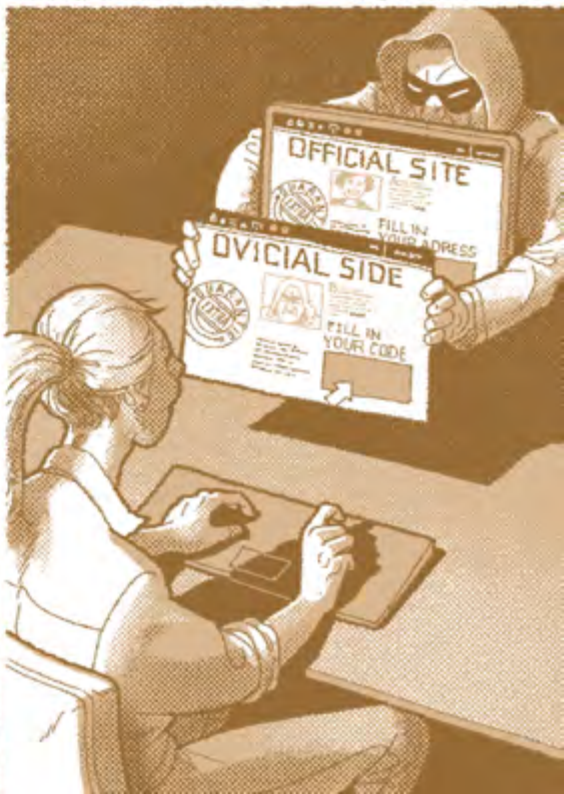
OMBUDSFIN

Rapport annuel 2022



Sommaire

AVANT-PROPOS 3

MISSION OMBUDSFIN 4

1

1. OMBUDSFIN EN CHIFFRES 6
1.1. Augmentation du nombre de demandes introduites 6
1.2. Qualification des demandes introduites 6
1.3. Délais de traitement des plaintes recevables 7
1.4. Interruption de la procédure de médiation 7
1.5. Les institutions financières concernées par les plaintes recevables 7

2

2. DEMANDES INTRODUITES PAR LES CONSOMMATEURS 8
2.1. Augmentation du nombre de demandes 8
2.2. Forte augmentation du nombre de plaintes recevables 8
2.3. Résultats des plaintes recevables de consommateurs clôturées en 2022 8
2.4. Recommandations individuelles 9
2.5. Collège d'experts 10
2.6. Thèmes des plaintes recevables des consommateurs 10
2.7.Un aperçu des sous-thèmes les plus importants 11

3

3. DEMANDES INTRODUITES PAR LES ENTREPRISES 14
3.1. Forte augmentation des dossiers introduites 14
3.2. Presque une réduction de moitié des plaintes recevables 14
3.3. Résultats des plaintes des entreprises clôturées en 2022 14
3.4. Thèmes des plaintes recevables des entreprises 14

4

4. DOSSIERS DE FRAUDE EN LIGNE 16
4.1. Opérations de paiement (non) autorisées 17
4.2. Obligation de remboursement immédiat 21
4.3. Partage de responsonsabilité en cas d'opérations de paiement non autorisées 23
4.4. Systèmes de détection des fraudes 36
4.5. Mesures visant à limiter le nombre ou le montant des fraudes 37
4.6. Recommandations 38

5

5. RUPTURE DE LA RELATION CLIENTELE 39

6

6. LIMITATIONS DES OPERATIONS EN ESPECES 39

7

7. PAIEMENTS – AUTRES PROBLEMATIQUES 40

8

8. LES GROUPES VULNÉRABLES 40

9

9. CREDITS 41

10

10. INVESTISSEMENTS 42

11

11. VARIA 44

12

12. FIN-NET : PLAINTES TRANSFRONTALIERES 46
12.1. Procédure 46
12.2. Exemples concrets 46

13

13. COLLABORATION 47
13.1. BELGIQUE 47
13.2. EUROPE 47
13.3. INTERNATIONAL 47

14

14. MOYENS FINANCIERS 48

AVANT-PROPOS

Mesdames et Messieurs,

Avec le printemps revient le temps des rapports annuels et Ombudsfin n'échappe pas à cette règle !

Comme vous pourrez le constater à la lecture du présent rapport, l'année 2022 a été à nouveau marquée par une augmentation des dossiers qui ont été soumis à notre examen. Une augmentation de 11.5 % pour les dossiers introduits et de 9 % pour les dossiers recevables.

Comme les années précédentes, les dossiers de fraude sont de loin les plus nombreux dont nous avons eu à connaître. Pas moins de 967 dossiers ont en effet été analysés par nos soins (contre 658 en 2021).

Force est toutefois de constater que les points de vue d'Ombudsfin et des institutions financières en cette matière ne se sont guère rapprochés en 2022, ces dernières continuant à invoquer la négligence grave du consommateur dans nombre de cas pour refuser d'intervenir, ce qui a conduit à une diminution globale du nombre de dossiers dans lesquelles une solution équilibrée a pu être trouvée.

Nous ne pouvons évidemment que regretter cette situation qui laisse nombre de citoyens désemparés et, souvent, dans une situation financière dramatique.

On ne peut certes reprocher aux établissements financiers de rester les bras croisés devant ce phénomène: les campagnes de sensibilisation se multiplient, certaines initiatives très concrètes voient le jour (mise au point d'une permanence téléphonique 24h/24 et 7j/7 ; envoi de SMS pour avertir les consommateurs de l'installation d'une application liée à leur compte...) mais les fraudeurs se professionnalisant toujours plus, ces améliorations sont malheureusement impuissantes à empêcher le phénomène de continuer à prendre de l'ampleur.

L'essentiel du présent rapport est consacré à cette problématique. Vous trouverez une analyse exhaustive des problèmes que nous rencontrons et du raisonnement que nous suivons pour régler les problèmes qui nous sont confiés.

Les autres thématiques, pour lesquelles il est heureusement beaucoup plus aisé d'arriver à une solution équilibrée (plus de 93% de succès), ne sont toutefois pas oubliées et vous pourrez prendre connaissance de certains problèmes qui ont été « à la mode » en cette année 2022.

Il me reste à vous souhaiter une bonne lecture de ce rapport annuel et à espérer que 2023 soit enfin une année de décrue et non une année de nouveaux records.

Jean Cattaruzza
Ombudsman

MISSION OMBUDSFIN

Ombudsfin est une entité qualifiée en vertu de l'article XVI.24 du Code de droit économique. Ombudsfin a pour objet de régler de manière extrajudiciaire les litiges entre les institutions financières et les consommateurs. Pour ce faire, elle fournit des conseils et des recommandations sur le litige en question et agit en qualité d'ombudsman.

Outre les litiges entre les institutions financières et les consommateurs, Ombudsfin peut également intervenir dans certains litiges entre les institutions financières et les entreprises. En offrant une résolution impartiale et efficace des litiges, Ombudsfin contribue à la confiance des consommateurs et des entreprises dans le secteur financier.

Qui peut introduire une plainte ?

Chaque client d'une institution financière ou d'un intermédiaire financier belge, agissant comme personne physique dans le cadre de ses intérêts privés, peut faire appel à Ombudsfin quand il n'a pas obtenu satisfaction.

Les entreprises peuvent aussi soumettre des plaintes à Ombudsfin. Il doit s'agir de plaintes dans le cadre de l'exécution d'un contrat de crédit, de plaintes en rapport avec un paiement transfrontalier d'un montant maximum de 50.000 €, de plaintes concernant MIFs (les frais d'interchange facturés dans le cas d'opérations de paiement par carte) ou le service bancaire de base pour les entreprises.

Comment introduire une plainte ?

La plainte doit être introduite par écrit, par la poste, par e-mail ou via le formulaire web sur le site www.ombudsfin.be et doit être formulée et documentée de façon claire et détaillée. Ombudsfin met à cette fin un cadre à disposition sur son site internet qui reprend les étapes à suivre.

Les documents peuvent être transmis :

Par courrier à l'adresse
Ombudsfin
North Gate II
Avenue du Roi Albert II n°8, boîte 2
1000 Bruxelles

Per e-mail
ombudsman@ombudsfin.be

En ligne sur
www.ombudsfin.be

Gratuit

La procédure chez Ombudsfin est gratuite pour le demandeur.

Conditions de recevabilité principales

- L'institution financière contre laquelle une plainte peut être introduite, doit être affiliée auprès d'Ombudsfin. La liste des institutions affiliées avec leurs services compétents est disponible sur le site.
- Le client a déjà introduit une plainte par écrit auprès du service compétent de l'institution financière et il n'a pas obtenu satisfaction ou n'a pas reçu une réponse dans un délai raisonnable (1 mois).
- La plainte a été introduite il y a moins d'un an auprès du service de plaintes compétent.
- Le litige n'est pas soumis au tribunal et il n'a pas encore fait l'objet d'une décision judiciaire. Le litige n'a pas non plus été traité par une autre entité qualifiée (ex. : ombudsman des assurances).
- Le litige ne vise pas à régler un surendettement. Ombudsfin ne fait pas de la médiation de dettes.

Vous trouverez un résumé de toutes les conditions de recevabilité dans notre Règlement de procédure, publié sur notre site web.

Comment se déroule le traitement d'un dossier recevable concrètement?

Ombudsfin envoie d'abord le dossier à l'institution financière pour s'informer de sa position dans l'affaire.

Si des informations complémentaires sont requises, contact est pris avec les parties concernées.

Après examen de la plainte et des négociations, l'ombudsman remet un avis.

Si le dossier remet en question un principe général ou si le dossier est plus complexe, celui-ci est soumis à l'avis d'un Collège d'experts.

Force obligatoire des avis

Excepté les avis concernant les services bancaires de base, les avis de l'ombudsman ne sont pas contraignants. Chaque partie reste libre de ne pas suivre cet avis et peut, le cas échéant, porter l'affaire devant un tribunal.

Collaborateurs et conseillers de l'ombudsman

Pour le traitement des demandes, l'ombudsman est entouré de 3 assistants et de 7 conseillers :

Assistants

Serge Henris, Christel Speltens et Ingrid Vertenten (partiellement conseiller).

Conseillers

Christine Buisseret, Vincent Chambeau, Jean Deschuijteneer, Bérengère de Crombrugghe, Brent De Waele, Elke Heymans et Aline Umwali.

Pour les dossiers complexes et de principe, l'ombudsman peut faire appel aux collèges d'experts suivants :

Collège d'experts

Le Collège est composé d'experts permanents indépendants. Composition du Collège d'experts en 2022 (jusqu'au 15 mars 2023): Françoise Sweerts (présidente), Nadine Spruyt (jusque fin juin 2022), Johan Vannerom, Reinhard Steennot, Alain Guigui, Philippe D'Haen, Piet François (à partir de septembre 2022).

La composition du Collège d'experts à partir de 15 mars 2023: Reinhard Steennot (président), Johan Vannerom, Alain Guigui, Philippe D'Haen, Piet François, Erik Van den Haute.

Collège d'experts pour les plaintes crédits aux entreprises

Ce Collège est composé d'une présidente indépendante et de 2 représentants des entreprises (Unizo, FEB) : Lieven Cloots et Arie Van Hoe et de 2 représentants du secteur financier : Luc Declercq et Wim Hendrickx.

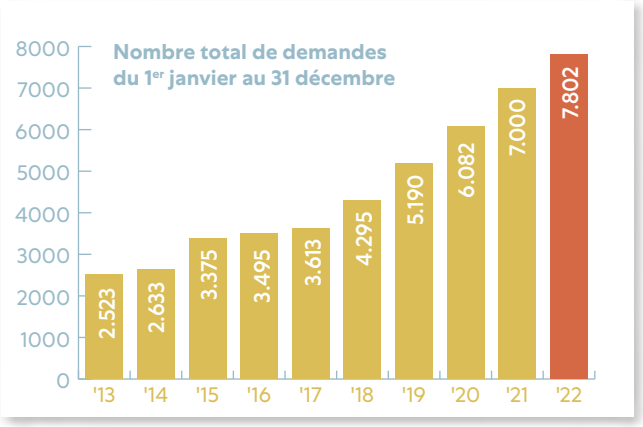
De gauche à droite : Bérengère de Crombrugghe, Serge Henris, Elke Heymans, Jean Deschuijteneer, Vincent Chambeau, Aline Umwali, Jean Cattaruzza, Ingrid Vertenten, Brent De Waele en Christine Buisseret. Non présente: Christel Speltens.

1. OMBUDSFIN EN CHIFFRES

1.1. Augmentation du nombre de demandes introduites

Le nombre total de demandes introduites par les consommateurs et les entreprises en 2022 s'élève à 7.802. Cela représente une augmentation de 802 dossiers (11,5%) par rapport à 2021.

Le tableau ci-dessous montre une augmentation soutenue depuis 2015, avec une accélération de cette tendance au cours des quatre dernières années.



Ces chiffres comprennent toutes les nouvelles demandes d'informations et les plaintes écrites qui ont été soumises à Ombudsfin en 2022.

Dans chacun de ces dossiers, le client a reçu d'Ombudsfin une réponse à sa demande ou s'est vu redirigé vers le service adéquat au cas où Ombudsfin n'était pas compétent pour agir.

1.2. Qualification des demandes introduites

1.2.1. Plainte ou demande d'information

Parmi les 7.802 nouvelles demandes introduites par les consommateurs et les entreprises, 7.616 concernaient une plainte et 186 étaient des demandes d'information.

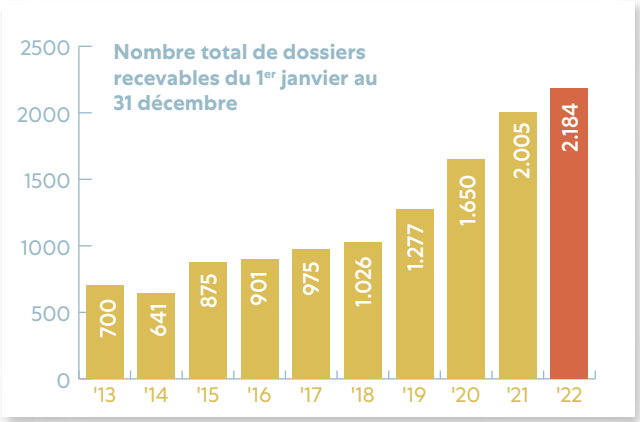
1.2.2. Plaintes recevables

Les plaintes recevables sont celles pour lesquelles Ombudsfin est l'entité qualifiée compétente et qui remplissent toutes les conditions de recevabilité.[1]

Pour chaque plainte recevable, l'ombudsman remet, après une analyse approfondie du dossier et des positions des parties et après médiation, un avis par lequel il communique le résultat de la médiation aux parties concernées. Dans certains dossiers, Ombudsfin émet également une recommandation (voir infra 2.4.).

En 2022, 7.616 plaintes ont été introduites.

Parmi ces plaintes, 2.033 (26,7 %) ont été déclarées recevables. Outre ces plaintes, 1 plainte supplémentaire de 2018, 3 plaintes de 2020 et 147 plaintes de 2021 ont été acceptées en 2022. Cela signifie qu'au total, 2.184 plaintes ont été déclarées recevables en 2022. Il s'agit d'une augmentation de 8,9 % (ou 179 plaintes) par rapport à 2021, où 2.005 plaintes avaient été acceptées.



[1] https://www.ombudsfin.be/fr/particuliers/introduire-une-plainte/proc%C3%A9dure/

1.2.3. Plaintes non recevables

Parmi les 7.616 plaintes reçues en 2022, 5.583 (soit 73,3%) ne répondaient pas aux critères de recevabilité. Les requérants ont toujours été informés de façon étendue quant aux raisons de l'impossibilité de traiter leur demande. Vous trouverez ci-dessous un récapitulatif des différentes raisons invoquées avec les nombres respectifs pour 2022, 2021 et 2020.

Raison	Nombre 2022	Nombre 2022	Nombre 2022
La plainte n'a pas encore été introduite auprès de l'institution financière en première ligne	3.922	3.560	3.092
Le client, l'institution ou l'objet de la demande n'est pas identifiable	519	489	515
Ombudsfin n'est pas compétent en la matière	798	671	604
L'institution financière n'est pas affiliée chez Ombudsfin (p.e. bureaux de recouvrement, institutions financières étrangères)	219	187	181
Combinaison de raisons mentionnées dans ce tableau	108	48	46
Procédure judiciaire ou demande déjà traitée par une entité qualifiée	3	7	8
Demande soumise il y a plus d'un an au service des plaintes de l'institution financière	14	6	9
Demande fantaisiste, vexatoire ou diffamatoire	0	0	0
Le traitement de la demande porterait sérieusement atteinte au bon fonctionnement d'Ombudsfin	0	0	2
TOTAL	**5.583**	**4.968**	**4.457**

Si un autre service était compétent ou si la première ligne de l'institution financière concernée n'avait pas encore été interpellée, les coordonnées du service compétent ont été transmises au requérant.

1.3. Délais de traitement des plaintes recevables

Le délai moyen de traitement de toutes les plaintes recevables, clôturées en 2022, est de 50,6 jours calendrier. En 2021, le délai moyen de traitement était de 48 jours calendrier.

Depuis juin 2015, Ombudsfin doit, en tant qu'entité qualifiée, traiter toutes les plaintes dans un délai de 90 jours calendrier. Ce délai peut être prolongé une seule fois d'une période équivalente, en raison de la complexité du dossier. En 2022, 189 dossiers ont été prolongés. Les parties ont été prévenues en temps utile de cette prolongation.

1.4. Interruption de la procédure de médiation

Au cours de la procédure de médiation, six dossiers ont été interrompus à la demande du plaignant. Dans un cas, le client souhaitait mettre un terme à sa relation avec la banque et cesser toute communication. Dans un autre cas, le problème avait déjà été résolu et dans un autre encore, le client souhaitait communiquer directement avec la banque. Dans les trois autres cas, aucune raison n'a été donnée pour arrêter le dossier.

1.5. Les institutions financières concernées par les plaintes recevables

Vous trouverez ci-dessous les catégories d'institutions financières concernées par les plaintes recevables en 2022, avec mention des chiffres et pourcentages respectifs.

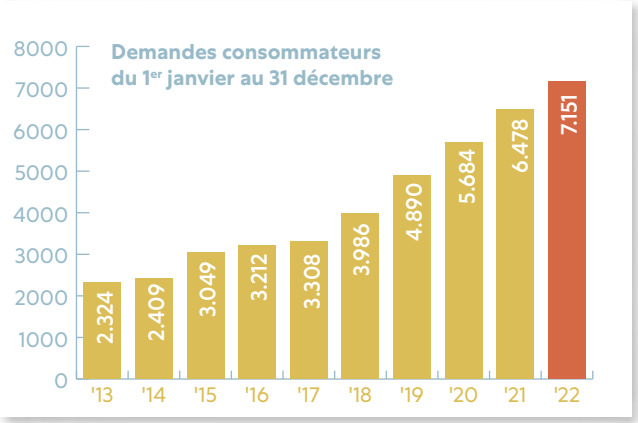
Banque	1.919	87,87%
Etablissement de paiement	141	6,46%
Société de crédit	70	3,21%
Etablissement de monnaie éléctronique	32	1,47%
Courtier de crédit	5	0,23%
Prêteur social	5	0,23%
Entreprise d'investissement	4	0,18%
Société de leasing	3	0,14%
Asset Management	2	0,09%
Compagnie d'assurances	2	0,09%
Société de bourse	1	0,05%
TOTAL	**2.184**	**100,00%**

2. DEMANDES INTRODUITES PAR LES CONSOMMATEURS

2.1. Augmentation du nombre de demandes

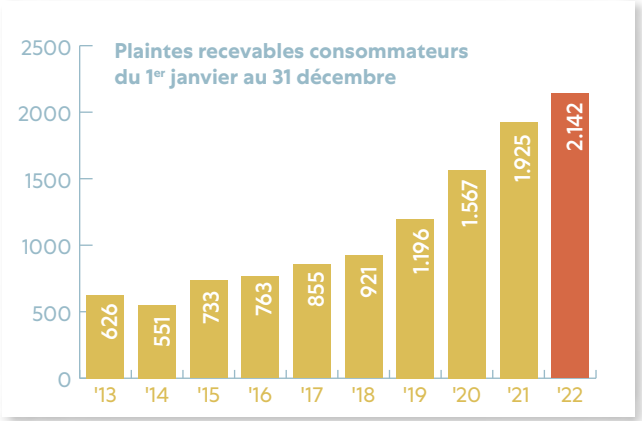
En 2022, Ombudsfin a reçu 7.151 demandes de consommateurs contre 6.478 en 2021, ce qui représente une augmentation de 673 dossiers (10,4%) par rapport à 2021.

7.042 demandes concernaient une plainte et 109 avaient trait à des demandes d'information.



2.2. Forte augmentation du nombre de plaintes recevables

En 2022, Ombudsfin a enregistré 2.142 demandes de consommateurs comme étant recevables (contre 1.925 en 2021), ce qui représente une augmentation de 217 dossiers (11,3%) par rapport à 2021.



