraudes, tout en procédant également à une mise en balance entre sécurité et facilité d'utilisation. Un outil de détection de la fraude ne peut jamais couvrir entièrement un risque de fraude lorsque le client effectue lui-même certaines confirmations.

Dans le présent dossier, nous n'avons pas constaté d'éléments suffisants pour mener une médiation auprès de la banque en vue d'une intervention fondée sur une éventuelle détection défaillante de la fraude.

(iii) En ce qui concerne les tentatives de récupération après notification de la fraude

Après la notification d'une fraude assortie d'une contestation d'opérations de paiement, la banque doit fournir des efforts raisonnables afin de récupérer les fonds des opérations de paiement contestées. Cela signifie qu'après la notification, la banque doit faire le nécessaire dans les plus brefs délais pour (i) bloquer, dans la mesure du possible, les opérations contestées, (ii) bloquer les éventuels comptes bénéficiaires auprès de la banque elle-même et (iii) envoyer un message à chaque institution financière bénéficiaire en lui demandant de bloquer les comptes bénéficiaires et de restituer les fonds éventuellement disponibles. Ces obligations de la banque s'inscrivent dans la norme

générale de prudence qui s'impose à chacun, et plus spécifiquement dans le devoir général de diligence de la banque à l'égard de ses clients.

La banque nous a indiqué, au cours de notre médiation, que les fonds relatifs au virement international avaient été transférés rapidement après la confirmation par la banque et qu'il n'était donc pas exact que le virement pouvait encore être bloqué.

Nous constatons toutefois que la banque n'a envoyé une demande de restitution à la banque du bénéficiaire que le lendemain, alors que la fraude était déjà connue le jour même, lorsque le client s'est présenté dans votre agence bancaire locale pour signaler la fraude.

Dans la pratique d'avis d'Ombudsfin, nous considérons qu'un délai de plus de 20 heures après la notification de la fraude est trop long pour lancer une tentative de récupération auprès de la banque du bénéficiaire. Nous l'avons soumis à la banque au cours de notre médiation et nous avons demandé à la banque d'intervenir dans le préjudice financier subi, au moins dans la mesure où des fonds étaient encore disponibles auprès des institutions financières bénéficiaires immédiatement après votre signalement de la fraude.

La banque n'a toutefois pas souhaité y donner suite et nous a communiqué ce qui suit :

> *« Nous ne sommes pas d'accord avec l'affirmation selon laquelle la banque aurait transmis son recall tardivement. En outre, une éventuelle demande plus rapide n'aurait pas non plus fait de différence, dès lors que la banque bénéficiaire se retranche derrière sa législation nationale, qui prévoit que le bénéficiaire doit confirmer son accord écrit pour un éventuel remboursement. Une demande encore plus rapide n'aurait pas davantage permis le remboursement. »*

En conclusion, bien que nous maintenions que l'intervention de la banque auprès de la banque bénéficiaire a été tardive, nous ne pouvons effectivement pas, compte tenu de l'absence de coopération obligatoire de la banque étrangère, démontrer l'existence d'un lien de causalité entre le lancement tardif de la tentative de récupération par la banque et votre préjudice financier.

Conclusion

Vous avez été victime d'une fraude commise par un fraudeur expérimenté. Dans ce contexte, vous avez sans aucun doute agi sous pression et possiblement sous l'effet d'une réaction de panique, en suivant les instructions téléphoniques d'un fraudeur.

Nous sommes heureux que la banque ait accepté de vous indemniser à concurrence du montant de 11.250 euros (à savoir le dommage subi sur votre compte privé).

Nous avons par ailleurs considéré qu'il existait une marge de médiation en ce qui concerne le préjudice financier restant résultant de l'opération de paiement non

autorisée effectuée depuis les comptes des ACP vers le compte de la société. Ainsi, nous estimions que l'absence d'application de l'authentification forte du client lors des virements effectués depuis les comptes des ACP vers le compte de la société pouvait être reprochée à la banque. La banque n'a toutefois pas souhaité suivre notre argumentation à ce sujet.