2.3. Résultats des plaintes recevables de consommateurs clôturées en 2022

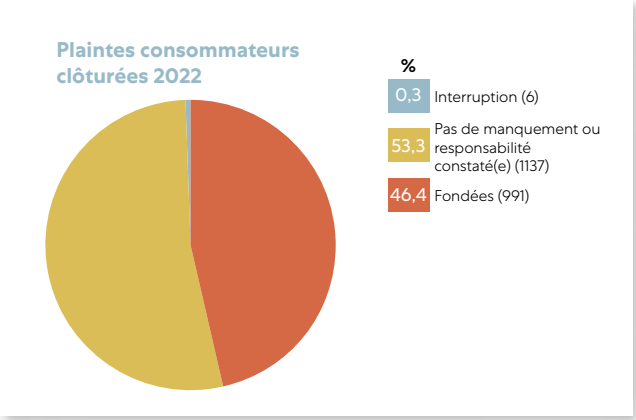
Ces résultats concernent toutes les plaintes des consommateurs réglées en 2022. Certaines plaintes introduites avant 2022 auprès d'Ombudsfin sont donc aussi incorporées dans ces résultats.

2.134 dossiers ont été clôturés.

Dans 46,4% des cas (soit 991 dossiers), Ombudsfin a considéré la plainte comme fondée sur la base de la législation, des dispositions contractuelles, des codes de conduite, des pratiques du marché, des codes déontologiques ou de tout autre élément utile à la résolution du conflit.

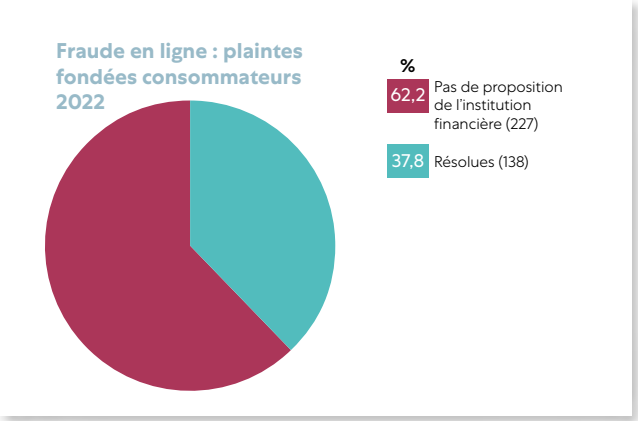
Dans 53,3% des cas (soit 1.137 dossiers), Ombudsfin n'a, en revanche, pas relevé de manquement ou de responsabilité dans le chef de l'institution financière. Dans ces dossiers, des informations et explications additionnelles nécessaires ont été données au client afin qu'il puisse comprendre pourquoi Ombudsfin était parvenu à cette conclusion et pourquoi une réparation, une information ou une indemnité de la part de l'institution financière ne pouvait être réclamée.

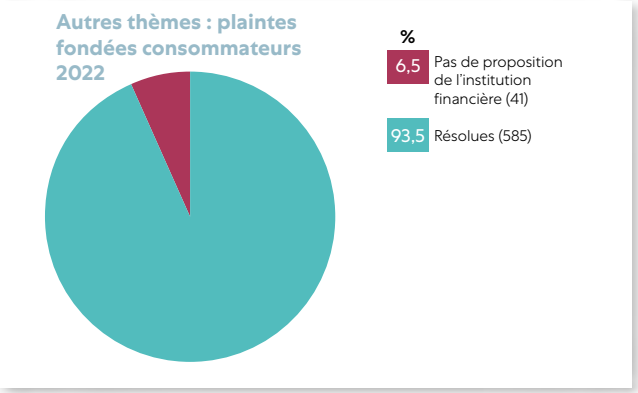
Dans 6 dossiers, la procédure de médiation a été interrompue par le consommateur (0,3%).



Des 991 plaintes considérées comme fondées par Ombudsfin, 73% (723 plaintes) ont été résolues. Ombudsfin regrette ce pourcentage historiquement bas.

Les graphiques suivants montrent que ce résultat est la conséquence directe des mauvais résultats dans les dossiers de fraude en ligne (phishing). Ils confirment également les bons résultats dans les dossiers portant sur d'autres thèmes :





Pour les dossiers de fraude en ligne, l'analyse de l'ombudsman ne coïncide en effet pas toujours avec celle des institutions financières. Le caractère autorisé ou non des opérations frauduleuses est quelquefois perçu différemment par la banque et par Ombudsfin mais c'est surtout au niveau de la preuve de la négligence grave dans le chef du consommateur que les opinions divergent.

Notre appréciation finale, qui aboutit ou non à une demande d'intervention dans le chef de la banque, repose sur l'analyse des éléments de fait et du degré d'implication du consommateur dans le processus de fraude (en particulier en cas de « phishing »).

2.4. Recommandations individuelles

Depuis juin 2015, le règlement de procédure d'Ombudsfin prévoit que l'ombudsman peut faire des recommandations individuelles aux institutions financières. Ombudsfin demande, dans ces cas-là, de réagir dans un délai de 30 jours à ces recommandations.

Ces recommandations portent sur une solution concrète limitée au cas examiné ou sont formulées dans un cadre plus large comme une adaptation des procédures, des conditions générales ou de la liste des tarifs.

En 2022, 36 recommandations individuelles ont été formulées.

Les institutions financières ont donné une suite favorable à 26 recommandations (72,2%). 9 recommandations (soit 25%) n'ont pas été suivies, l'institution en ayant expliqué les raisons. 1 recommandation (soit 2,8%) faisait encore l'objet d'une enquête plus approfondie de la part de l'institution financière au moment de la rédaction du présent rapport.

2.5. Collège d'experts[2]

Le Collège d'experts traite les questions de principe et les dossiers plus complexes.

En 2021, 4 dossiers ont été soumis au Collège dans les matières suivantes : crédit hypothécaire, compte à vue, vente de titres et succession.

3 des 4 dossiers (75%) soumis au Collège ont été considérés fondés.

Dans 2 de ces 3 dossiers (soit 66,7%), l'institution financière a proposé une solution à l'amiable. Dans l'autre dossier (soit 33,3%), l'institution financière n'a pas suivi l'avis du collège.[3]

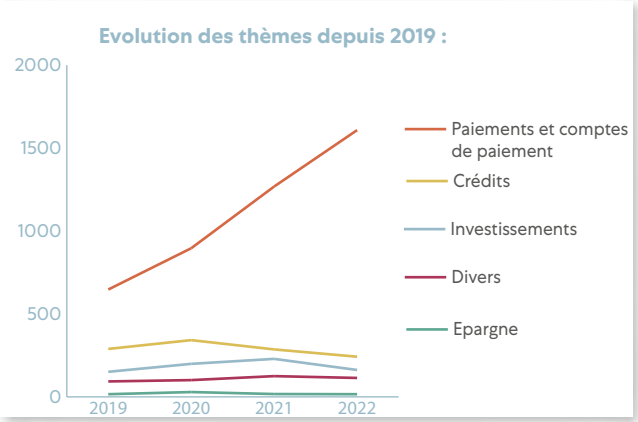
2.6. Thèmes des plaintes recevables des consommateurs

Les thèmes des plaintes recevables des consommateurs en 2022 étaient les suivants (évolution en nombre et en pourcentage depuis 2019) :

THEMES	2022	2021	2020	2019	2022	2021	2020	2019
	Nombre				%			
Paiements et comptes de paiement	1.608	1.268	896	647	75,07	65,87	57,18	54,10
Crédits, dont	242	286	342	289	11,30	14,86	21,83	24,16
Crédits à la consommation	88	133	142	159	4,11	6,91	9,06	13,29
Crédits hypothécaires	154	153	200	130	7,19	7,95	12,76	10,87
Investissements	162	229	199	151	7,56	11,90	12,70	12,63
Divers	114	125	101	93	5,32	6,49	6,45	7,78
Epargne	16	17	29	16	0,75	0,88	1,85	1,34
TOTAL	**2.142**	**1.925**	**1.567**	**1.196**	**100%**	**100%**	**100%**	**100%**

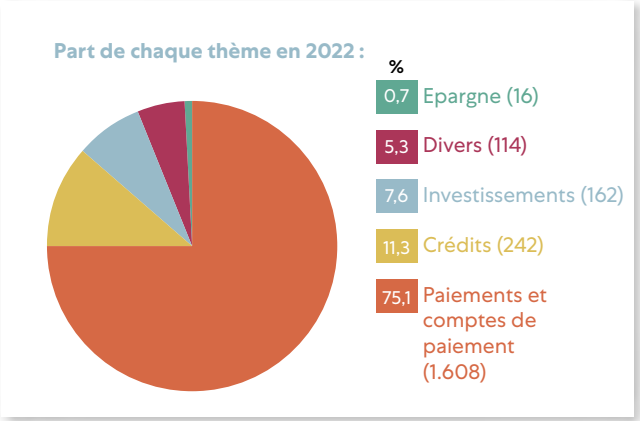
Le principal thème de 2022 est, comme dans les années précédentes, de loin « Paiements et comptes de paiement » avec 1.608 dossiers. Ce thème, en augmentation constante ces dernières années, représente donc désormais 75% des plaintes recevables. Il englobe notamment les cas de fraudes et de cessation des relations. Nous reviendrons plus loin en détail sur l'analyse d'Ombudsfin dans les cas de fraude.

Evolution des thèmes depuis 2019 :



[2] Composition du Collège, voir supra Mission Ombudsfin – Collaborateurs et conseillers de l'ombudsman
[3] L'institution financière concernée est la Banque Nagelmackers.

Part de chaque thème en 2022 :



2.7. Un aperçu des sous-thèmes les plus importants

2.7.1. Paiements et comptes de paiement

Paiements et comptes de paiement	Nombre de plaintes
Opérations via PC ou mobiles (contestées après phishing ou autre fraude)	967
Comptes à vue (résiliation, blocage, clôture)	226
Comptes à vue (généralités et tarification)	115
Paiements internationaux	102
Cartes (opérations contestées après vol, perte)	51
Opérations via PC ou mobiles (mal executées ou autres)	40
Cartes (généralités)	37
Guichets automatiques (Self)	23
Découverts sur compte (non-autorisé)	13
Mobilité bancaire	8
Service bancaire de base	8
Opérations guichet	6
Domiciliations et ordres permanents	5
Opérations de change	4
Chèques	3
TOTAL	**1.608**

L'aperçu des sous-thèmes est éloquent. La contestation d'opérations à la suite d'un phishing ou d'une autre fraude (à l'exclusion des investment scam) constitue le thème le plus important traité par Ombudsfin. Avec 967 dossiers, ce thème représente 45,1 % du nombre total de plaintes de consommateurs recevables.

Le blocage et la résiliation/clôture des comptes courants restent également un thème important avec 226 dossiers, soit 10,6 % du nombre total de plaintes de consommateurs recevables.

Le service bancaire de base pour les consommateurs

La législation qui régit le service bancaire de base se trouve au Chapitre 8, « Accès aux comptes de paiement et service bancaire de base », Section 1, Livre VII du Code de Droit Économique.

Ombudsfin est l'organisme compétent pour traiter une procédure de plainte et d'appel extrajudiciaire. À noter qu'Ombudsfin a une compétence contraignante en cette matière. En 2022, Ombudsfin a reçu 8 plaintes concernant le service bancaire de base.

Les établissements de crédit fournissent chaque année à Ombudsfin les statistiques sur le nombre de comptes ouverts, de refus et de résiliations, ainsi que leur motivation.

Ci-dessous, les chiffres pour l'année 2022 :

Statistiques Service bancaire de base (SBB)	2022
Nombre de banques ayant enregistré une demande de SBB	13
Nombre de comptes SBB ouverts	42.672
Nombre total de comptes SBB existants	68.753
Nombre de refus d'ouverture d'un compte SBB	10
Nombre de comptes SBB résiliés(*)	5.886

(*) Ceci inclut les comptes SBB qui sont transformés en comptes à vue réguliers

En 2022, 13 banques ont enregistré des demandes de services bancaires de base, soit 2 de plus qu'en 2021.
Le nombre de services bancaires de base ouverts en 2022 a augmenté de 234 % pour atteindre 46.672. En 2021, il n'y avait eu que 12.771 ouvertures de tels comptes.

Cette augmentation importante est principalement due à l'ouverture des services bancaires de base par les réfugiés ukrainiens.

En 2022, 10 demandes d'ouverture de services bancaires de base ont été refusées en raison d'antécédents négatifs auprès de la banque (80%) et du fait que le demandeur était déjà titulaire d'un compte à vue (20%).

La principale raison d'une fermeture est la demande du titulaire (98,81%), suivi par :

- Compte courant dans une autre institution (1,4%)
- Autres produits non compatibles avec le service bancaire de base (1,13%)
- Antécédents négatifs à la banque (0,53%)
- Autres comptes supérieur à 6.000 euros (0,13%)

2.7.2. Crédits

2.7.2.1. Crédits hypothécaires

Crédits hypothécaires	Nombre de plaintes
Exécution du contrat	82
Formation du contrat	58
Désolidarisation	5
Conditions générales (autres)	5
Crédit pont	2
Mandat hypothécaire	1
Sûretés	1
Publicité	0
Total	**154**

La plupart des plaintes concernant les crédits hypothécaires se situent dans le cadre de l'exécution du crédit (82 dossiers). Le motif de la plainte est souvent le taux annuel effectif global (TAEG) (20 dossiers) et les problèmes de remboursement (16 dossiers).

Les dossiers relatifs à la conclusion du contrat (58 dossiers) concernent souvent le déroulement de la procédure d'octroi (18 dossiers) et un refus de crédit (13 dossiers).

2.7.2.2. Crédits à la consommation

Crédits à la consommation	Nombre de plaintes
Exécution du contrat	61
Formation du contrat	22
Conditions générales (autres)	4
Publicité	1
Total	**88**

La plupart des plaintes relatives aux crédits à la consommation concernaient l'exécution du crédit (61 dossiers). Le motif de la plainte est souvent un signalement négatif à la Banque Nationale de Belgique (21 dossiers) ou des problèmes de remboursement (11 dossiers).

Les dossiers concernant la conclusion du contrat (22 dossiers) impliquent souvent un refus de crédit (8 dossiers).

2.7.3. Investissements

Investissements	Nombre de plaintes
Comptes titres	44
Investment scam	40
Achat et vente de titres (execution only)	29
Aspects fiscaux	13
Fonds de pension/épargne-pension	10
Conseil et placement	9
Divers	7
Corporate action	6
Publicité et information à la souscription	3
Gestion de fortune	1
Financial planning	0
Information sur tarif/coûts	0
Total	**162**

La plupart des plaintes concernant les investissements portent sur un compte-titres (44 dossiers) et sur les *investment scams* (40 dossiers).

2.7.4. Divers

Divers	Nombre de plaintes
Successions	49
Garantie locative (aussi compte d'épargne)	24
Produits d'épargne	16
Know Your Customer	9
Coffres	8
Divers	8
Incapacité (mineur)	7
Privacy	5
Discrimination	4
Fraude employé	0
Total	**130**

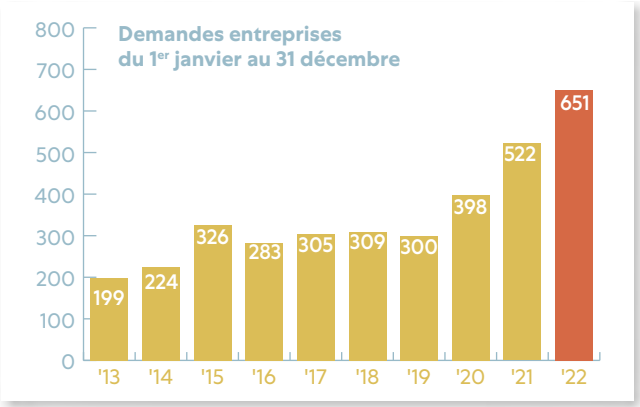
Les thèmes majeurs restent, comme les années précédentes, les successions (49 dossiers) et les garanties locatives (24 dossiers). Ces thèmes seront brièvement abordés dans ce rapport.

3. DEMANDES INTRODUITES PAR LES ENTREPRISES

3.1. Forte augmentation des dossiers introduits

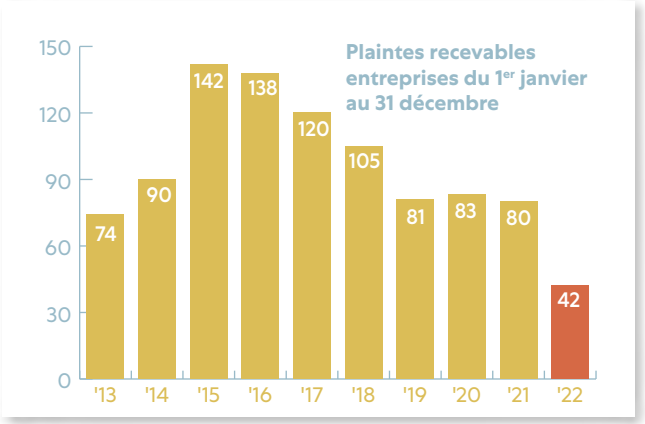
En 2022, Ombudsfin a reçu un total de 651 demandes écrites d'entreprises, contre 552 en 2021. Cela représente une augmentation de 129 dossiers (24,7%). Cette évolution est partiellement le résultat des nombreuses questions d'information qui ont été posées concernant le service bancaire de base pour les entreprises. Bien qu'elle soit en vigueur depuis mai 2021, la loi n'était toujours pas effective en 2022.[4] On observe également que de nombreuses plaintes sont introduites pour des problèmes qui ne ressortent pas de la compétence d'Ombudsfin.

574 demandes concernaient une plainte, tandis que 77 demandes concernaient une demande d'information.



3.2. Presque une réduction de moitié des plaintes recevables

En 2022, Ombudsfin a enregistré 42 demandes d'entreprises comme plaintes recevables, contre 80 demandes en 2021, ce qui représente presque une réduction de moitié (38 dossiers en moins, soit une diminution de 47,5 %). C'est une évolution historique. Jamais au cours des dernières années un chiffre aussi bas n'avait été enregistré.

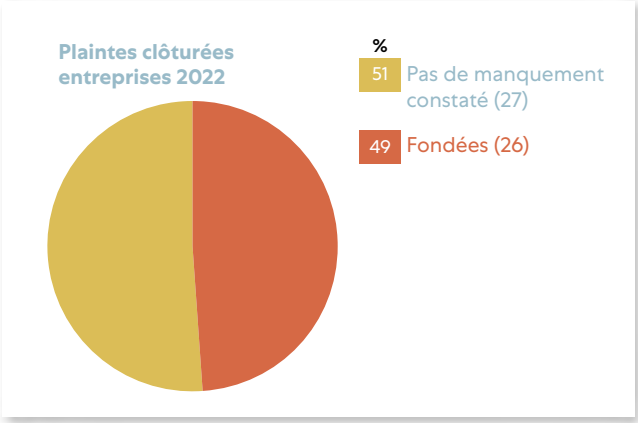


3.3. Résultats des plaintes des entreprises clôturées en 2022

Les résultats dont question ci-dessous concernent toutes les plaintes des entreprises qui ont été traitées et clôturées en 2022. Ces résultats comprennent également certaines plaintes qui avaient déjà été soumises à Ombudsfin en 2021, mais qui n'ont été traitées et clôturées qu'en 2022.

Au total, il s'agit de 53 dossiers.

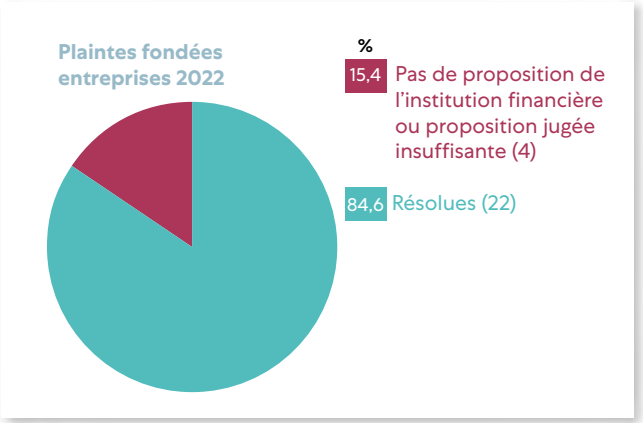
Dans 26 dossiers (soit 49,1%), Ombudsfin a estimé que la plainte était fondée sur la base de la législation, des clauses contractuelles, des codes de conduite ou des pratiques du marché.



[4] Suite à la publication de l'arrêté royal et de l'arrêté ministériel, les procédures auprès de la chambre du service bancaire de base peuvent désormais être menées. Pour de plus amples informations : https://economie.fgov.be/fr/themes/services-financiers/services-de-paiement/service-bancaire-de-base/service-bancaire-de-base-pour-0

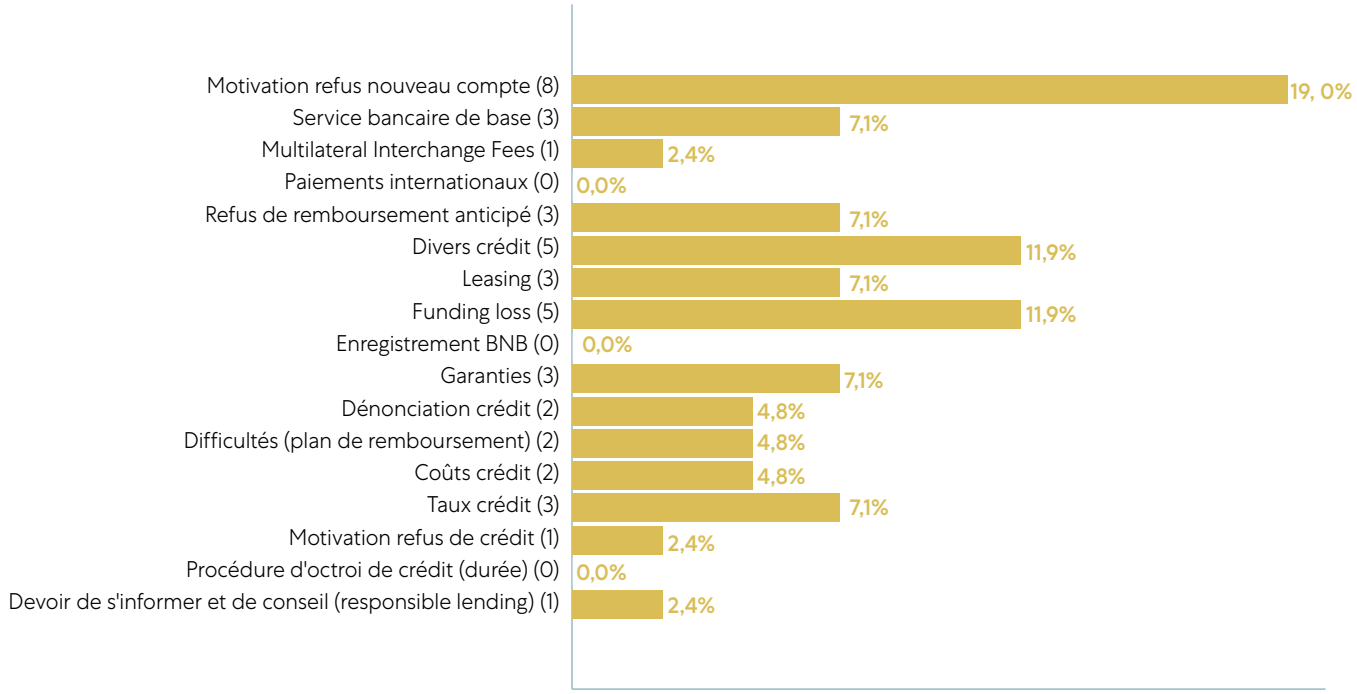
Dans 27 dossiers (soit 50,9%), Ombudsfin n'a décelé aucune faute dans le chef de l'institution financière. Dans ces dossiers, les explications nécessaires ont été données à l'entreprise afin qu'elle puisse comprendre pourquoi Ombudsfin a pris cette décision et pourquoi aucune correction ou compensation ne pouvait être demandée à l'institution financière.

Dans les 26 dossiers qui ont été considérés comme fondés, Ombudsfin a poursuivi les négociations. Dans 22 dossiers (84,6% des plaintes fondées), cela a conduit à un règlement à l'amiable. En revanche, aucune solution n'a été trouvée dans 4 dossiers (15,4%).



3.4. Thèmes des plaintes recevables des entreprises

En 2022, les plaintes concernaient les thèmes suivants:



4. DOSSIERS DE FRAUDE SUR INTERNET : Dans quels cas les établissements financiers doivent-ils intervenir dans le dommage subi par leurs clients ?

INTRODUCTION

La fraude sur Internet n'a jamais suscité autant d'attention médiatique que ces dernières années. Safeonweb, Febelfin, les institutions financières et d'autres organismes multiplient les campagnes de sensibilisation pour diminuer ce type de fraude. Les institutions financières déploient par ailleurs des mesures toujours plus nombreuses et ne cessent d'adapter leurs processus de paiement, entre autres, afin d'endiguer autant que possible la fraude sur Internet. Cela n'a toutefois rien de surprenant, étant donné l'omniprésence du phishing et de la fraude sur Internet en général à l'heure actuelle. Les Belges n'ayant encore jamais reçu de messages de phishing ou d'appels téléphoniques d'un fraudeur deviennent, hélas, de plus en plus rares. Les fraudeurs sont en outre de plus en plus professionnels et ingénieux, adaptant leurs scénarios à l'actualité et aux systèmes de paiement des différentes institutions financières.

Cette évolution est évidemment liée à la numérisation toujours plus poussée des services bancaires. On peut aussi l'observer dans les statistiques annuelles d'Ombudsfin.

Le nombre de dossiers de fraude sur internet traités par Ombudsfin n'a cessé d'augmenter ces dernières années. En 2019, Ombudsfin a examiné 221 dossiers de ce type, (soit 18,5% du nombre total de dossiers traités), alors que ce chiffre s'est élevé à 393 dossiers en 2020 (25,1% du total) et à 658 dossiers en 2021 (34,2% du total). En 2022, la plus grande partie des cas traités par Ombudsfin a porté sur la contestation d'opérations frauduleuses : 1.018 dossiers sur les 2.142 considérés comme recevables. 51 de ces dossiers concernaient la contestation d'opérations frauduleuses avec utilisation de la carte physique et 967 dossiers (soit 45,1% du nombre total de dossiers recevables) concernaient des fraudes sur Internet.

Compte tenu de l'importance de ce phénomène, il nous a paru utile de reprendre dans ce rapport annuel l'ensemble du raisonnement suivi par Ombudsfin dans les dossiers de fraude en ligne en ce qui concerne la réglementation relative à la répartition des responsabilités en cas d'opérations de paiement non autorisées, comme le prévoit le Livre VII du Code de droit économique (ci-après CDE). Notre point de vue, tel qu'exposé dans notre rapport annuel de 2019, a en effet évolué depuis, notamment au regard de la doctrine et de la jurisprudence récentes. Nous nous pencherons également sur les différents contre-arguments des institutions financières, auxquels Ombudsfin est confronté dans sa mission de médiation, et mentionnerons différents exemples illustrant des techniques de fraude pertinentes. Enfin, nous examinerons un certain nombre d'évolutions

(potentielles) et formulerons quelques recommandations générales à l'adresse des consommateurs et de l'industrie.

Avant d'entamer cet exposé juridique, nous allons brièvement passer en revue les résultats obtenus suite aux médiations effectuées en 2022 dans le cadre de dossiers de fraude, ainsi que les scénarios mis en œuvre par les fraudeurs :

Résultats des médiations : À l'instar des années précédentes, Ombudsfin constate que les résultats des médiations effectuées dans le cadre de dossiers de fraude sont loin d'être satisfaisants. En effet, nous ne sommes parvenus à une médiation positive que dans 38 % (138 dossiers) des dossiers de fraude en ligne considérés comme fondés. La faiblesse de ce pourcentage est due au fait que l'éventuelle obligation légale des banques d'intervenir dans les dommages résultant d'opérations de paiement non autorisées dépend de la mesure dans laquelle la victime pouvait détecter la fraude à l'avance ainsi que de l'évaluation de la négligence grave dans le chef de la victime (cf. infra). Ces deux critères exigent la prise en compte de toutes les circonstances factuelles. Nous constatons qu'actuellement, les banques évaluent souvent les faits d'une autre manière qu'Ombudsfin. Les discussions liées à ces dossiers portent essentiellement sur la question de savoir si le client a fait preuve ou non de négligence grave. Ombudsfin constate que les banques appliquent une définition très large de ce concept.

Il convient toutefois de préciser que tous les dossiers de fraude sur Internet ne sont pas considérés comme fondés. Dans certains dossiers, nous retenons également la négligence grave tandis que, dans d'autres, nous ne sommes pas en mesure de formuler d'opinion concrète car nous ne connaissons pas suffisamment les circonstances effectives de la fraude. En 2022, nous avons ainsi clôturés 549 dossiers de fraude sur Internet (60% du nombre total) comme non fondés et 365 (40%) comme fondés.

Typologie : Ombudsfin constate, d'une manière générale, que les scénarios déployés par les fraudeurs demeurent identiques. En 2022, Ombudsfin a encore traité de nombreux dossiers dans lesquels les fraudeurs avaient approché les victimes par phishing via e-mail ou SMS ou à la suite d'un achat ou d'une vente via un site de petites annonces, ont renvoyé les victimes à un faux site Web de leur banque auquel elles ont tenté de se connecter ou ont contacté les victimes par téléphone dans des cas de fraude aux comptes « à sécurité renforcée », etc. Si les techniques et scénarios mis en œuvre sont demeurés identiques, ils ont toutefois été affinés et adaptés à l'actualité (par exemple l'obtention d'une prime d'énergie) ainsi qu'aux éventuels ajustements apportés par l'institution financière dans les processus de paiement et aux procédures d'installation des applications bancaires mobiles, par exemple. Pour des conseils et mises en garde concernant les scénarios de fraude les plus courants, nous vous renvoyons à www.safeonweb.be.

4.1. Opérations de paiement (non) autorisées

4.1.1. Définition d'une opération de paiement autorisée

Le livre VII du CDE prévoit un régime de responsabilité pour les opérations de paiement non autorisées. Avant de pouvoir appliquer ces règles, il faut logiquement vérifier si une opération de paiement contestée par le payeur peut être considérée comme autorisée ou non. En effet, ce n'est pas parce qu'il y a fraude en matière de paiement qu'il y a automatiquement opération de paiement non autorisée.

Le CDE stipule qu'une opération de paiement n'est réputée autorisée que si le payeur a consenti à l'exécution de l'ordre de paiement. En l'absence de ce consentement, l'opération de paiement est réputée non autorisée. L'exposé des motifs de la loi dispose qu'il ne peut être question d'une opération de paiement autorisée que si le payeur y a **explicitement** consenti.

Bien que la distinction entre opérations de paiement autorisées et non autorisées semble relativement simple, elle soulève cependant diverses discussions dans la pratique. Ces débats portent essentiellement sur l'interprétation de la notion de « consentement ». Avant d'aborder ce point, il nous paraît toutefois utile de nous pencher sur le régime de la preuve tel qu'il figure à l'article VII.42 du CDE.

4.1.2. Charge de la preuve : l'opération a-t-elle été autorisée ou non ?

L'article VII.42 du CDE définit la charge de la preuve concernant le caractère autorisé ou non autorisé d'une opération contestée. Ainsi, il stipule que lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe au prestataire de services de paiement de prouver que cette opération a été authentifiée, dûment enregistrée et comptabilisée, et qu'elle n'a pas été affectée par une déficience technique ou autre du service fourni par le prestataire de services de paiement. Si ce dernier ne peut fournir ces preuves techniques, l'utilisateur des services de paiement ne pourra pas être tenu responsable.

Par ailleurs, l'article VII.42 du CDE stipule que l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, ne suffit pas nécessairement à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent. Par conséquent, si le prestataire de services de paiement fournit les preuves mentionnées à l'article VII.42, §1 alinéa 1 du CDE, cela n'implique pas automatiquement que l'opération contestée doit être considérée comme autorisée.

L'utilisation des termes « pas nécessairement » a pour corollaire que, dans certains cas, l'enregistrement de l'utilisation de l'instrument de paiement peut constituer une preuve suffisante du caractère autorisé de l'opération contestée, mais ce n'est pas toujours et pas automatiquement le cas. Une fois que le prestataire de services de paiement a fourni les preuves susmentionnées, le payeur doit démontrer de manière plausible qu'il n'a pas consenti sciemment à l'opération. Le payeur ne doit donc pas en fournir la preuve absolue. Si le payeur peut démontrer de manière plausible qu'il n'a pas consenti à l'opération contestée, le prestataire de services de paiement ne peut plus se limiter au fait que l'utilisation de l'instrument (et du code secret correspondant) a été enregistrée pour prouver que l'opération a été autorisée. Si le payeur ne parvient pas à rendre cette hypothèse plausible, les preuves techniques constituent une preuve suffisante que l'opération a été autorisée.

Pour le payeur, la meilleure façon de démontrer de manière plausible qu'il n'a pas consenti à l'/aux opérations contestées consiste à fournir un compte rendu détaillé de la fraude (modus operandi du fraudeur). Dans certains cas, le caractère non autorisé des opérations contestées peut être rendu plausible par le dépôt d'une plainte auprès de la police, par certaines circonstances rendant impossible l'exécution des opérations contestées par le payeur, ou par la nature, l'ampleur ou la succession des opérations contestées, etc.

En pratique, Ombudsfin traite souvent des dossiers où un payeur conteste une ou plusieurs opérations, dont l'institution financière peut prouver qu'elles ont été correctement authentifiées (par exemple au moyen d'un code généré avec une carte bancaire, un code PIN et un digipass[5] ou via une application mobile nouvellement installée et liée aux comptes de la victime), mais pour lesquelles le plaignant ne peut fournir la moindre information quant au processus de fraude. Ombudsfin peut alors considérer, en fonction des circonstances concrètes du dossier, que le plaignant ne rend pas suffisamment plausible le fait qu'il n'a pas consenti à l'/aux opération(s) contestée(s), de sorte que les preuves techniques fournies par l'institution financière seront suffisantes pour conclure qu'il est question d'opération(s) de paiement autorisée(s).

[5] Ce terme englobe à la fois le digipass et le lecteur de carte bancaire. Le présent document n'établit aucune distinction entre un digipass et un lecteur de carte, et utilise donc indifféremment les deux termes.

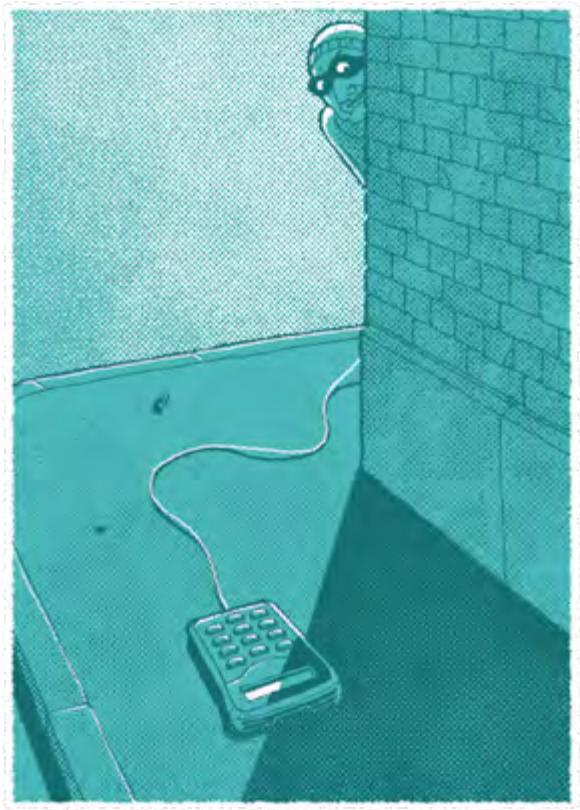
4.1.3. Consentement subjectif ou objectif ? Autorisation ≠ authentification

4.1.3.1. Point de vue d'Ombudsfin

Ombudsfin applique le principe du consentement explicite subjectif. D'après Ombudsfin, il ne peut être question d'une opération de paiement autorisée que si le payeur y a librement et sciemment consenti. Cela signifie qu'Ombudsfin ne considérera une opération comme autorisée que si, au moment du paiement, le payeur connaît le montant et le bénéficiaire ou l'objet de l'opération.

Le principe du consentement explicite subjectif s'explique mieux par le biais de quelques exemples. Ainsi, de nombreux cas de whaling (phishing via un réseau social) impliquent clairement des opérations de paiement autorisées. Dans ce type de fraude, les fraudeurs envoient un message à leur victime, (généralement) via WhatsApp, en se faisant passer pour un membre de sa famille. Ils prétendent que leur téléphone portable est hors d'usage et qu'ils ont donc un nouveau numéro de téléphone. Après une brève conversation avec la victime, le fraudeur lui demande ensuite d'effectuer plusieurs virements pour lui. Dans ce cas, la victime effectue elle-même les virements via son propre système bancaire en ligne ou son application mobile, de sorte qu'il est clairement question d'opérations de paiement autorisées. Le motif de l'opération (le fait que l'on pensait effectuer une opération à la demande d'un membre de la famille) n'est pas pertinent en l'occurrence.

Un deuxième exemple concerne les cas de phishing ou de smishing (SMS + phishing) où la victime reçoit un e-mail ou un message concernant par exemple un nouveau digipass qui peut prétendument être demandé via un lien en annexe, ou signalant que le compte itsme de la victime a été bloqué et demandant de le débloquer via un lien en annexe. Dans ces cas, la victime clique sur le lien concerné dans le message frauduleux et aboutit sur un faux site



Web contrôlé par le fraudeur. Elle sera alors invitée à saisir certaines coordonnées bancaires, à effectuer des opérations avec sa carte bancaire et son digipass, et à saisir les codes de réponse ainsi générés, prétendument pour confirmer la demande du nouveau digipass ou le déblocage du compte itsme. Comme le fraudeur a le contrôle du faux site Web, il parvient à intercepter les données saisies. Il utilise ensuite les codes interceptés, par exemple, pour confirmer des paiements sur le site Web d'un commerçant ou pour installer une application mobile liée aux comptes de sa victime puis utiliser cette application pour confirmer des virements ou des paiements. Selon le point de vue d'Ombudsfin, ces cas de figure impliquent toujours des opérations de paiement non autorisées. La victime pensait en effet que ses actions allaient confirmer la demande d'un nouveau digipass ou le déblocage de son compte itsme. Elle ignorait qu'elles allaient permettre de confirmer des paiements ou permettre à un tiers d'installer une application mobile qui pourrait ensuite être utilisée pour confirmer des opérations.

4.1.3.2. Point de vue de certaines institutions financières et d'une partie de la doctrine juridique

a) Autorisation = authentification

Malgré les termes clairs de la loi, Ombudsfin constate que plusieurs institutions financières assimilent encore autorisation et authentification. Après avoir fourni la preuve d'une authentification correcte, conformément au régime de preuve évoqué ci-dessus, les institutions concernées concluent qu'il est question d'une opération de paiement autorisée et que les règles relatives aux opérations de paiement non autorisées ne s'appliquent donc pas, de sorte qu'elles ne sont pas tenues de créditer provisoirement le compte de paiement de la victime et estiment qu'elles ne doivent pas procéder à une analyse plus approfondie du dossier, par exemple pour évaluer une éventuelle négligence grave.

Les institutions financières concernées invoquent généralement l'article VII.32, §2, alinéa 1 du CDE, sur la base duquel le consentement à l'exécution d'une opération de paiement ou d'une série d'opérations de paiement est donné sous la forme convenue entre le payeur et le prestataire de services de paiement et conformément à la procédure convenue. Après avoir apporté la preuve du respect de la procédure et de la forme convenues dans les règlements de l'institution (exécution des achats sur Internet au moyen d'un digipass, d'une carte bancaire, de la saisie d'un code PIN et de la génération de codes de réponse, par exemple), les institutions financières concernées estiment avoir apporté la preuve du caractère autorisé des opérations contestées.

Ombudsfin estime toutefois que ces institutions financières invoquent à tort l'article VII.32 du CDE lorsqu'elles affirment que, si le fraudeur a respecté la procédure convenue, le titulaire de l'instrument de paiement a consenti à l'opération. En effet, selon Ombudsfin, le seul but de cette disposition est de faire en sorte qu'une opération ne puisse être consentie que via la procédure convenue. Elle ne stipule pas que le payeur a automatiquement accepté l'opération en question si la procédure convenue a été respectée. C'est d'ailleurs logique : ce n'est pas parce que les moyens d'accès de l'utilisateur des services de paiement ont été utilisés que ce dernier a effectivement autorisé l'opération.

De plus, cette affirmation en vertu de laquelle une opération est automatiquement réputée autorisée dès que la procédure convenue a été respectée est incompatible avec le libellé de l'article VII.42, §2, alinéa 1 du CDE, qui stipule que l'utilisation de l'instrument de paiement ne constitue pas nécessairement une preuve suffisante que le payeur a autorisé l'opération. Une telle interprétation de la loi, dans laquelle l'autorisation serait pleinement équivalente à l'authentification, éroderait en effet presque totalement la protection que les législateurs européens et belges ont voulu offrir au payeur. En effet, son application impliquerait des opérations de paiement autorisées dans chacun des exemples évoqués à la section précédente.

b) Consentement technique

Certains auteurs modèrent la position ci-dessus en adoptant la théorie du consentement objectif explicite, également qualifié de technique. Ces auteurs soutiennent que s'il peut être démontré que l'authentification a été effectuée par le titulaire légitime de la carte, l'opération de paiement est réputée autorisée. D'après ces auteurs, le respect de la procédure de paiement stipulée devrait donc suffire pour qu'il soit question d'un paiement autorisé, à condition qu'elle soit effectuée par le titulaire légitime de la carte. Ce raisonnement ne tient pas compte de l'intention du payeur, de la question de savoir s'il a effectivement consenti au résultat du paiement.

Selon la thèse de ces auteurs, la manière dont l'authentification a eu lieu devra toujours être prise en considération. Ainsi, si un fraudeur effectue par exemple des paiements directement sur le site Web d'un commerçant en utilisant des codes de réponse générés par la victime à l'aide du digipass puis interceptés via un e-mail de phishing, les opérations de paiement seront réputées autorisées. En effet, la procédure d'authentification, c'est-à-dire le calcul des codes de réponse à l'aide du digipass, aura été effectuée par le titulaire légitime de la carte. En revanche, si le fraudeur utilise les codes interceptés, par exemple, pour installer une application mobile liée aux comptes de la victime et qu'il se sert ensuite de cette application pour effectuer les opérations contestées (sans que la victime doive entreprendre des démarches supplémentaires), ces auteurs considèrent les opérations de paiement comme non autorisées. Dans ce cas, en effet,

le processus d'authentification - c'est-à-dire la confirmation des opérations via l'application - aura été réalisé par le fraudeur.

4.1.3.3. Point de vue de la jurisprudence

Dans un arrêt du 21 mai 2021, la Cour suprême des Pays-Bas, organe similaire à la Cour de cassation belge, a explicitement jugé que la circonstance selon laquelle les ordres de paiement contestés ont été émis conformément à la forme et à la procédure convenues entre le payeur et le prestataire de services de paiement n'empêche pas de qualifier ces opérations de paiement comme non autorisées. En d'autres termes, la Cour suprême a explicitement jugé qu'on ne peut assimiler authentification et autorisation. Ainsi, cet arrêt réfute d'emblée la thèse selon laquelle les opérations de paiement seraient toujours réputées autorisées si l'authentification a eu lieu selon la forme et la procédure convenues, indépendamment de la personne (victime ou fraudeur) ayant appliqué la procédure d'authentification.

Dans un arrêt du 9 janvier 2020, la Cour d'appel de Liège a jugé, lors d'une affaire de phishing, que l'opération de paiement en question était non autorisée bien que le consentement aux opérations contestées ait été donné selon la forme et la procédure convenues entre le prestataire de services de paiement et le payeur. La Cour d'appel fait ici référence à la disposition selon laquelle l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, n'est pas en soi nécessairement suffisante pour prouver que l'opération de paiement a été autorisée par le payeur. Pour conclure au caractère non autorisé de l'opération de paiement, la Cour d'appel souligne que le payeur n'avait jamais eu l'intention de confirmer l'opération litigieuse. La Cour prend donc en considération l'intention du payeur - l'élément intentionnel - confirmant ainsi la position d'Ombudsfin sur le consentement explicite subjectif. De plus, dans cette affaire, la procédure d'authentification - à savoir la génération d'un code de réponse à l'aide de la carte bancaire et du digipass, qui avait ensuite été utilisé pour confirmer le virement litigieux via le système bancaire en ligne - avait été effectuée par le payeur lui-même, de sorte que l'arrêt en question réfute clairement la thèse du consentement objectif explicite, ou technique.

Il convient toutefois de constater que cet arrêt n'a pas été suivi par l'ensemble de la jurisprudence. Une partie des décisions de première instance rendues après cette date estime en effet que la transmission d'un code au fraudeur témoigne à suffisance de la volonté de la victime d'autoriser l'opération, quand bien même il est établi que celle-ci ne connaissait, ni le montant ni le bénéficiaire de l'opération frauduleuse. Si cette transmission peut, dans certains cas, fonder une négligence grave dans le chef de la victime, il nous semble en revanche qu'elle n'est, à elle seule, pas relevante pour qualifier une opération d'autorisée.

Ombudsfin note enfin que nombre de cas de jurisprudence dont il a connaissance n'accordent que peu ou pas d'attention à la question de savoir si les opérations litigieuses peuvent ou non être réputées non autorisées. Cela s'explique par le fait que les institutions financières impliquées dans ces affaires ne contestent pas le caractère non autorisé des opérations litigieuses. Le caractère non autorisé des opérations litigieuses est pour ainsi dire considéré comme évident.

4.2. Obligation de remboursement immédiat

4.2.1. Dispositions de l'article VII.43 du CDE

L'article VII.43 du CDE dispose qu'en cas d'opérations de paiement non autorisées, le prestataire de services de paiement doit immédiatement rembourser au payeur le montant des opérations en question. Ce remboursement immédiat doit être effectué à partir du moment où le prestataire de services de paiement a pris connaissance ou a été informé de l'opération. La loi dispose que le remboursement doit être effectué au plus tard à la fin du jour ouvrable suivant.

Cette obligation de remboursement immédiat ne s'applique toutefois pas si le prestataire de services de paiement a des motifs raisonnables de soupçonner une fraude dans le chef du payeur et communique ces motifs par écrit au SPF Économie. Le prestataire de services de paiement a, par conséquent, la possibilité de mener une enquête prima facie à ce sujet dans un délai raisonnable avant de rembourser le payeur. Ainsi, si le prestataire de services de paiement a une forte présomption qu'une opération non autorisée résulte d'un comportement frauduleux de l'utilisateur de services de paiement et que cette présomption repose sur des raisons objectives qui sont communiquées à l'autorité nationale concernée, le prestataire de services de paiement

doit avoir la possibilité de mener une enquête dans un délai raisonnable avant de rembourser le payeur.

Une fois qu'il est établi qu'une opération de paiement non autorisée a eu lieu et qu'il n'y a aucun soupçon de fraude dans le chef du payeur, le compte de paiement débité doit être rétabli dans son état initial comme si l'opération de paiement non autorisée n'avait jamais eu lieu. La date valeur de ce remboursement ne peut pas être postérieure à la date de débit du montant en question. En d'autres termes, le prestataire de services de paiement ne peut pas attendre que la responsabilité du payeur soit définitivement fixée pour recréditer le compte de l'utilisateur de services de paiement.

L'objectif de cette obligation de remboursement immédiat dans le chef de l'institution financière est donc de réglementer provisoirement la répartition des responsabilités en attendant le partage définitif en vertu de l'article VII.44 du CDE. Cette obligation confirme qu'en principe, sauf en cas de fraude dans le chef du payeur lui-même, le prestataire de services de paiement est responsable et assume le risque des opérations de paiement non autorisées. Dans ce contexte, certains juristes estiment que le prestataire de services de paiement ne peut pas débiter unilatéralement le compte de paiement du payeur si le régime de responsabilité définitive prévu à l'article VII.44 du CDE l'amène à la conclusion qu'il n'est pas responsable (à moins qu'une enquête plus approfondie ne démontre que le payeur lui-même a agi frauduleusement). Le prestataire de services de paiement ne sera autorisé à débiter que si le payeur y consent ou s'il a obtenu un titre exécutoire pour ce faire.

Cette obligation de remboursement immédiat offre au payeur l'avantage de ne pas devoir se retourner contre le prestataire de services de paiement si celui-ci estime qu'il n'est pas responsable, au sens de la loi. En revanche, le prestataire de services de paiement affirmant que le payeur est responsable devra lui réclamer le montant des opérations de paiement non autorisées. En cas de refus de rembourser le montant litigieux, le prestataire de services de paiement devra entamer une action en justice, ce qui entraînera également des répercussions négatives pour le payeur, eu égard au coût d'une telle procédure. Par ailleurs, une augmentation du nombre de procédures judiciaires encombrera encore davantage nos tribunaux.

4.2.2. Non-respect fréquent dans la pratique

Ombudsfin constate qu'en pratique - du moins dans les dossiers traités par ses soins – la plupart des institutions financières ne respectent pas cette obligation. S'appuyant, entre autres, sur l'argument erroné selon lequel une opération authentifiée est également autorisée, les institutions concernées ne s'estiment pas tenues de procéder à un remboursement immédiat. Comme indiqué ci-dessus, cette obligation de remboursement immédiat n'est en effet valable que pour les opérations non autorisées.

D'un autre côté, certains juristes font valoir que l'obligation de remboursement immédiat ne s'applique, le cas échéant, qu'aux opérations de paiement non autorisées sans instrument de paiement. Les auteurs concernés reconnaissent néanmoins que la Commission européenne a un point de vue différent. Cette position est en outre contredite par un jugement du 11 février 2022 du tribunal de première instance néerlandophone de Bruxelles.[6]

Comme le livre VII du CDE ne prévoit pas de sanction spécifique, le payeur ne peut réclamer une indemnisation que pour le préjudice causé par le non-respect de cette obligation. A cet égard, le Collège d'experts d'Ombudsfin a déjà jugé que le payeur ne subit aucun préjudice en cas de non-respect de cette obligation de remboursement immédiat s'il est établi, en vertu du régime de responsabilité définitive prévu à l'article VII.44 du CDE, que la responsabilité incombe finalement au payeur. En revanche, si la responsabilité finale incombe au prestataire de services de paiement, le payeur pourra réclamer le paiement d'intérêts au taux légal à compter de la date à laquelle il aurait dû être crédité, conformément à l'article VII.43 du CDE.

[6] Le reste de la jurisprudence connue par Ombudsfin n'accorde que peu ou pas d'attention à cette problématique.

4.3. Partage de responsonsabilité en cas d'opérations de paiement non autorisées

4.3.1. Principe de base

Le prestataire de services de paiement est tenu d'assurer la mise en place ou l'organisation, au sein de son entreprise, de structures permettant de réaliser les opérations de paiement de manière sécurisée. En principe, c'est donc lui qui doit être tenu responsable en premier lieu du bon déroulement des paiements. On ne peut en effet pas attendre du payeur moyen qu'il ait une connaissance complète de ce processus technique.

Les travaux préparatoires de la loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique stipulent expressément qu'en cas de doute, cette réglementation doit être interprétée en faveur du payeur. Cette réglementation vise en effet à offrir une protection maximale au payeur.

4.3.2. Opérations de paiement contestées avant et après notification de la fraude

Le CDE établit une distinction entre les opérations qui ont eu lieu avant et après la notification de la perte, du vol, du détournement ou de l'utilisation non autorisée de l'instrument de paiement.

4.3.2.1. Obligation de notification sans délai

En vertu de l'article VII.38 du CDE, l'utilisateur de services de paiement est tenu d'informer immédiatement le prestataire de services de paiement ou l'entité désignée par ses soins (généralement Card Stop) de la perte, du vol, du détournement ou de l'utilisation non autorisée de l'instrument de paiement, dès qu'il en a connaissance.

L'article VII.41 du CDE dispose en outre que l'utilisateur de services de paiement ne pourra obtenir la rectification d'une opération non autorisée que s'il notifie cette opération au prestataire de services de paiement sans délai et au plus tard treize mois après la date valeur du débit ou du crédit. Il est plus ou moins admis dans la doctrine que les critères en question relèvent de deux conditions distinctes et cumulatives. La Commission européenne l'a d'ailleurs confirmé. Cela signifie que l'utilisateur de services de paiement doit, en tout état de cause, informer sans délai son institution financière dès qu'il a constaté la fraude. Si la notification n'a lieu que treize mois après le débit (ou plus tard), il y aura présomption irréfragable que le payeur a accepté l'opération de paiement et il ne pourra plus contester avec succès les opérations non autorisées auprès de la banque sur la base de l'article VII du CDE. En revanche, la présomption d'acceptation sera réfutable si la notification n'est pas effectuée immédiatement, mais bien dans un délai de treize mois. Dans ce cas, le payeur pourra donc toujours contester l'opération.

Les délais susmentionnés sont toutefois soumis à la condition que le prestataire de services de paiement ait honoré ses obligations légales d'information, notamment l'apport en temps utile de renseignements exacts sur l'opération de paiement. Si le prestataire de services de paiements ne s'est pas conformé à ces exigences d'information, le payeur pourra contester les opérations avec succès même après les délais susmentionnés. À cet égard, Ombudsfin conseille aux payeurs de vérifier régulièrement leurs extraits de compte et leurs états de dépenses.

Dans un arrêt du 2 septembre 2021, la Cour de justice s'est prononcée sur la question de savoir si, après l'expiration du délai de treize mois précité, le payeur peut encore engager la responsabilité de sa banque sur la base d'un autre régime de responsabilité, en l'occurrence le droit commun, et plus précisément le devoir de diligence du prestataire de services de paiement, compte tenu des délais de prescription correspondants. La Cour de justice a répondu à cette question par la négative, en invoquant l'effet d'harmonisation maximale[7] de PSD I et l'intention de créer un marché unique par le biais de cette directive. Comme PSD II vise également une harmonisation maximale, il nous semble que l'arrêt de la Cour de justice en question peut être appliqué par analogie à l'actuel article VII.41 du CDE.

De son côté, le prestataire de services de paiement est tenu, en vertu de l'article VII.39 du CDE, de veiller à ce

7 Notre législation belge relative aux opérations de paiement non autorisées résulte en effet de la transposition de plusieurs directives européennes. Ces directives visent une harmonisation maximale, ce qui signifie que les États membres ne peuvent pas offrir une protection supplémentaire au payeur lors de leur transposition en droit national.

que le payeur puisse effectuer cette notification à tout moment (24h/24, 7j/7). L'article VII.39, 4° du CDE dispose en outre que le payeur doit pouvoir effectuer cette notification gratuitement. Le CDE ne réglemente toutefois pas la manière dont la notification prévue à l'article VII.41 du CDE doit être effectuée. Par conséquent, l'article VII.39, 3° du CDE n'implique aucune obligation pour le prestataire de services de paiement de fournir une permanence téléphonique, par exemple. Il pourrait donc opter pour une notification de la fraude par e-mail, ce qui serait toutefois problématique pour les clients dépourvus d'adresse e-mail. Cette question ne présente toutefois plus d'intérêt pratique depuis peu. Alexia Bertrand, secrétaire d'État chargée du Budget et de la Protection des consommateurs, a en effet annoncé le 23 janvier que, depuis janvier 2023, toutes les banques disposent d'un service clientèle joignable 24h/24, 7j/7. Bien qu'il n'y ait aucune obligation légale en la matière, les banques belges assurent donc aujourd'hui bel et bien une permanence téléphonique. On ne peut que s'en réjouir.

L'article VII.189 du CDE dispose qu'en cas de non-respect de l'obligation prévue par l'article VII.39,3° du CDE[8], le prestataire de services de paiement devra assumer toutes les conséquences inhérentes à l'utilisation de l'instrument de paiement par un tiers non autorisé, quelles que soient les circonstances (sauf si le prestataire de services de paiement prouve que le payeur a agi frauduleusement). Comme l'article VII.189 du CDE n'exige pas de lien de causalité entre la méconnaissance de cette obligation légale et l'opération de paiement non autorisée, le payeur n'aura pas à supporter les conséquences des opérations qui ont eu lieu avant le moment où il a tenté d'effectuer une notification.

Par ailleurs, le prestataire de services de paiement doit, sur la base des articles VII.22 et VII.21 du CDE, fournir à l'utilisateur de ces services, sur un support durable et préalablement à la conclusion de l'accord-cadre, l'information relative à la manière dont l'utilisateur doit informer le prestataire.

Ombudsfin note qu'il faut parfois notifier la fraude plusieurs fois dans un même dossier pour bloquer tous les instruments de paiement. Ainsi, si le fraudeur a réussi à installer une application mobile liée aux comptes de sa victime, le blocage de la carte de paiement via Card Stop sera insuffisant chez certaines banques. En effet, le fraudeur ne pourra plus utiliser les données de la carte mais pourra toujours effectuer des opérations frauduleuses via l'application nouvellement installée. Les conditions générales de ces banques exigent donc une double notification de la fraude. Cela n'est pas toujours pratique pour le payeur car il n'a pas nécessairement une connaissance exhaustive de la procédure de notification et ignore en outre souvent quels instruments de paiement le fraudeur a pu installer en arrière-plan. Il lui est donc fréquemment impossible de savoir qu'une notification à Card Stop ne suffit pas à prévenir d'autres dommages. Une partie du monde politique demande, par conséquent, que les règles soient modifiées et que l'on mette en place un système permettant au payeur de bloquer à la fois sa carte bancaire, son compte bancaire et son application bancaire d'un simple clic ou appel téléphonique. On ne peut qu'espérer que cette demande soit rapidement entendue.

En plus de l'obligation, prévue à l'article VII.22 du CDE, d'informer le payeur sur la méthode de notification de la fraude avant la conclusion de l'accord-cadre, Ombudsfin estime également que le prestataire de services de paiement devrait toujours indiquer clairement la procédure de notification sur son site Web. Ces informations doivent en outre être aisément accessibles (sur la page d'accueil du site Web, par exemple). Cela ne peut, en effet, que contribuer à une notification correcte de la fraude.

4.3.2.2. Importance de la notification

a) Responsabilité du prestataire de services de paiement pour les opérations frauduleuses après notification

En vertu de l'article VII.39 du CDE, le prestataire de services de paiement est tenu d'empêcher toute utilisation ultérieure de l'instrument de paiement après la notification de la fraude par le payeur. Il s'agit là d'une obligation de résultat.

L'article VII.44, §3 du CDE établit explicitement que l'utilisation après notification de l'instrument de paiement perdu, volé ou détourné ne peut avoir aucune conséquence financière pour le payeur, sauf si le prestataire de services de paiement prouve que le payeur a agi frauduleusement. Le payeur ne peut donc, dans aucun autre cas, être tenu

[8] Le législateur a oublié d'adapter dans l'article VII. 189 CDE la numérotation à la nouvelle numérotation suite à la transposition de PSD II. Voir aussi art. 74, §3, al. 2 PSD II.

pour responsable des opérations effectuées après la notification, même s'il est établi qu'il a manqué à ses obligations par négligence grave.

Par conséquent, le prestataire de services de paiement ne peut pas s'exonérer de sa responsabilité en démontrant, par exemple, que le système (de paiement) concerné ne permet pas d'éviter une nouvelle utilisation de l'instrument de paiement immédiatement après la notification. Ainsi, Ombudsfin a constaté dans certains dossiers que le blocage de la carte bancaire via Card Stop ne pouvait pas empêcher toutes les utilisations de la carte physique. Dans les cas concernés, la carte bloquée via Card Stop avait encore pu être utilisée après son blocage, afin de générer des codes à l'aide du lecteur de cartes pour se connecter via la banque en ligne et effectuer des opérations. Le blocage de la carte pour les connexions aux services bancaires en ligne et l'exécution d'opérations n'avait pas été traité immédiatement, mais par lots, dans les dossiers concernés. Or, une carte bloquée via Card Stop ne doit plus pouvoir être utilisée physiquement, y compris pour générer des codes à l'aide du lecteur de carte et ensuite initier des opérations en ligne. Si le blocage de la carte de paiement avait été correctement effectué et immédiatement traité, tous les dommages survenus dans ces dossiers après la sollicitation de Card Stop auraient pu être évités. Ombudsfin note avec satisfaction que dans ces cas, les banques sont toujours intervenues pour tous les dommages survenus après le blocage de la carte.

En ce qui concerne la contestation des opérations de paiement non autorisées effectuées avant la notification, nous nous référons aux règles énoncées aux points 3.3. à 3.6 ci-dessous.

b) Tentative de récupération

Le moment de la notification de la fraude à l'institution financière est également important dans la mesure où l'institution financière a l'obligation, à partir de ce moment, de prendre des mesures raisonnables pour récupérer les sommes détournées. Cette obligation relève du devoir général de diligence dans le chef de la banque. L'institution financière est censée, dès la notification de la fraude, entreprendre les démarches requises dans les meilleurs délais et dans la mesure du possible, afin d'arrêter les opérations contestées, de bloquer les éventuels comptes bénéficiaires détenus dans la même institution et d'envoyer à toute institution financière bénéficiaire un avis lui demandant de bloquer le ou les comptes bénéficiaires et de restituer les fonds éventuellement disponibles. Cette procédure permet souvent de récupérer certains montants (parfois relativement conséquents).[9]

La question se pose de savoir dans quelle mesure le prestataire de services de paiement peut être tenu pour responsable en cas de non-respect de cette obligation de recouvrement ou de mise en œuvre tardive des mesures de recouvrement. Sur la base de l'arrêt de la Cour de Justice du 2 septembre 2021 précité, on pourrait considérer que cela n'est pas possible et que le régime de responsabilité est définitivement réglé dans le Livre VII du CDE. Néanmoins, dans le cadre de sa mission de médiation, Ombudsfin vérifiera le respect de l'obligation de recouvrement et, si nécessaire, demandera à l'institution financière concernée de formuler une proposition pour compenser une partie du dommage. Les éventuels dommages résultant de mesures de recouvrement tardives seront alors souvent difficiles à déterminer, voire à prouver. Malheureusement, les institutions financières n'interviennent que dans un nombre très limité de cas, en vertu de cet argument.

4.3.3. Authentification forte du client

4.3.3.1. Réglementation

En vertu de l'article VII.44, §2 du CDE, le payeur ne doit pas subir de pertes financières si le prestataire de services de paiement n'exige pas une authentification forte du client, à moins que le payeur lui-même n'ait agi frauduleusement. Dans pareil cas, le payeur ne peut donc pas être tenu responsable de l'opération de paiement non autorisée.

L'article I.9, 33/16° du CDE définit l'authentification forte du client comme suit : «une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît), « possession » (quelque chose que seul l'utilisateur possède) et « inhérence » (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité

[9] Le succès de ces démarches dépend évidemment de la bonne collaboration de la banque du bénéficiaire. Nous observons que celle-ci existe dans la plupart des cas lorsqu'il s'agit d'une banque belge. C'est malheureusement souvent plus compliqué lorsque cette banque est établie à l'étranger.

des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification». Il est question d'authentification forte du client dès que deux des facteurs susmentionnés sont combinés. Dans un avis du 21 juin 2019, l'Autorité bancaire européenne (ABE) a fourni davantage d'explications sur l'interprétation de ces concepts. Les données de la carte, la carte bancaire et l'application bancaire mobile sont des exemples d'éléments de la catégorie «possession». Le code PIN de la carte de paiement et le code d'accès de l'application bancaire mobile sont des exemples d'éléments de la catégorie «connaissance». Le scanning de l'empreinte digitale et du visage est un exemple d'«inhérence».

Si un paiement en ligne par carte de crédit est effectué uniquement via les données de la carte de crédit, qui relèvent de la catégorie «possession», il n'est pas question d'authentification forte du client au sens de la définition ci-dessus et compte tenu de l'avis de l'ABE du 21 juin 2019. En revanche, il y a bien authentification forte du client si un paiement en ligne est confirmé au moyen d'un code de réponse généré via la carte bancaire, le code PIN et le digipass. La création de ce code de réponse nécessite en effet la carte bancaire (puce électronique), un élément de la catégorie «possession», et le code PIN, un élément de la catégorie «connaissance».

La PSD II prévoit que les prestataires de services de paiement doivent assurer une authentification forte du client lorsqu'un payeur accède à son compte en ligne, initie un paiement électronique ou effectue un acte de quelque nature que ce soit via tout moyen de communication à distance susceptible d'entraîner un risque de paiement frauduleux ou d'autres abus. La réglementation relative aux exigences d'authentification forte des clients figure également dans le Règlement délégué de la Commission du 27 novembre 2017 portant sur des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (RD AFC).

En principe, les prestataires de services de paiement doivent donc assurer une authentification forte du client dans les cas prévus à l'article 97, §1 de PSD II. Le RD AFC prévoit toutefois un certain nombre d'exemptions. Parmi les exemples connus ne nécessitant pas une authentification forte du client figurent, d'une part, les opérations de paiement électronique à distance d'un montant inférieur à 30 €, pour lesquelles, par exemple, seuls le numéro de carte, la date d'expiration et le code CVC sont demandés, et, d'autre part, les paiements sans contact d'un montant inférieur à 50 € pour lesquels aucun code PIN n'est requis.

Si la plupart des exemptions prévues dans le RD AFC sont claires, il n'est tout de même pas toujours évident d'indiquer sans ambiguïté quand une opération doit ou non être confirmée par une authentification forte du client. En effet, l'article 18 du RD AFC dispose que les prestataires de services de paiement ne doivent pas appliquer d'authentification forte du client aux opérations de paiement électronique à distance si les opérations en question ont été identifiées comme des opérations à faible risque sur la base d'une analyse du risque de l'opération (mécanisme de contrôle des opérations). Cette disposition prévoit en outre un certain nombre de conditions cumulatives auxquelles une opération doit satisfaire pour être réputée à faible risque. Cette exemption laisse donc une certaine marge de manœuvre pour déterminer si une authentification forte du client est nécessaire.

Si un payeur est victime d'opérations de paiement non autorisées sans authentification forte du client, il sera toujours (sauf s'il a lui-même agi frauduleusement) exonéré de toute responsabilité. Il ne pourra pas être tenu pour responsable s'il a méconnu certaines obligations par négligence grave. La même règle s'applique si le prestataire de services de paiement est exempté de l'exigence d'authentification forte du client en vertu du RD AFC. En d'autres termes, si le prestataire de services de paiement décide de ne pas exiger d'authentification forte du client dans certains cas, c'est lui qui en assumera le risque.

Si l'absence d'authentification forte du client est due au fait que le bénéficiaire ou son prestataire de services de paiement n'accepte pas l'authentification forte du client, le payeur pourra toujours poursuivre son propre prestataire de services de paiement afin d'être indemnisé en vertu de l'article VII.44, §2 du CDE. Sur la base de cet article, le prestataire de services de paiement de la victime pourra se tourner vers le (prestataire de services de paiement du) bénéficiaire.

Il va de soi que les commerçants et les prestataires de services de paiement non européens ne sont pas liés par les obligations européennes en matière d'authentification forte des clients. Si le payeur est victime d'opérations de

paiement non autorisées, sans authentification forte du client, au bénéfice de commerçants non européens, il pourra toujours se tourner vers son prestataire de services de paiement sur la base de l'article VII.44, §2 du CDE pour obtenir une indemnisation complète de son préjudice. C'est également ce qu'a jugé le Collège d'experts d'Ombudsfin, en se référant à l'article VII.2, §1 alinéa 3 du CDE, qui régit le champ d'application des chapitres pertinents du Livre VII du CDE. L'article VII.2, §1, alinéa 3 du CDE stipule, en effet, que les règles en question s'appliquent aux opérations de paiement dans toutes les devises lorsqu'un seul des prestataires de services de paiement est situé dans un État membre, pour ce qui concerne les parties de l'opération de paiement effectuées dans un État membre.

4.3.3.2. Application : installation frauduleuse d'Apple Pay

Dans un jugement non publié du 11 février 2022, le tribunal de première instance néerlandophone de Bruxelles a estimé qu'il est question d'authentification forte du client dans les cas où un fraudeur parvient à installer une application bancaire mobile, liée aux comptes de sa victime, sur son propre appareil (au moyen d'un ou plusieurs codes de réponse générés avec la carte bancaire de la victime et un digipass, c'est-à-dire une authentification forte du client) puis à utiliser cette application pour confirmer des opérations frauduleuses au moyen d'un code choisi par le fraudeur lors de l'installation de l'application, ou d'un scanning de l'empreinte digitale ou du visage.

Ce jugement n'empêche toutefois pas Ombudsfin d'être occasionnellement confronté à des cas intéressants où l'on peut se demander si certaines opérations effectuées via une application nouvellement installée ont été confirmées ou non par une authentification forte du client. En 2021, par exemple, Ombudsfin a mené des discussions intéressantes avec une banque concernant la procédure d'installation d'Apple Pay. Dans les dossiers soumis à Ombudsfin, le fraudeur était chaque fois parvenu à relier une carte de paiement de sa victime à sa propre application Apple Pay sur son propre appareil (Apple), puis à utiliser cette application pour effectuer des paiements frauduleux tant en ligne que chez des commerçants. Les opérations concernées pouvaient être confirmées via Apple Pay par un code d'accès présélectionné (par le fraudeur) ou par un scanning de l'empreinte digitale ou du visage (du fraudeur).

La question qui se posait dans les dossiers en question était de savoir si Apple Pay avait été installée via une authentification forte du client. L'établissement financier en question prévoyait deux procédures d'installation.[10]

(i) Dans certains dossiers, le fraudeur était parvenu à installer d'abord l'application mobile de la banque sur son propre appareil puis, à partir de cette application, à lier la carte de paiement de la victime à son application Apple Pay. L'application mobile de la banque était toujours installée au moins sur la base d'un ou plusieurs codes générés avec la carte bancaire, le code PIN et le digipass. Dans ces cas, on pouvait donc parler d'authentification forte du client.

(ii) Des fraudeurs étaient aussi parvenus à associer la carte de paiement de leur victime à leur propre application Apple Pay à partir de l'application « portefeuille » (« Wallet ») de leur appareil. Cette démarche était rendue possible grâce aux données de la carte et à un code d'activation généralement envoyé par SMS au numéro de téléphone mobile de la victime. Dans ces dossiers, Ombudsfin note que la carte de paiement n'était pas couplée à une authentification forte du client. En effet, compte tenu de l'avis de l'ABE du 21 juin 2019, tant les données de la carte que le code d'activation envoyé par SMS doivent être considérés comme des éléments de la catégorie « possession ». Selon l'ABE, ce code d'activation ne peut être considéré comme relevant de la catégorie « connaissance », car il ne peut être question d'un élément de la catégorie « connaissance » que si ce dernier existe déjà avant le début d'une opération ou d'un accès en ligne.

Ombudsfin constate que, compte tenu des éléments qui précèdent, la banque concernée a proposé une intervention systématique dans les dossiers de fraude liés à la deuxième procédure d'installation.

[10] Veuillez noter que la procédure d'installation d'Apple Pay peut varier d'une banque à l'autre.

3.4. Règle de base : responsabilité du prestataire de services de paiement après déduction d'une franchise de 50 €

En ce qui concerne le partage des responsabilités pour les opérations de paiement non autorisées, avant notification et effectuées par le biais d'une authentification forte, l'article VII.44, §1, alinéa 1 du CDE dispose que, jusqu'à la notification, le payeur ne doit supporter qu'à concurrence de 50 € les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu, volé ou détourné. Le payeur ne supporte donc qu'un risque limité, à savoir une franchise limitée à 50 €. Cette franchise s'applique à la totalité des opérations de paiement non autorisées effectuées à l'aide d'un instrument de paiement et pas par opération. Si un fraudeur parvient à effectuer des opérations de paiement non autorisées en utilisant plusieurs instruments de paiement, cette franchise devra alors être appliquée par instrument de paiement.

Cette règle de base n'est applicable que si aucune des hypothèses évoquées aux points 3.5 et 3.6 ne s'applique. Elle connaît une seule exception, en vertu de laquelle le payeur ne supporte aucun dommage si la perte a été causée par les actes ou omissions d'un employé, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité à laquelle ses activités ont été externalisées. Nous ne nous y attarderons toutefois pas car nous n'avons encore jamais dû l'appliquer.

4.3.5. Caractère détectable de la fraude

4.3.5.1. Réglementation et application

L'article VII.44, §1, alinéa 2, 1° du CDE stipule que le payeur ne doit supporter aucune perte, donc pas non plus la franchise de 50 €, 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 celui-ci a agi frauduleusement. Cela signifie donc que la victime d'une fraude ne peut être tenue pour responsable si elle n'était pas en mesure de détecter au préalable le détournement de son instrument de paiement.

Les travaux préparatoires de la loi indiquent que cet article peut notamment s'appliquer dans certains cas de hacking et phishing de données de sécurité personnalisées ou de skimming de cartes. Ils précisent en outre que le « détournement » couvre également, par exemple, le vol des données de paiement alors que le payeur est encore en possession de son instrument de paiement (phishing, clonage de l'instrument de paiement, etc.).

La possibilité de détecter préalablement une fraude doit être évaluée compte tenu de l'ensemble des faits. Il est, par conséquent, incorrect d'affirmer qu'une victime de phishing, par exemple, peut automatiquement invoquer l'article VII.44, §1, alinéa 2, 1° du CDE et ne devra dès lors supporter aucun préjudice. Il convient d'abord de déterminer, à la lumière des circonstances concrètes, si la disposition en question est applicable ou non. Dans la négative, il faudra revenir à la règle de base et procéder à une évaluation de l'éventuelle négligence grave.

Cette règle prévoit donc que le payeur ne doit supporter aucune perte si le détournement de l'instrument de paiement ne pouvait être décelé avant l'exécution d'un paiement. A cet égard, il faut déterminer si, compte tenu de toutes les circonstances de l'affaire, un payeur moyen aurait dû détecter la fraude. La question centrale est donc de

savoir si l'on peut parler de négligence (simple) par rapport au comportement du payeur moyen.

Dans la pratique, Ombudsfin prend plusieurs éléments en considération pour évaluer le caractère détectable de la fraude. Il faut ainsi tenir compte de la manière dont le message frauduleux a été rédigé et de la présence ou non d'erreurs grammaticales ou orthographiques. L'adresse e-mail utilisée par le fraudeur et l'endroit d'où provient le message fallacieux sont également importants, de même que le lien utilisé et l'URL du site frauduleux. Ombudsfin vérifie aussi si la procédure à suivre aurait pu permettre au payeur de déceler la fraude. À titre d'exemple, la fraude est généralement détectable lorsque le client doit générer des codes à l'aide de sa carte bancaire et de son digipass pour recevoir une certaine somme d'argent. Elle l'est aussi lorsqu'un payeur est invité à fournir certains codes par téléphone, pour quelque raison que ce soit. Les circonstances concrètes de la fraude sont également pertinentes. Ainsi, une fraude peut être considérée comme détectable lorsqu'une personne répond à un SMS frauduleux censé provenir d'itsme et portant sur le blocage du compte itsme du destinataire, alors que la personne n'a jamais utilisé itsme. La fraude peut aussi être détectable, par exemple, via l'affichage de certains messages contextuels sur le digipass de la banque. Si un message contextuel indiquant l'installation d'une nouvelle application apparaît sur le digipass, alors que le payeur pense accuser réception d'un paiement ou effectuer un paiement, ce message contextuel rendra la fraude détectable, à condition d'être clairement rédigé. Par ailleurs, depuis quelques années, les banques envoient plusieurs SMS après une nouvelle installation de leur application mobile. Le point 3.7 examine plus en détail l'incidence de ces messages sur le partage des responsabilités.

Le CDE ne réglemente pas explicitement la charge de la preuve concernant le caractère détectable préalable de la fraude par le payeur. Comme l'article VII.44, §1, alinéa 2, 1° du CDE doit être considéré, d'après Ombudsfin, comme une exception, favorable au payeur, à la règle selon laquelle le prestataire de services de paiement doit supporter la perte, après déduction d'une franchise de 50 €, Ombudsfin estime que, par application du droit commun de la preuve, il appartient au payeur de fournir des éléments prouvant que la fraude ne pouvait être détectée au préalable.

Le payeur qui souhaite invoquer la règle de l'article VII.44, §1, alinéa 2, 1° du CDE doit donc fournir des éléments prouvant que la fraude ne pouvait être détectée à l'avance. Ombudsfin est souvent confronté à des plaintes dans lesquelles, par exemple, le payeur ne peut présenter une copie du message frauduleux ou de la communication avec le fraudeur (par exemple via Messenger ou WhatsApp) parce qu'il l'a supprimée. Dans d'autres cas, le payeur a oublié le lien frauduleux sur lequel il a cliqué. Dans ces dossiers, le payeur ne pourra donc pas invoquer avec succès l'article VII.44, §1, alinéa 2, 1° du CDE.

4.3.5.2. Indépendamment d'une négligence grave

On verra au point 3.6. ci-dessous qu'il existe une autre exception à la règle de base pour les cas de négligence grave dans le chef du payeur. L'article VII.44, §1, alinéa 4 du CDE prévoit en effet que le payeur doit supporter toutes les pertes liées aux opérations de paiement non autorisées s'il les a subies en raison de son manquement à certaines obligations par négligence grave.

Ombudsfin note que la manière dont l'article VII.44, §1 du CDE est rédigé (ordre de succession des différentes hypothèses) crée une ambiguïté quant à la relation entre les deuxième et quatrième alinéas de l'article VII.44, §1 du CDE. En d'autres termes, la question se pose de savoir si l'exception liée à une négligence grave s'applique ou non aux cas relevant de l'article VII.44, §1, alinéa 2, 1° du CDE. Autrement dit, s'il est établi que le payeur n'aurait pas pu détecter la fraude à l'avance, pourra-t-il automatiquement poursuivre le prestataire de services de paiement en vertu de l'article VII.44, §1, alinéa 2, 1° du CDE pour obtenir le remboursement intégral du préjudice subi, indépendamment de toute négligence grave, ou faut-il d'abord déterminer si le payeur a fait preuve ou non de négligence grave ?

La doctrine adopte généralement la position selon laquelle l'existence ou non d'une négligence grave dans le chef de la victime ne joue aucun rôle dans l'hypothèse où le payeur n'aurait pas pu détecter la fraude au préalable. Si l'article VII.44, §1, alinéa 2, 1° du CDE s'avère applicable, le payeur ne devra donc supporter aucune perte même s'il a commis une négligence grave. Cette interprétation ressort, en effet, clairement du texte de la loi, vu que cette dernière ne prévoit aucune exception explicite pour la négligence grave dans le cadre de cette hypothèse. En outre, le quatrième alinéa de l'article VII.44, §1 du CDE (concernant la négligence grave) ne déroge qu'au premier alinéa, et donc pas au deuxième. Pour

défendre ce point de vue, on peut en outre se référer au considérant 71 de PSD II, qui stipule que la responsabilité du payeur ne devrait pas être engagée lorsque celui-ci n'est pas en mesure de prendre conscience de la perte, du vol ou du détournement de l'instrument de paiement.

La jurisprudence n'accorde souvent que peu voire pas du tout d'attention à cette question. Dans un jugement du 23 mars 2021, le tribunal de l'entreprise de Louvain a expressément confirmé que l'alinéa 2 de l'article VII.44, §1 du CDE constitue une règle spéciale qui prévaut sur l'alinéa 4. Ce point de vue est confirmé par un jugement du tribunal de l'entreprise d'Anvers, mais contredit par un jugement du tribunal de première instance néerlandophone de Bruxelles du 4 avril 2022. Le tribunal bruxellois souligne que les deuxième et quatrième alinéas de l'article VII.44, §1 du CDE constituent chacun une exception indépendante, de signification opposée, au principe de l'article VII.44, §1, alinéa 1 du CDE.

Compte tenu du principe selon lequel la réglementation de l'article VII.44 du CDE doit être interprétée en faveur du payeur en cas de doute, Ombudsfin accorde ses faveurs à la première interprétation, selon laquelle l'exception en cas de négligence grave n'entre pas en ligne de compte pour les dossiers relevant de l'article VII.44, §1, alinéa 2 du CDE.

L'importance de cette discussion ne doit toutefois pas être surestimée dans la mesure où les hypothèses dans lesquelles la victime a fait preuve de négligence grave alors que la fraude n'était pas détectable sont, de notre expérience, extrêmement rares.

3.6. Négligence grave, fraude ou intention dans le chef du payeur

Si l'article VII.44, §1, alinéa 2, 1°du CDE n'est pas applicable, parce qu'il est établi que la fraude pouvait être détectée à l'avance par le payeur ou que ce dernier ne fournit pas d'éléments suffisants pour prouver que la fraude ne pouvait être détectée à l'avance, il faut revenir à la règle de base de l'article VII.44 du CDE. Cette dernière stipule que le prestataire de services de paiement doit intervenir dans les dommages, après déduction d'une franchise de 50 €.

L'article VII.44, §1, alinéa 4 du CDE stipule toutefois que, contrairement à ce que prévoit la règle de base, le payeur devra supporter 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, à une ou plusieurs des obligations qui lui incombent en vertu de l'article VII.38 du CDE.

4.3.6.1. Évaluation de la négligence grave

Cet article impose plus particulièrement les obligations suivantes au payeur :

- Le payeur doit utiliser l'instrument de paiement conformément aux conditions régissant l'émission et l'utilisation de cet instrument de paiement. Ces conditions sont fixées contractuellement. Elles doivent être objectives, non discriminatoires et proportionnées. Les travaux préparatoires à la loi précisent que cette dernière porte essentiellement sur les dispositions visant à préserver la sécurité des instruments de paiement et des données de sécurité personnalisées.

- Le payeur est tenu d'informer sans délai le prestataire de services de paiement ou son entité désignée dès qu'il constate la perte, le vol ou le détournement de son instrument de paiement.

- Afin de se conformer aux obligations susmentionnées, l'utilisateur de services de paiement doit prendre toutes les mesures raisonnables pour préserver la sécurité de l'instrument de paiement et de ses données de sécurité personnalisées. Et ce, dès qu'il a reçu l'instrument de paiement.

La PSD II et le CDE ne donnent aucune définition de la notion de «négligence grave». Cela dit, le considérant 72 de la PSD II précise clairement qu'une négligence grave doit inclure plus que de la simple négligence. Elle doit comporter un défaut de vigilance caractérisé. Il ne faut donc pas conclure trop facilement à l'existence d'une négligence grave. Comme cette règle, qui oblige donc le payeur à supporter l'intégralité de la perte s'il n'a pas respecté certaines obligations en raison d'une négligence grave, constitue une exception au niveau élevé de protection que la PSD II entend procurer, le concept de «négligence grave» doit toujours être interprété de manière restrictive. Il doit s'agir d'une erreur ou d'une négligence grave et tellement excessive qu'elle est incompréhensible pour une personne raisonnable, ou d'un comportement qu'un payeur raisonnablement prudent n'adopterait jamais. La jurisprudence utilise également cette définition ou une définition similaire. Pour l'évaluation de la négligence grave, Ombudsfin tient compte des mêmes éléments que pour l'évaluation du caractère détectable de la fraude, si ce n'est qu'en l'occurrence, il faudra vérifier si ces éléments reflètent un très haut niveau de négligence plutôt qu'une «simple» négligence.

L'article VII.44, §4, alinéa 3 du CDE stipule que l'évaluation de la négligence doit tenir compte de l'ensemble des circonstances factuelles. Cela signifie qu'il faut une évaluation globale de toutes les données factuelles pertinentes. Ainsi, une série d'éléments factuels qui, pris

séparément, ne constituent pas nécessairement une négligence grave, peuvent néanmoins être considérés comme une négligence grave dans leur ensemble. L'appréciation de la négligence grave doit être complète, ce qui signifie qu'elle ne doit pas non plus dépendre d'un seul élément factuel.

L'article VII.44 §4, alinéa 2 du CDE comporte en outre une liste non exhaustive de comportements assimilés à des négligences graves. Il s'agit simplement d'exemples de négligence grave, ce qui signifie que d'autres comportements pourraient aussi être considérés comme des négligences graves. Le CDE donne les exemples suivants :

- Le fait, pour le payeur, de noter ses données de sécurité personnalisées, comme son numéro d'identification personnel ou tout autre code, sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement ou sur un objet ou un document conservé ou emporté par le payeur avec l'instrument de paiement ;

- Le fait de ne pas avoir notifié au prestataire de services de paiement ou à l'entité indiquée par celui-ci, la perte ou le vol dès qu'il en a eu connaissance.

L'exposé des motifs insiste sur le fait que même dans les cas susmentionnés prévus par la loi, la négligence grave dépend de l'ensemble des circonstances de fait. On peut donc considérer que, dans ces cas, il est généralement question de négligence grave mais que les circonstances factuelles peuvent amener à conclure différemment.

Ombudsfin note, par ailleurs, que de nombreuses institutions financières spécifient dans leurs conditions générales les comportements constitutifs de négligence grave. Ombudsfin estime toutefois que de telles clauses ne peuvent exclure sa liberté d'appréciation. Ainsi, d'après Ombudsfin, les comportements qualifiés de négligence grave par les règlements de la banque ne peuvent pas automatiquement être considérés comme tels. Dans ces cas également, l'appréciation de la négligence grave doit donc tenir compte de l'ensemble des circonstances factuelles. Les dispositions relatives au partage des responsabilités en cas d'opérations de paiement non autorisées sont, en effet, impératives. Il s'ensuit que les droits du payeur ne peuvent être limités. Les conditions générales d'une institution financière ne peuvent par conséquent pas étendre la responsabilité du payeur.

Les clauses contractuelles spécifiant les comportements assimilés à une négligence grave peuvent toutefois s'avérer pertinentes pour l'évaluation de la négligence grave par le juge. En effet : la désignation contractuelle de certains comportements comme relevant d'une négligence grave permet en quelque sorte de sensibiliser le payeur au caractère risqué de ces comportements.

Enfin, la Cour d'appel d'Anvers a estimé que la négligence grave devait être appréciée à l'aune du comportement présumé d'un payeur normalement soigneux et prudent placé dans les mêmes circonstances extérieures concrètes. Elle a ajouté explicitement que dans ce contexte, il ne fallait pas tenir compte de caractéristiques propres au payeur, telles que son âge. En d'autres termes, la négligence grave doit être évaluée de manière abstraite. D'après Ombudsfin, cela ne signifie toutefois pas que l'expérience professionnelle et l'historique du client ne peuvent pas être pris en considération (par exemple dans le cas d'une récidive, lorsque le payeur est victime d'un même type de fraude à plusieurs reprises).

L'appréciation de la négligence grave devra toujours s'effectuer au cas par cas. Il est donc difficile de tirer des conclusions univoques de la jurisprudence plutôt limitée. On ne peut jamais être sûr de ce que le juge décidera. Cette évaluation est en outre sujette à évolution dans une certaine mesure. Aujourd'hui, en effet, le payeur moyen en sait plus sur le phishing qu'il y a trois ans, par exemple.

4.3.6.2. Charge de la preuve

L'article VII.44, §4, alinéa 1 du CDE stipule que la charge de la preuve en matière de fraude, d'intention ou de négligence grave incombe au prestataire de services de paiement. L'article VII.44, §4, alinéa 3 du CDE dispose, par ailleurs, que l'utilisation de l'instrument de paiement avec le code connu du seul utilisateur de services de paiement ne constitue pas une présomption suffisante de la négligence de celui-ci. Comme expliqué ci-dessus, la loi dispose que l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, ne suffit pas nécessairement à prouver que l'opération de paiement a été autorisée par le payeur ou que celui-ci a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent. Depuis le 9 août 2018, le

prestataire de services de paiement doit en outre fournir des éléments à l'appui afin de prouver la fraude ou la négligence grave commise par le payeur.

L'exposé des motifs précise expressément qu'il est exclu de faire valoir une présomption de négligence grave, en application de laquelle le payeur aurait manqué à ses obligations, commis une négligence grave, ou agi frauduleusement. En effet, une telle présomption affaiblirait considérablement la protection conférée au payeur par la loi. L'interdiction d'invoquer une présomption de négligence grave n'empêche toutefois pas d'utiliser d'autres présomptions graves et concordantes pour conclure à une négligence grave.

En pratique, Ombudsfin est souvent confronté à des cas de fraude où le récit factuel du payeur ne correspond pas entièrement aux données techniques de la banque. Par exemple, le payeur affirme qu'il n'a pas saisi de codes générés par le digipass sur le site Web frauduleux, tandis que la banque peut prouver que le fraudeur a saisi un tel code de réponse pour chaque opération contestée. Un autre exemple concerne les cas où la banque peut démontrer que le fraudeur a installé une application mobile liée aux comptes de sa victime et qu'un code d'activation a été envoyé par SMS au numéro du payeur connu de la banque afin d'activer cette application, tandis que le payeur nie avoir reçu ou utilisé un tel code. Dans ces cas, sur la base de présomptions sérieuses et concordantes, on pourrait estimer que le payeur a bien saisi les codes en question sur le site Web frauduleux et conclure, sur la base de cette présomption, à l'existence d'une négligence grave en fonction des circonstances spécifiques. Ombudsfin ne procède toutefois pas de cette manière en pratique. Comme Ombudsfin ne peut, dans ces cas, pas vérifier les déclarations du client et n'exclut pas non plus la possibilité que le fraudeur ait pu techniquement intercepter les codes de l'une ou l'autre manière, inconnue, Ombudsfin estime plus prudent de ne pas se prononcer sur une éventuelle négligence grave.

4.3.7. Cas d'application de la détectabilité et de la négligence grave : messages envoyés dans le cadre de l'installation de l'application bancaire mobile.

Il est fréquent qu'un fraudeur se serve de données obtenues ou interceptées pour installer sur son propre appareil une application mobile liée aux comptes de sa victime. Grâce à cette application, le fraudeur peut ensuite accéder aux comptes de sa victime puis confirmer des paiements et virements frauduleux à l'aide d'un code choisi par le fraudeur lors de l'installation de l'application. Dans ce genre de dossier, les dommages peuvent souvent être très élevés.

Au fil des ans, les institutions financières ont pris certaines mesures pour prévenir ou minimiser les pertes. Ombudsfin constate ainsi que ces dernières années, conformément à ses recommandations, de plus en plus de banques ont adapté la procédure d'installation de leur application mobile en utilisant des codes ou des liens d'activation supplémentaires, qui sont envoyés par SMS ou par e-mail au numéro de téléphone mobile ou à l'adresse e-mail connus de la banque. Mais il y a encore des institutions financières qui se contentent d'envoyer un message donnant des informations sur l'installation d'une nouvelle application, sans que le payeur doive effectuer la moindre opération supplémentaire pour activer l'application en question.

Examinons dès lors l'incidence des messages envoyés par la banque sur l'installation et/ou l'activation frauduleuse d'une nouvelle application mobile, en fonction du contenu de ces messages.

a) Simple message donnant des informations sur l'installation d'une nouvelle application, sans code ni lien d'activation.

Après l'installation d'une nouvelle application mobile, certaines institutions financières envoient au payeur un message purement informatif signalant l'installation. Ce message est envoyé par SMS ou courrier électronique au numéro de téléphone mobile ou à l'adresse e-mail du client enregistrés dans les systèmes de la banque. Il inclut souvent des instructions au cas où le payeur n'aurait pas installé l'application lui-même. Ces institutions n'envoient donc pas de (deuxième) message avec un code d'activation ou un lien supplémentaire.

Une telle notification est, certes, susceptible de renforcer la vigilance du payeur mais offre logiquement moins de protection qu'une demande d'activation supplémentaire de l'application mobile nouvellement installée. En effet, il est toujours possible que le payeur ne voie pas immédiatement le message en question, permettant ainsi au fraudeur d'agir dans l'intervalle.

S'il est établi que le payeur a (immédiatement) vu la notification relative à la nouvelle installation d'une application mobile - parce qu'il l'a signalée à la banque ou à la police, par exemple - cela peut être pris en compte lors de l'évaluation du caractère détectable préalable de la fraude et de la négligence grave. Dans ce cas, néanmoins, la prise de connaissance du message ou le non-respect des instructions qu'il contient ne signifiera pas nécessairement que la fraude aurait pu être détectée au préalable ou que le client a fait preuve d'une négligence grave. Cette évaluation doit toujours tenir compte des circonstances concrètes de la fraude. À titre d'exemple, si le payeur a réagi à un e-mail de phishing lui demandant de réinstaller et réactiver son application bancaire, on ne pourra pas conclure au caractère détectable de la fraude ou à la négligence grave sur la base de la notification en question. En revanche, si l'e-mail de phishing portait par exemple sur la demande d'un nouveau digipass, il est de nature à rendre la fraude détectable. Pour déterminer si le non-respect des instructions relatives au blocage de l'application mobile constitue ou non une négligence grave, il faut tenir compte, entre autres, de toutes les circonstances de la fraude ainsi que de la plausibilité des explications données par le payeur pour justifier l'absence de réaction. Il convient également d'examiner si la notification en question a été rédigée avec suffisamment de clarté, en soulignant une fraude potentielle, par exemple.

Si le payeur déclare qu'il n'a pas reçu ladite notification concernant l'installation d'une nouvelle application ou qu'il ne l'a pas lue à temps. Il sera alors très difficile pour le prestataire de services de paiement de prouver le contraire. Dans ces cas, selon Ombudsfin, la notification en question ne pourra pas être prise en compte lors de l'évaluation du caractère détectable de la fraude et de la négligence grave. Le prestataire de services de paiement assumera donc le risque lié à son choix d'envoyer uniquement un message d'information, sans code ni lien d'activation.

La jurisprudence est divisée sur cette question. Dans un jugement du 11 février 2022, le tribunal civil de Bruxelles a déclaré que le fait de ne pas réagir immédiatement à la notification ne pouvait être considéré comme une négligence grave. Le tribunal a motivé sa décision en déclarant que ni la loi ni la norme de diligence n'imposaient d'avoir son téléphone portable sur soi en permanence. En revanche, dans un jugement du 4 avril 2022, le même tribunal a déclaré que le fait d'être injoignable durant une longue période, en l'occurrence en omettant de recharger la batterie de son smartphone, n'est pas conciliable avec le comportement d'une personne normalement prudente et raisonnable dans la société actuelle. Ombudsfin estime que cette dernière position est beaucoup trop stricte et préfère donc se rallier à la première.

Aux institutions financières qui choisissent de n'envoyer qu'un message purement informatif concernant l'installation d'une nouvelle application, Ombudsfin recommande de laisser l'application en question inactive durant quelques heures. Ainsi, le payeur aura encore une certaine possibilité de prendre connaissance de la notification dans un délai raisonnable et de réagir de manière appropriée. Cela permettra d'éviter des dommages dans plusieurs cas.

b) Message avec code ou lien d'activation

De plus en plus d'institutions financières prévoient une étape supplémentaire dans la procédure d'installation d'une nouvelle application mobile, à savoir l'envoi d'un code ou lien d'activation au client par SMS ou e-mail. Cette étape d'activation offre évidemment une sécurité accrue et présente en outre l'avantage de permettre à la banque de s'assurer, via les SMS et e-mails en question, que c'est bien le client lui-même qui effectue les actions concernées. Si une telle mesure renforce la sécurité, elle n'éliminera toutefois jamais complètement la fraude. En effet, les fraudeurs en tiennent compte et adaptent constamment leurs stratégies et méthodes afin d'intercepter ou obtenir les données nécessaires à l'activation.

Si les payeurs reconnaissent avoir reçu les messages concernés et utilisé le lien ou le code d'activation, il faudra évidemment en tenir compte lors de l'évaluation du caractère détectable de la fraude et de la négligence grave. Une fois encore, cela n'entraînera pas automatiquement la responsabilité du payeur. Ainsi, si le message de phishing concerne l'installation de l'application bancaire, la saisie du code d'activation ne constitue pas en soi une négligence grave. En revanche, s'il porte sur la réception d'une prime quelconque, la conclusion peut être différente. Il convient à nouveau de déterminer si les messages envoyés par le prestataire de services de paiement sont suffisamment clairs ou non.

Si le prestataire de services de paiement transmet un code ou un lien d'activation, le payeur pourra moins facilement

nier avoir reçu les messages envoyés par la banque ou prétendre ne pas avoir utilisé le code ou le lien reçu puisque l'application aura, en effet, été activement utilisée par le fraudeur.

Compte tenu de ce qui précède, Ombudsfin renouvelle ses recommandations aux institutions financières en les encourageant à demander une activation supplémentaire au payeur durant la procédure d'installation de l'application mobile. Cette démarche accroît non seulement la sécurité pour le client mais entraîne aussi des implications positives pour le prestataire de services de paiement en ce qui concerne l'évaluation du partage des responsabilités conformément à l'article VII.44 du CDE. L'argument relatif à l'activation préalable est également étayé par l'article 25 du Règlement délégué AFC. Cet article dispose en effet que les prestataires de services de paiement sont tenus de s'assurer, lorsque la fourniture de données de sécurité personnalisées s'effectue en dehors des locaux du prestataire de services de paiement ou via un moyen de communication à distance (en l'occurrence l'installation de l'application de paiement), que les données de sécurité personnalisées fournies et le matériel ou logiciel d'authentification doivent être activés avant de pouvoir être utilisés.

Ombudsfin note également qu'après l'installation de l'application mobile ou une connexion au système bancaire en ligne de certaines banques, des fraudeurs parviennent à remplacer le numéro de téléphone mobile ou l'adresse e-mail de la victime par leur propre numéro de téléphone mobile ou adresse électronique, de sorte que le code d'activation est ensuite envoyé à un numéro de téléphone mobile du fraudeur. Pour ce faire, le fraudeur utilise généralement un ou plusieurs codes générés via une carte bancaire et un lecteur de carte. Ombudsfin estime que dans pareil cas, les banques concernées manquent à leur devoir de fournir un mécanisme de sécurité impliquant l'envoi d'un code d'activation ou de confirmation supplémentaire par SMS. En effet, d'après Ombudsfin, l'utilité d'un SMS ou d'un e-mail avec un code supplémentaire réside dans le fait qu'il permet à la banque de s'assurer que c'est bien le client lui-même qui effectue une opération ou installe une application mobile. Le fraudeur sera généralement déjà parvenu à tromper sa victime dans une première phase et à l'inciter à saisir des codes générés, par exemple, sur un faux site Web à l'aide d'un lecteur de carte. Il sera donc plus facile pour un fraudeur d'amener sa victime à saisir des codes supplémentaires générés par un lecteur de carte via ce site Web que de la convaincre de saisir un code envoyé au moyen d'un SMS indiquant clairement qu'il s'agit d'un code d'activation à ne partager avec personne. Ombudsfin recommande donc qu'en cas de modification du numéro de téléphone mobile du client, les banques concernées prennent les mesures nécessaires pour éviter ce genre de situation et vérifient au moins la légitimité du numéro de téléphone mobile modifié auprès du client. Une alternative pourrait être d'empêcher la modification de certaines données durant une période donnée après l'installation d'une nouvelle application.

4.4. Systèmes de détection des fraudes

Sur la base de l'article 2 du Règlement délégué AFC, les prestataires de services de paiement sont tenus de fournir des mécanismes de contrôle des opérations. Cette disposition énumère en outre une série de facteurs de risque que ces systèmes de détection des fraudes doivent prendre en considération. Le prestataire de services de paiement définira, par conséquent, des paramètres précis afin de détecter les éventuelles opérations suspectes. Si ses systèmes identifient certaines opérations comme étant suspectes, c'est-à-dire potentiellement frauduleuses, le prestataire de services de paiement doit arrêter les opérations concernées. Il prendra alors contact avec le payeur afin de déterminer si ce dernier souhaite effectivement procéder à l'opération en question. Cette démarche permet souvent d'éviter des opérations frauduleuses et donc de limiter les dommages. Lors du paramétrage des systèmes de détection des fraudes, le prestataire de services de paiement devra toujours trouver un équilibre entre sécurité et facilité d'utilisation. En effet, une détection des fraudes trop stricte peut entraîner, à tort, l'arrêt de certaines opérations de paiement légitimes.

Dans quelle mesure un prestataire de services de paiement peut-il être tenu pour responsable si ses systèmes de détection des fraudes ont manifestement échoué ? Ombudsfin est parfois confronté à des cas où un fraudeur parvient, souvent après l'installation d'une nouvelle application mobile, à effectuer des dizaines d'opérations pour un montant (à peu près) identique et au profit du même bénéficiaire dans un laps de temps (souvent) relativement court. Ombudsfin considère alors que les systèmes de détection des fraudes du prestataire de services de paiement auraient dû détecter la fraude (après cinq opérations identiques, par exemple). Dans ce contexte, il est néanmoins important de souligner que la détection des fraudes constitue une obligation de moyens et n'est pas une science exacte.

Ni la PSD II ni le Règlement délégué AFC ne prévoient de sanction pour le cas où les systèmes de détection des fraudes du prestataire de services de paiement ne seraient pas suffisamment performants. Sur la base de l'arrêt de la Cour de justice du 2 septembre 2021 mentionné précédemment, on pourrait même considérer que le régime de responsabilité prévu à l'article VII.44 du CDE est définitif et qu'il n'est pas possible d'invoquer le devoir de diligence du prestataire de services de paiement pour augmenter sa responsabilité. La Cour de justice a en effet jugé qu'un recours supplémentaire à un régime de responsabilité autre que celui prévu par la PSD I n'est pas compatible avec l'effet d'harmonisation maximale de la directive. Comme la PSD II vise également une harmonisation maximale, cet arrêt pourrait être appliqué par analogie à la réglementation actuelle.

Néanmoins, dans le cadre de sa mission de médiation, Ombudsfin vérifiera toujours si les systèmes de détection des fraudes ont été suffisamment performants ou non. S'il estime que les systèmes de détection des fraudes ont manifestement échoué, Ombudsfin demandera au prestataire de services de paiement concerné - sur la base du devoir de diligence qui lui incombe - d'intervenir dans tous les dommages encourus après le moment où, selon Ombudsfin, la fraude aurait dû être détectée par les systèmes de la banque. La doctrine préconise également que le régime de responsabilité relatif aux opérations de paiement non autorisées ayant eu lieu avec une authentification forte du client ne dépende pas uniquement du comportement du payeur, mais tienne également compte des efforts du prestataire de services de paiement, tant en termes de recouvrement que de détection des fraudes.

4.5. Mesures visant à limiter le nombre ou le montant des fraudes

Les banques s'efforcent de limiter le nombre de fraudes sur Internet et les dommages qui en découlent, par exemple en adaptant les processus de paiement et la procédure d'installation de l'application bancaire mobile. Ainsi, plusieurs banques ont suivi la recommandation d'Ombudsfin et intégré, lors de l'installation de l'application mobile, une étape supplémentaire impliquant l'envoi d'un lien ou code d'activation par SMS ou par e-mail au numéro de téléphone mobile ou à l'adresse e-mail connus de la banque. Certaines institutions financières proposent en outre une assurance contre la fraude, qui couvre aussi certaines fraudes pour lesquelles le payeur n'aurait (éventuellement) pas droit à une intervention au titre de l'article VII.44 du CDE.

Le monde politique appelle également à la mise en place de certains systèmes ou à l'optimisation des processus existants afin de prévenir la fraude sur Internet dans des cas précis ou de réduire les dommages qu'elle occasionne. À titre d'exemple, le secteur bancaire belge œuvre à l'introduction de la vérification de la concordance entre le numéro de compte IBAN et le nom du titulaire de ce compte. De même, on note la demande de simplifier la procédure de notification de la fraude pour le payeur et, plus récemment, une demande d'introduction d'un profil dit de « slow banking ».

a) Vérification de la concordance entre le numéro de compte IBAN et le nom du titulaire de ce compte

L'article VII.55/2, §1 du CDE dispose que le prestataire de services de paiement chargé d'exécuter un ordre de paiement n'est pas tenu de vérifier la concordance entre le numéro de compte bancaire et le bénéficiaire spécifiés. Sur la base de cette disposition, le prestataire de services de paiement n'est responsable que de l'exécution conformément à l'identifiant unique correct, c'est-à-dire le numéro de compte. Néanmoins, à l'instar des Pays-Bas et du Royaume-Uni, le secteur bancaire belge planche actuellement sur une vérification du nom du titulaire de l'IBAN, qui devrait entrer en vigueur l'année prochaine. Ainsi, lors de la saisie d'un ordre de virement, la banque vérifiera si le numéro de compte et le nom du bénéficiaire correspondent. Si tel n'est pas le cas, le payeur recevra une notification et aura alors la possibilité de confirmer ou non l'ordre de virement. Pour éviter trop de rejets d'opérations, le système tiendra compte, dans une certaine mesure, des éventuelles variations dans l'orthographe des noms et prénoms.

La vérification du nom du titulaire de l'IBAN a pour objectif de contribuer à prévenir les cas de fraude. Il convient toutefois de noter qu'une vérification du nom du titulaire de l'IBAN ne sera utile que pour prévenir les cas de fraude où le payeur lui-même, et non le fraudeur, effectue le virement via sa banque en ligne ou son application bancaire mobile. Ainsi, la vérification du nom IBAN permettra d'éviter certains cas de fraude à la facture, de fraude aux comptes à sécurité renforcée et de whaling. Elle ne sera évidemment d'aucune utilité dans les dossiers de phishing classiques, où un fraudeur utilise un faux site Web pour intercepter des données bancaires et des codes générés par une carte bancaire et un lecteur de carte afin d'effectuer lui-même des transferts et paiements.

Bien que la PSD II vise un effet d'harmonisation maximale, qui interdit en principe aux États membres de fournir une protection supplémentaire aux payeurs, elle n'empêche pas les prestataires de services de paiement de convenir entre eux d'une telle vérification du nom lié à l'IBAN. L'article 107 de la PSD II dispose en effet ce qui suit : « Les prestataires de services de paiement peuvent toutefois décider d'accorder des conditions plus favorables aux utilisateurs de services de paiement. » Les discussions se poursuivent au niveau européen afin d'introduire une obligation de vérification du nom lié à l'IBAN pour les virements instantanés.

b) Simplification de la procédure de notification : permanence téléphonique et système unique pour bloquer la carte bancaire, le compte et l'application.

La question de la notification de la fraude au prestataire de services de paiement a été abordée plus haut. Nous avons ainsi indiqué que, quoiqu'elles ne soient pas légalement obligées d'assurer une permanence téléphonique, tant que le payeur a la possibilité de notifier une fraude gratuitement et à tout moment, toutes les banques disposent désormais, depuis janvier 2023, d'un service téléphonique joignable 24h/24, 7j/7. Les coordonnées de ces services sont faciles à trouver sur le site Web de Card Stop.

Nous avons aussi regretté que le payeur devait effectuer plusieurs notifications distinctes de la fraude pour bloquer tous ses moyens de paiement. Or, une meilleure accessibilité téléphonique des banques et une procédure de notification plus simple pourraient conduire à un blocage plus rapide des instruments de paiement en cas de fraude et l'initiation plus rapide des démarches de recouvrement requises.

Le monde politique, par la voix des deux dernières secrétaires d'Etat au budget et à la protection des consommateurs, Mesdames Eva de Bleeker et Alexia Bertrand, a également fait savoir qu'il soutenait cette initiative.

c) Profil de «slow banking» [11]

L'ancienne secrétaire d'État Eva De Bleeker souhaitait que les institutions financières proposent aux consommateurs un profil d'utilisateur universel pour favoriser le «slow banking». Le consommateur pourrait ainsi définir des limites quotidiennes strictes, qui ne pourraient être augmentées que par l'intermédiaire d'une agence bancaire ou d'un guichet automatique. Une telle mesure n'entraînerait sans doute pas une réduction des occurrences de fraudes, mais pourrait limiter dans de nombreux cas le montant du dommage. L'actuelle secrétaire d'État Alexia Bertrand est également favorable à cette idée.

4.6. Recommandations

4.6.1. Recommandations générales aux consommateurs en matière de lutte contre la fraude

- Consultez régulièrement http://safeonweb.be/. Vous y trouverez de nombreux conseils utiles et mises en garde contre toutes les pratiques de fraude connues sur Internet.
- Vérifiez toujours l'adresse **e-mail complète** ou **l'URL complète** d'un site Web. La moindre faute d'orthographe ou l'utilisation de noms de domaine ou d'adresses e-mail atypiques sont des indices de fraude. Au moindre doute, cessez toute action ou communication et procédez aux vérifications requises via des recherches supplémentaires.
- Si quelque chose semble trop beau pour être vrai, c'est probablement le cas et il s'agit donc d'une fraude. Ne tombez pas dans le piège et cessez toute action ou communication.
- Un fraudeur peut utiliser des codes (générés par votre lecteur de carte) pour exécuter des paiements à distance, effectuer des virements via votre système de Home Banking ou même installer votre application bancaire sur son smartphone personnel. **Ne communiquez donc jamais à un tiers les codes générés par votre lecteur de carte.** Et sachez que votre banquier ne vous demandera jamais de faire cela.
- N'utilisez jamais votre lecteur de carte lorsque vous devez recevoir un paiement. Un lecteur de carte n'est **jamais** nécessaire pour ce type d'opération.
- Les touches et le texte de votre lecteur de carte vous en disent déjà beaucoup sur les actions que vous effectuez. Ce n'est pas pour rien que certaines touches sont libellées «Buy», «Sign», «Identify», «M1 = Identify = Appli 1», «M2 = Sign = Appli 2». Soyez conscient de ce que vous faites et lisez le texte éventuellement affiché sur votre lecteur de carte.

4.6.2. Recommandations au secteur en matière de lutte contre la fraude

- Ombudsfin recommande aux banques de s'assurer que le blocage d'une carte de paiement via Card Stop empêche toute utilisation physique ultérieure de la carte en question. En effet, il n'est pas logique qu'il soit encore possible, par exemple, de se connecter en ligne et d'effectuer des virements avec une carte bloquée.
- Ombudsfin recommande aux banques de rédiger leurs SMS consécutifs à l'installation d'une application mobile le plus clairement possible et d'informer les clients des actions qu'ils peuvent entreprendre pour bloquer l'application mobile au cas où ils ne l'auraient pas installée eux-mêmes.
- Les banques informent les clients de l'installation d'une application mobile en leur envoyant immédiatement un SMS. Ils ne sont toutefois pas toujours invités à activer cette application mobile. Ombudsfin a déjà recommandé aux banques de demander aux clients une activation supplémentaire d'une application nouvellement installée. Cela permettrait d'éviter la fraude dans de nombreux dossiers. Il est conseillé aux banques qui ne demandent pas d'activation supplémentaire, mais se contentent d'une simple notification relative à l'installation d'une nouvelle application, de laisser l'application en question inactive durant une période limitée (par exemple quelques heures) afin que le payeur ait encore une certaine possibilité de prendre connaissance du message en question dans un

[11] Il s'agit d'empêcher l'augmentation instantanée des limites de paiement enregistrées et d'obliger les particuliers à suivre une procédure plus formelle pour ce faire.

délai raisonnable et d'y réagir de façon appropriée.

- Pour renforcer la sécurité des opérations de paiement, les banques doivent adapter leur système de surveillance et veiller à ce qu'une alarme se déclenche lorsqu'une nouvelle application est installée et que le numéro de téléphone mobile du client est modifié très peu de temps après. Le 2e SMS de la banque avec le code d'activation peut en effet ne pas parvenir au client lui-même. Dans cette situation, il convient de prévoir un contact direct avec le client avant de procéder à toute opération.
- Ombudsfin se réjouit que plusieurs banques demandent désormais aux clients d'activer eux-mêmes l'installation de l'application. Il est toutefois regrettable que le 2e SMS contenant le code d'activation ne précise pas toujours clairement qu'il s'agit du code d'activation de l'application nouvellement installée. Nous notons cependant que quelques banques ont déjà fait des efforts pour clarifier les SMS en question.
- Prévoir des procédures de notification, de blocage et de recouvrement adaptées à la vitesse d'exécution actuelle des opérations.
- Expliquer clairement aux clients le fonctionnement du mécanisme de paiement et l'impact de l'utilisation du lecteur de carte.
- Lorsqu'une carte a été liée à un portefeuille de paiement en ligne, tel qu'Apple Pay, le blocage de cette carte doit la rendre inutilisable au sein de ce portefeuille de paiement en ligne.
- L'activation de la liaison d'une carte à un portefeuille de paiement en ligne requiert une action spécifique de la part du client. Une simple notification relative à cette activation, par exemple par SMS, n'est pas suffisante.

5. RUPTURE DE LA RELATION CLIENTELE

Ombudsfin a à nouveau eu à connaître, en 2022, de nombreux dossiers relatifs au blocage de comptes et/ou à la rupture unilatérale de la relation avec le client par l'institution financière (198 dossiers). Ces mesures constituent souvent un « outil » pour leur permettre de respecter leurs obligations de vigilance reprises dans la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces. Eu égard au droit des banques de mettre fin à tout moment à la relation bancaire, sans avoir à justifier cette décision, le rôle d'Ombudsfin se limite, en pratique, à contrôler si les formes et délais conventionnels relatifs à la résiliation de la relation bancaire ont été respectés. Sur ce point, Ombudsfin s'en réfère à son exposé détaillé dans le rapport annuel de 2021, p. 13.

6. LIMITATIONS DES OPERATIONS EN ESPECES

Nous avons, dans notre rapport annuel précédent, déjà mis en exergue les barrières mises par certaines banques aux versements ou retraits en cash (voir point 5.4. du rapport annuel 2021). Lors de la période sous revue, nous avons rencontré quelques dossiers où les plaignants s'étonnaient de ne pas pouvoir redéposer auprès de leur banque le même montant (conséquent) que celui qu'ils avaient retiré quelques temps auparavant. Les arguments avancés par les plaignants sont divers (l'opération envisagée n'a pas pu avoir lieu, retrait panique à cause de la guerre en Ukraine ...). Les banques concernées ont refusé le versement en mettant en avant leurs obligations anti blanchiment (et plus particulièrement l'obligation de vérifier l'origine des fonds) et nous ont indiqué avoir attiré l'attention de leurs clients, lors du retrait, sur le fait qu'un dépôt ultérieur de ces fonds risquait de poser problème. Cette communication ayant été faite oralement, Ombudsfin n'est évidemment pas en mesure de vérifier si elle était suffisamment claire pour ne pas induire le client en erreur.

Dans cette matière, les recommandations suivantes ont été formulées :

- Les restrictions concernant les opérations en espèces dans une banque doivent être définies aussi clairement que possible dans les conditions générales.

- Si une banque n'autorise plus les retraits d'argent liquide au guichet, l'alternative proposée (par exemple, les distributeurs automatiques de billets) doit être suffisamment sécurisée.

7. PAIEMENTS – AUTRES PROBLEMATIQUES

Les sanctions prises par l'Union européenne contre la Russie, et plus particulièrement le gel des avoirs russes appartenant à certaines personnes et l'interdiction d'exécuter des transferts d'argent vers ou de la Russie ont donné lieu à différentes plaintes introduites par des consommateurs. Les uns estimaient avoir été injustement mis sur une « liste noire » alors que les autres se plaignaient de ne pouvoir obtenir le remboursement effectif de sommes versées à des sociétés russes pour des prestations qui n'avaient pu être effectuées suite aux sanctions prises (ex : paiement de billets d'avion pour un vol vers Moscou avec la société Aéroflot).

Dans le premier cas, Ombudsfin a indiqué aux plaignants qu'ils pouvaient, le cas échéant, demander à bénéficier d'une dérogation auprès de l'administration générale de la trésorerie du SPF Finances. Dans le second cas, Ombudsfin n'a pu que constater que les établissements financiers agissaient en conformité avec les sanctions qui s'imposaient à eux.

Ombudsfin a formulé les recommandations suivantes dans les dossiers de paiement :

- Lorsque l'exécution d'une opération est retardée, la banque doit en informer le client.
- Les institutions de paiement devraient mettre en place des procédures d'identification suffisamment concluantes pour prévenir la fraude à l'identité et identifier suffisamment le bénéficiaire d'un virement international au moment de l'encaissement.

8. LES GROUPES VULNÉRABLES

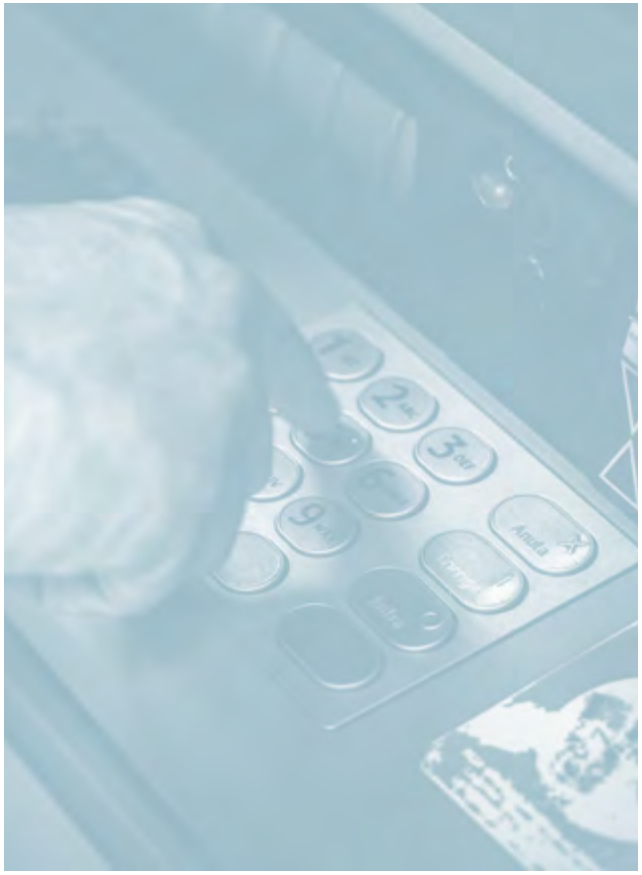
Au cours de l'année 2022, Ombudsfin a de nouveau reçu de nombreux signaux de la part de certaines organisations sociales selon lesquels les personnes en situation de vulnérabilité financière et sociale rencontrent de plus en plus de problèmes dans leur recherche de services bancaires adaptés à leurs besoins.

Ombudsfin a pris note de ces signaux. Ombudsfin est conscient de l'existence de ces problèmes, mais ne peut les confirmer par ses propres activités.

En effet, nous devons noter que, même en 2022, peu de plaintes ont été déposées par des personnes appartenant à ces groupes. Cela peut être dû à une connaissance insuffisante de l'existence et du rôle de notre service. C'est évidemment regrettable. Nous tenons à rappeler aux CPAS et aux autres institutions d'appui qu'ils peuvent introduire une plainte auprès d'Ombudsfin au nom et pour le compte des personnes qu'ils aident, mais après avoir préalablement introduit la plainte auprès du service de plaintes compétent de la banque concernée.

À cet égard, les recommandations suivantes ont été formulées :

- Les procédures devraient être conçues de manière à ce qu'un mineur étranger non accompagné (ci-après : MENA) ne soit pas inutilement bloqué en termes d'opérations financières. Si le MENA ne vit pas avec son tuteur (ce qui est généralement le cas), la banque doit prévoir l'envoi de la carte au tuteur.
- Dans la pratique, les banques ne devraient pas être plus strictes en termes d'exigences d'identité lors de l'ouverture d'un service bancaire de base que les exigences fournies dans la FAQ de Febelfin.



9. CREDITS

Comme les années précédentes, Ombudsfin a également traité un certain nombre de plaintes relatives à des crédits aux consommateurs en 2022, qu'il s'agisse de crédits hypothécaires ou de crédits à la consommation.

En ce qui concerne les plaintes relatives aux crédits, nous attirons particulièrement l'attention sur les points suivants :

Crédit hypothécaire - désolidarisation

En matière de crédit hypothécaire, Ombudsfin constate encore cette année que, dans le cadre d'une séparation entre deux partenaires qui sont co-crédité(e)s et co-propriétaires d'un bien immeuble donné en garantie de ce crédit, le(a) co-crédité(e) qui cède ses parts dans l'immeuble concerné à son ancien(ne) partenaire omet souvent de régler le sort du crédit et d'obtenir préalablement à cette cession de droit indivis l'accord de la banque de le(a) désolidariser de ce crédit, pensant que les termes de la convention entre ex-époux suffisent à la tenir indemne de toute obligation.

La banque n'est pourtant jamais tenue de faire droit à une telle demande de désolidarisation. Son acceptation dépend avant tout de la capacité financière du (de la) partenaire qui reprend seul(e) l'immeuble et le crédit. Une telle demande impose à la société prêteuse de constituer un nouveau dossier de crédit et de procéder à une nouvelle analyse de la capacité financière du (de la) repreneur(euse), puisque celle-ci est amenée à rembourser, postérieurement à la séparation, l'intégralité du crédit.

Ombudsfin insiste sur l'importance d'obtenir cet accord écrit de désolidarisation de la banque en cas de cession de droits indivis dans un immeuble grevé d'une hypothèque car celui (celle) qui cède ses droits n'est plus propriétaire et s'il (elle) n'a pas obtenu l'accord écrit de la banque d'être « déchargé(e) » du crédit, il (elle) reste malgré tout tenu par ce crédit. Les conséquences peuvent être dramatiques pour cette personne qui ne détient plus de droits réels dans l'immeuble et n'en jouit plus mais peut à tout moment être appelée par la banque à rembourser le crédit. De plus, sa capacité financière est ainsi réduite et cela peut être un obstacle pour obtenir un autre crédit pour acquérir un autre bien.

Pour cette raison, Ombudsfin invite les consommateurs à être actifs dans leur demande de désolidarisation et les banques à faire preuve de plus de créativité pour leur permettre de conserver leurs garanties mais éviter les conséquences dramatiques de cette situation pour celui qui n'est plus propriétaire.

Crédit à la consommation –usurpation d'identité

Parmi les escroqueries existantes sur internet, l'usurpation d'identité est très répandue ces dernières années. Elle est, en effet, rendue possible et facilitée par le nombre important d'informations personnelles qui transitent sur le net. L'usurpation d'identité en ligne va ainsi se traduire par la récupération par l'escroc de suffisamment de données personnelles relatives à une autre personne pour pouvoir réaliser des opérations financières au nom de cette dernière, la victime : l'ouverture d'un compte bancaire, la demande d'un crédit à la consommation, la demande d'envoi d'une nouvelle carte de crédit à une adresse autre que celle de la victime... Les conséquences d'une telle usurpation peuvent évidemment être gravement dommageables pour la victime : intentement d'une procédure de recouvrement de créances pour des sommes non perçues, fichage négatif à son nom auprès de la Centrale des Crédits aux Particuliers, poursuite judiciaire, ...).

Il est donc indispensable de réagir au plus vite pour les victimes, en déposant plainte à la police pour usurpation d'identité et, en même temps, en notifiant l'incident à la banque ou la société prêteuse.

Certains plaignants se tournent vers Ombudsfin en cas de fichage négatif ou lorsqu'ils reçoivent un rappel de paiement d'une société prêteuse pour un crédit à la consommation dont ils n'ont pas connaissance et dont ils n'ont pas bénéficié. Lorsque les victimes se rendent compte que leur identité a été usurpée pour conclure ledit crédit, elles portent alors plainte à la police pour usurpation d'identité et réclament l'annulation du contrat de crédit, via Ombudsfin, auprès de la société prêteuse pour échapper au recouvrement des montants à rembourser mais dont ils n'ont pas bénéficié. Lorsqu'une plainte est introduite chez Ombudsfin, les banques acceptent généralement de suspendre le recouvrement des sommes empruntées dans l'attente du résultat de la procédure pénale.

Le dossier pénal est, dans la plupart des cas, classé sans suite car l'usurpateur reste inconnu. Si les pièces rapportées par les deux parties démontrent à suffisance que l'usurpation d'identité est tout à fait vraisemblable,

Ombudsfin invite toutefois la société prêteuse à accorder à la victime l'annulation du crédit à la consommation et la suppression du fichage au volet négatif de la Centrale des Crédits aux Particuliers. Dans la plupart des cas, il est fait droit à une telle demande.

Dans d'autres dossiers, les plaignants constatent qu'un compte a été ouvert en ligne en usurpant leur identité et qu'une carte de débit a été utilisée, mettant ledit compte en dépassement non autorisé à la suite d'opérations non autorisées par le titulaire du compte. Les plaignants contestent généralement avoir demandé et reçu une telle carte de débit. Dans ces cas, la carte a effectivement souvent été envoyée à une autre adresse, celle de l'usurpateur ou d'un complice.

Si ces faits sont clairement établis, Ombudsfin invoque l'article VII.39, 6° du Code droit économique qui prévoit que la société prêteuse « supporte le risque lié à l'envoi d'un instrument de paiement à l'utilisateur de services de paiement ou de tout moyen qui en permet l'utilisation, en particulier toute donnée de sécurité personnalisée de celui-ci. » et demande la restitution des sommes ainsi détournées. Ombudsfin invite également la banque à supprimer l'éventuel fichage au volet négatif de la Centrale des Crédits aux Particuliers, quelle que soit l'issue pénale de la plainte déposée.

10. INVESTISSEMENTS

Parmi les plaintes relatives aux investissement, on épinglera plus particulièrement les deux problématiques suivantes :

A. Impossibilité de négociation de penny stocks via la banque :

Les titulaires d'actions dont la valeur marchande est très limitée, également appelées penny stocks, rencontrent parfois des difficultés à vendre leurs titres par l'intermédiaire de la banque qui les détient en portefeuille. Ils n'ont alors d'autre choix que de transférer leurs titres vers une autre institution financière acceptant le négoce de ces titres. Malheureusement, un tel transfert entraine des frais et il s'avère par ailleurs qu'il n'est pas aisé de trouver un intermédiaire acceptant de prendre ces titres en dépôt.

Le Collège d'experts d'Ombudsfin a été amené en 2022 à analyser une plainte concernant l'impossibilité pour un client de vendre ses actions auprès de sa banque.

Au mois d'octobre 2021, le plaignant souhaitait vendre ses actions car elles représentaient une contre-valeur importante. Il a signé un ordre de vente mais, un jour plus tard, la banque lui a annoncé qu'il n'était pas possible de vendre ces actions. Le plaignant a alors fait savoir que la banque ne l'en a jamais informé. Par ailleurs, ce dernier a demandé à d'autres banques si elles pouvaient réaliser une opération sur ces actions et il apparait que celles-ci étaient parfaitement négociable auprès d'elles. En revanche, les règles ayant été durcies pour les transferts d'actions depuis quelques années, ces titres n'étaient pas transférables.

Dans le cadre de la médiation, la banque a confirmé qu'il est possible que certains ordres ne puissent être exécutés en raison, entre autres, de règles spécifiques et/ou de choix politiques interne de la banque et/ou de ses propres intermédiaires (courtiers). C'est le cas pour les penny stocks. En effet, de nombreux courtiers refusent d'exécuter les ordres sur ces types d'actions car il s'agit souvent d'actions de sociétés moins transparentes sur lesquelles peu d'informations sont disponibles et où le risque de fraude et d'abus de marché est très élevé.

Néanmoins, la banque nous a expliqué que ces restrictions de vente n'affectaient pas le droit de transférer les titres à une autre institution financière. Par conséquent, bien que la vente par la banque ne soit pas possible, le transfert des titres reste une alternative possible à condition de trouver une institution capable et désireuse d'accepter les titres en question.

Sur le plan juridique, la banque estime que sa responsabilité ne peut être engagée. Cette dernière s'appuie notamment sur ses conditions générales, qui stipulent que le prestataire de services n'assume pas d'obligation de résultat en matière de négociabilité des actions, ainsi que son absence de responsabilité en cas de faute légère.

Le Collège d'experts estime pour sa part que la banque ne peut être tenue responsable de l'impossibilité de négocier les actions du plaignant. Cependant, le Collège d'experts est d'avis que la banque a commis une erreur grossière en n'informant pas à temps le client de la future non-négociabilité de ces actions, par son intermédiaire,

ni de la nécessité de transférer ces actions (en vue de leur négociation par un autre prestataire de services). En effet, fournir des informations claires sur les changements concernant la négociabilité des titres (que la banque devait être en mesure d'évaluer en tant que prestataire de services professionnel) fait partie de l'essence du devoir de diligence qui incombe au dépositaire. Le Collège d'experts estime que le défaut de communication de ces informations essentielles peut être qualifié de faute lourde et que la banque ne peut dès lors s'exonérer de sa responsabilité en vertu des conditions générales bancaires, qui n'excluent sa responsabilité qu'en cas de faute légère.

Le Collège d'experts note également que, même si une autre entité sur laquelle le prestataire de services s'appuie pour l'exécution de l'ordre a commis une erreur (quod non), le prestataire de services ne peut pas s'appuyer sur cette erreur pour échapper à sa responsabilité envers son client. En effet, le prestataire de services est responsable des erreurs commises par les entités auxquelles il fait confiance pour l'exécution des ordres de ses clients.

Le Collège d'experts a considéré qu'une indemnité forfaitaire, en plus du remboursement des frais payés pour la garde des actions en question, représenterait une solution équilibrée et équitable pour les deux parties. Le Collège d'experts a en effet estimé qu'il n'était pas certain que, dans le cas où le plaignant aurait été informé à temps, il aurait eu la possibilité de transférer les actions en question et de les vendre par l'intermédiaire d'un autre prestataire de services au prix en vigueur à la date où l'ordre de vente irréalisable a été donné.

B. Suspension des opérations de certificats d'actions émis par une banque :

Au cours de l'année 2022, Ombudsfin a été amené à traiter plusieurs plaintes relatives à la suspension des ordres de vente des certificats d'actions d'une banque. Cette impossibilité de vendre les titres en question entraine un préjudice important chez leurs détenteurs qui n'ont plus l'occasion de disposer de leurs fonds.

En effet, à ce jour, les certificats d'actions de la banque en question ne sont pas cotés sur un marché réglementé ou une plateforme de négociation multilatérale (Multilateral Trading Facility, en abrégé MTF). La banque facilite les opérations concernant les certificats d'actions et est ainsi la seule contrepartie effective pour les ordres d'achat et de vente.

Le fait que les certificats représentatifs d'actions ne soient pas cotés a évidemment des conséquences sur la négociabilité de ces certificats, qui présentent un « déficit de liquidité ».

Jusqu'ici, la banque avait toutefois toujours facilité les opérations sur les certificats de dépôt pour lesquelles elle était la seule contrepartie pour les ordres d'achat et de vente.

La négociation des certificats a toutefois été suspendue à partir du mois de janvier 2021. La banque en donne la raison suivante : La raison de cette suspension est, entre autres, la volatilité du marché (notamment dans le contexte de la pandémie de la Covid-19), un déséquilibre entre les ordres d'achat et de vente et la limite/restriction légale pour le rachat de ces certificats de dépôt, à savoir 3% du capital émis (conformément au règlement de l'Union européenne pour les établissements de crédit, connu sous le nom de CRR).

Estimant que le système actuel a atteint ses limites, la banque a décidé de cesser de négocier les certificats et de faciliter les échanges mais de les inscrire en contrepartie sur une plateforme de négociation multilatérale, c'est-à-dire un MTF. Cela devrait améliorer la négociabilité des certificats sur la base d'un prix déterminé par l'offre et la demande mais cette cotation ne pourra malheureusement être effective avant un délai important (plus d'un an) en raison des contraintes juridiques et techniques et de la complexité d'un tel processus.

Ombudsfin note toutefois que le risque de liquidité et le risque d'une éventuelle suspension de la négociation sont tous deux mentionnés dans le prospectus de référence publié par la banque. On ne peut donc, sur ce point, faire de reproches à la banque.

Remise administrative de 30%

La banque est légalement tenue de déclarer la valeur économique des certificats à la fin de chaque année civile aux autorités fiscales compétentes et aux détenteurs de certificats. Pour répondre aux exigences de l'administration fiscale, la banque a estimé la valeur économique du certificat au 31 décembre 2021, en tenant compte de la suspension de la négociation depuis le début de l'année 2021 et de

l'impact de cette suspension sur la liquidité des certificats. Pour ce faire, la banque a pris en compte les avis d'experts externes, des précédents dans d'autres entreprises et son propre jugement professionnel. Sur cette base, la banque a décidé d'appliquer une remise administrative de 30% sur la valeur des certificats et de les valoriser à 59 €. Cette valeur comptable ne préjuge évidemment pas du prix des certificats lors d'une future cotation sur un MTF.

Programme de rachat restreint

Par ailleurs, le 15 février 2022, la banque avait annoncé les détails d'un programme limité de rachat de certificats d'actions. Ce programme aurait permis aux détenteurs de certificats de vendre leurs certificats, sans avoir à attendre l'entrée en vigueur de la négociation sur un MTF. Le prix de ce rachat avait également été fixé à 59 € par certificat, soit le même prix que celui qui a été fixé pour les raisons fiscales et administratives mentionnées ci-dessus. Ce prix tenait donc compte d'une décote de 30% pour refléter le manque de liquidité du marché. Ce manque de liquidité est en effet un élément qui peut justifier une décote. Ce niveau est apparemment basé sur des éléments objectifs, cependant, nous devons souligner qu'Ombudsfin n'a pas reçu copie des avis reçus.

Il s'avère que par la suite, la banque a annoncé le retrait de ce projet de programme de rachat restreint de certificats d'actions (à hauteur d'un montant de 14,4 millions d'euros).

Suite au retrait du projet précité, la banque a annoncé en contrepartie qu'elle proposait de payer un dividende extraordinaire de 1,01 € (avant retenue d'impôt le cas échéant) par certificat d'action. Au total, un montant de 14,4 millions d'euros sera distribué, ce qui correspond à la marge de manœuvre dont la banque disposait pour le rachat de ses propres certificats d'actions. Cette mesure est évidemment loin de répondre aux souhaits des actionnaires.

Conclusion

Ombudsfin souhaite attirer l'attention des investisseurs sur le fait qu'un placement en actions est toujours risqué, quel qu'en soit l'émetteur.

Ombudsfin ne peut que constater que la situation actuelle est effectivement désagréable pour tous les actionnaires, puisqu'elle ne leur permet pas de vendre leurs titres à un prix correct. La banque concernée en est également consciente et s'efforce de trouver des alternatives pour aider ses actionnaires. Malheureusement, ces alternatives nécessitent beaucoup de temps pour être mises en place.

Compte tenu de ce qui précède, du fait qu'une action est un instrument financier risqué et que la possibilité de suspendre la négociation des titres était expressément prévue dans le prospectus, Ombudsfin a estimé qu'il n'y avait, à ce stade, pas (encore) lieu de demander à la banque une quelconque intervention dans le cadre des plaintes qui lui ont été adressées à ce sujet.

Toutefois, l'avis d'Ombudsfin pourrait bien sûr être reconsidéré si les différentes mesures annoncées par la banque ne devaient pas voir le jour dans un délai raisonnable.

11. VARIA

Ainsi qu'il ressort des statistiques, Ombudsfin a également traité en 2022 nombre de dossiers de succession (49) et de dossiers relatifs à des garanties locatives (24). Nous nous attarderons ci-dessous sur quelques problématiques qui ont été régulièrement abordées dans les dossiers de plainte.

Garanties locatives

En ce qui concerne les dossiers de garanties locatives, Ombudsfin souhaite attirer l'attention sur un problème spécifique, à savoir le défaut par la banque de pouvoir rapporter la preuve que le compte de garantie n'existe plus, et ce à cause de l'expiration, depuis la prétendue clôture dudit compte, du délai légal de conservation des données de 10 ans.

Ombudsfin observe que, dans certains cas, il n'est pas possible de réconcilier le point de vue du bailleur, qui présente des documents constituant à tout le moins un commencement de preuve de l'existence, au jour de l'introduction de la plainte, d'une garantie locative, et celui de la banque, qui se borne à constater qu'elle ne retrouve aucune trace de cette garantie dans ses livres et en déduit que le compte de garantie a dû être clôturé au moins 10 ans auparavant. Ce point de vue de la banque, sans élément concret et sans prouver que le bailleur a marqué accord sur la libération des fonds, rend difficile une analyse complète de ces dossiers.

Lorsque le plaignant est le bailleur, il lui est généralement difficile, voire impossible, de fournir des preuves

complémentaires (en sus des documents d'ouverture de compte ou d'un document non rempli de libération des fonds). Les comptes de garantie sont en effet toujours ouverts au nom du locataire, ce qui signifie que le bailleur ne reçoit pas d'informations périodiques sur le (solde du) compte ni sur le fait qu'il reste bien bloqué après son ouverture. Le bailleur n'est en principe activement impliqué que lors de l'ouverture du compte et de la libération des fonds. Si une erreur advient entre l'ouverture et la libération souhaitée, le bailleur n'en est évidemment pas informé et il peut donc, de bonne foi, penser que la garantie locative est toujours restée en vigueur pendant toute la durée du bail (durée qui, en cas de bail d'habitation, peut excéder 10 ans). Dans certains dossiers soumis à notre examen, il s'avère toutefois que cette supposition est erronée.

Dans ces dossiers, la banque ne peut souvent apporter aucune preuve à l'appui de ses dires (à cause du délai de conservation légal) alors que le bailleur (ou le locataire) peut avancer quelques éléments pertinents à l'appui de sa requête, à savoir la remise en état de la garantie locative, afin qu'il puisse faire valoir ses droits. Dans les dossiers dans lesquels, sur la base des arguments avancés et des documents produits par le requérant, Ombudsfin pouvait présumer que la banque avait commis une erreur dans la procédure suivie, par exemple, lors de la libération de la garantie, une solution adéquate a pu être obtenue de la part de la banque.

Ombudsfin craint toutefois que cette problématique continue à exister dans les prochaines années si le délai de conservation des données n'est pas adapté pour les comptes de garantie locative.

Succession : instruction notariale avec décharge de responsabilité, non exécutée

Dans les dossiers de succession, Ombudsfin a constaté à plusieurs reprises en 2022 que, malgré des instructions claires données par le notaire instrumentant la succession avec décharge de responsabilité, les banques n'obtempèrent pas et imposent le respect de leurs procédures internes, c'est-à-dire que les instructions doivent être données directement à la banque par les héritiers au terme d'un accord conclu et signé entre eux, même si une décharge de responsabilité est donnée par le notaire. Certaines banques exigent que leurs propres formulaires soient utilisés et à défaut, refusent d'exécuter lesdites instructions.

Ombudsfin s'est déjà prononcé plusieurs fois ce point et ne partage pas la position des banques.

Ombudsfin rappelle qu'un notaire est un officier public, nommé par le Roi, qui exerce cette fonction publique dans le cadre d'une profession libérale. Ainsi, il exerce un pouvoir public en établissant des actes authentiques qui ont la force d'un jugement mais il donne aussi des conseils et tente d'éviter les conflits. C'est précisément à ce titre qu'il donne les instructions sous décharge de responsabilité de la banque et qu'il dispose de comptes-tiers et de comptes rubriqués au nom de ses clients/héritiers/succession.

Ombudsfin constate malheureusement que le formalisme appliqué par les banques au nom de leur devoir de diligence et de prudence, entraine régulièrement la dégradation des relations entre héritiers et engendre parfois le blocage, pendant une longue durée, de la succession et du partage à la suite du refus d'exécuter les instructions du notaire.

Produits d'épargne

Le nombre de plaintes relatif aux produits d'épargne reste très limité (16 dossiers en 2022), même si différents épargnants ont été confrontés en 2022, contre leur volonté, à la clôture définitive de leurs comptes. Rabobank Groep a en effet décidé en 2021 de stopper les activités de Rabobank.be et de clôturer définitivement tous les comptes d'épargne en juillet 2022. Une telle cessation d'activité va souvent de pair avec nombre de questions et de plaintes de clients. Ombudsfin n'a pourtant reçu que 2 plaintes relatives à cette clôture et y voit un lien avec la communication claire, réalisée en temps opportun et répétée, de Rabobank à ce sujet.

Rabobank a en effet informé ses clients plus d'un an à l'avance de cette cessation et de son impact sur les dépôts. Rabobank a, via une période transitoire d'un an (de juillet 2021 à juillet 2022), tout fait pour donner à ses clients suffisamment de temps pour rechercher des alternatives et leur a communiqué des conseils simples et utiles pour éviter qu'ils perdent leur prime de fidélité. Les épargnants ont également été accompagnés tout au long de ce processus par différentes lettres et e-mails de la banque ainsi que par des instructions claires sur son site web expliquant comment l'épargnant pouvait simplement transférer son solde sur un autre compte et pouvait clôturer son compte à un moment favorable, compte tenu de l'échéance des primes de fidélité.

12. FIN-NET : PLAINTES TRANSFRONTALIERES

Ombudsfin fait partie de FIN-NET, le réseau européen pour la résolution des litiges transfrontaliers en matière de services financiers.

FIN-NET veille à la collaboration entre les services de médiation du secteur financier de la plupart des États membres européens en vue de régler les litiges transfrontaliers. Pour la Belgique, outre Ombudsfin, l'Ombudsman des assurances est aussi membre du réseau FIN-NET.

De plus amples informations sur FIN-NET sont disponibles sur le site de la Commission européenne: https://finance.ec.europa.eu/consumer-finance-and-payments/retail-financial-services/financial-dispute-resolution-network-fin-net_fr

12.1. Procédure

Si Ombudsfin est saisi d'un dossier destiné au service de médiation d'un autre État membre européen, membre de FIN-NET, il transmettra ce dossier à l'instance compétente à condition que ce dernier soit suffisamment documenté. Si le dossier n'est pas complet, Ombudsfin communiquera les coordonnées de l'organe compétent.

Chaque pays a ses particularités et ses propres structures de règlement alternatif des litiges. Toutefois, dans certains cas, il est impossible de rediriger vers un collègue européen. En effet, certains pays ne disposent pas d'organisme comme Ombudsfin couvrant toutes les matières en droit bancaire et financier. Dans certains pays, comme la France, l'organisme compétent est logé au sein même de l'institution financière, sans recours possible auprès d'un organisme indépendant. Dans de tels cas, l'organisme interne ne fait pas partie du réseau FIN-NET et Ombudsfin essayera tout de même d'orienter le requérant vers l'organisme de plainte interne.

12.2. Exemples concrets

En 2022, Ombudsfin a reçu 1 dossier dans lequel la procédure FIN-NET a été utilisée. Ce dossier concernait une institution financière espagnole. La plainte concernait les conditions et la tarification d'un compte à vue.

13. COLLABORATION

13.1. BELGIQUE

13.1.1. Service de Médiation pour le Consommateur

Le Service de Médiation des services financiers (Ombudsfin) est membre du Comité de Direction du Service de Médiation pour le Consommateur, créé par la loi du 4 avril 2014 et ayant pour vocation :

- D'informer les consommateurs sur les possibilités de règlement extrajudiciaire des litiges de consommation;
- De réceptionner les plaintes et soit les transmettre à l'entité compétente en la matière, soit les traiter lui-même;
- D'intervenir dans le traitement des plaintes pour lesquelles aucune entité qualifiée n'est compétente.

Ombudsfin est une entité qualifiée au sens de la loi et reste compétent dans le domaine des services bancaires, des crédits, des investissements et des paiements.

13.1.2. OMBUDSMAN.BE

L'ombudsman fait partie d'Ombudsman.be, le réseau belge des médiateurs. Ceci regroupe les médiateurs publics et privés ayant souscrit aux principes de base de la fonction d'ombudsman.

Si un consommateur s'adresse à un ombudsman qui n'est pas compétent pour régler son problème, ce dernier veillera à ce que le litige soit soumis à l'ombudsman compétent.

De plus amples informations sont disponibles sur le site www.ombudsman.be

13.1.3. BELMED

Ombudsfin est affilié à Belmed.

Belmed est un portail numérique fondé par le SPF Économie qui offre une information complète sur les instances de médiation existantes et la manière dont un conflit peut être géré à l'amiable. Une demande de médiation peut être introduite en ligne via le site suivant : https://economie.fgov.be/fr/themes/line/belmed-mediation-en-ligne/belmed-votre-partenaire-en

13.2. EUROPE

13.2.1. FIN-NET

Ombudsfin participe activement aux deux réunions FIN-NET que la Commission européenne organise chaque année.

Pour davantage d'explications, nous renvoyons au chapitre 11 : « FIN-NET : plaintes transfrontalières ».

13.2.2. ODR

La plateforme ODR est une plateforme lancée en 2016 par la Commission européenne et destinée aux consommateurs et aux professionnels effectuant des opérations en ligne dans l'UE.

L'objectif est d'aider gratuitement les particuliers à résoudre une plainte concernant des biens ou des services achetés en ligne dans l'UE, sans aller en justice. Dans certains pays, il est aussi possible, en tant que professionnel, de déposer une plainte contre un consommateur.

(https://webgate.ec.europa.eu/odr/main/?event=main.complaints.odrList)

13.3. INTERNATIONAL

Ombudsfin est membre d'INFO, l'International Network of Financial Services Ombudsman Schemes, qui regroupe les services de règlement alternatif des litiges dans le domaine financier au niveau mondial. Pour de plus amples informations : www.networkfso.org.

14. MOYENS FINANCIERS

Au moment de la publication de ce rapport annuel 2021, les comptes annuels de l'exercice comptable d'Ombudsfin asbl de 2022 n'ont pas encore été approuvés par l'assemblée générale. Dès que ceux-ci auront été approuvés, les grandes lignes en seront publiées sur le site web d'Ombudsfin sous la forme d'un addendum au rapport annuel (www.ombudsfin.be – Publications – Rapports annuels).

Il est toutefois possible de donner un aperçu du budget établi pour 2022:

	Budget 2022
Revenus	
Cotisation fixe membres Ombudsfin asbl	657.083,50
Cotisation variable membres Ombudsfin asbl	657.083,50
Revenus totaux	**1.314.167,00**
Dépenses	
Frais de personnel + honoraires	1.162.551,00
Frais de fonctionnement	136.616,00
Moins-values factures impayées + notes de crédits	15.000,00
Dépenses totales	**1.314.167,00**

Lors du calcul et de l'approbation du budget, il est toujours gardé à l'esprit qu'en tant qu'entité qualifiée indépendante et impartiale, Ombudsfin asbl doit disposer d'un budget propre et spécifique, qui est suffisant pour l'accomplissement de ses missions (voir article 2 de l'Arrêté Royal du 16 février 2015).

Le budget nécessaire est demandé aux membres d'Ombudsfin asbl au moyen d'une cotisation fixe et d'une cotisation variable, celles-ci sont établies annuellement par le conseil d'administration et ratifiées par l'assemblée générale d'Ombudsfin asbl. Chaque membre d'Ombudsfin asbl est redevable d'une cotisation fixe. La cotisation variable n'est réclamée qu'aux membres pour lesquels Ombudsfin a enregistré des plaintes recevables au cours de l'année civile précédente.

North Gate II
Avenue du Roi Albert II n°8, boîte 2
1000 Bruxelles

ombudsman@ombudsfin.be

www.ombudsfin.be