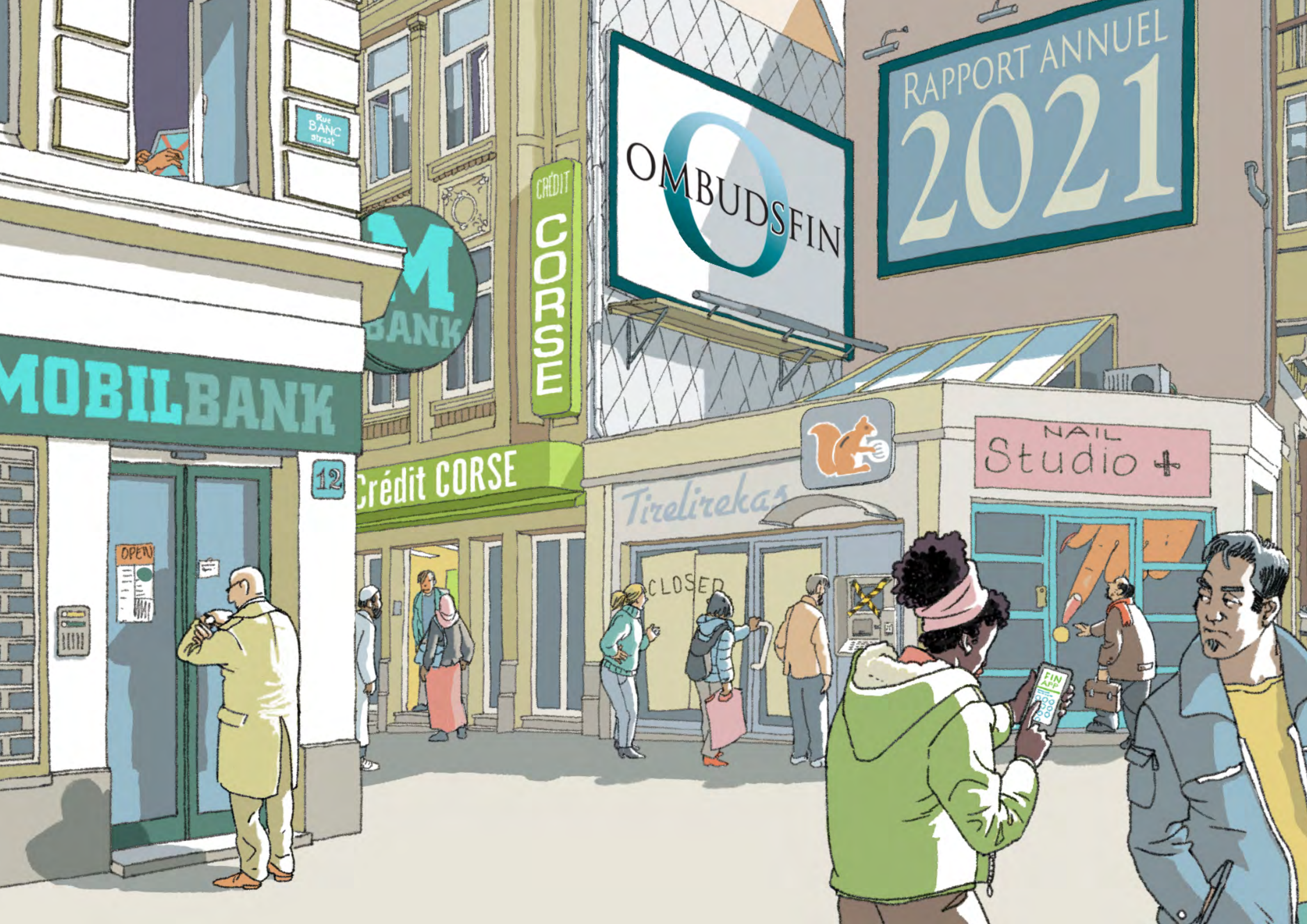

RAPPORT ANNUEL
2021
OMBUDSFIN
MOBILBANK
Rue BANC straat
BANK
CRÉDIT CORSE
Crédit CORSE
12
OPEN
CLOSED
Tirelirekas
NAIL Studio
FIN APP

SOMMAIRE

AVANT-PROPOS

Mesdames et Messieurs,

J'ai le plaisir de vous présenter notre rapport annuel 2021, le premier depuis que je suis devenu l'Ombudsman du secteur financier, en juillet 2021.

Durant ces premiers mois, deux choses m'ont particulièrement impressionné : d'une part, le professionnalisme, le dévouement et l'empathie de mes nouveaux collaborateurs et, d'autre part, le désarroi de nombreux plaignants, victimes de toutes sortes de fraude ou simplement en peine de trouver un interlocuteur pour régler leurs problèmes.

Nonobstant l'augmentation importante du nombre de plaintes introduites et la complexité de nombre d'entre elles, je constate par ailleurs que nous avons pu respecter les délais qui nous sont légalement impartis pour traiter tous les dossiers qui nous ont été confiés et que nous avons, sans relâche, essayé d'arriver à des solutions équilibrées, respectueuses des intérêts des différentes parties.

Si, comme vous pourrez le lire dans la suite du présent rapport, nous avons obtenu de belles avancées, il ne nous faut néanmoins pas cacher quelques problèmes récurrents.

Ainsi, dans les nombreux dossiers de fraudes qui nous sont soumis, force est de constater que les établissements de crédit continuent à interpréter la notion de négligence grave, qui les dispensent d'intervenir financièrement, d'une manière qui nous paraît excessive. S'il est vrai que les campagnes d'information sur les risques de fraude se multiplient, il est tout aussi vrai que les techniques des fraudeurs se professionnalisent d'année en année et qu'ils excellent à surfer sur les émotions de leurs victimes pour arriver à leurs fins. De plus en plus nombreux sont donc les consommateurs à continuer à tomber dans le panneau, parfois pour des montants fort élevés.

Nous sommes également assez démunis lorsqu'il s'agit d'aider les consommateurs qui font l'objet d'une rupture de relation bancaire et qui aimeraient connaître les raisons pour lesquelles la banque les a mis dehors, parfois après de nombreuses années de relation et sans que les contours de celle-ci aient apparemment changé. Les banques sont malheureusement fort réticentes à fournir ces explications que le consommateur est pourtant légitimement en droit d'attendre. En l'espèce, il serait toutefois injuste de stigmatiser l'attitude des banques, celles-ci étant soumises, par ailleurs, à des obligations strictes qui leur interdisent, dans nombre de cas, de communiquer ces raisons a à leurs clients ou à Ombudsfin.

Enfin, nous devons regretter le retard conséquent mis par le gouvernement à rendre effective la nouvelle loi sur le service bancaire de base aux entreprises, loi dans le cadre de laquelle notre service s'est vu octroyer un rôle important. En l'absence de cadre normatif complet, nous n'avons pu aider, comme nous l'aurions voulu, les entreprises qui se sont adressées à nous pour obtenir ce service bancaire de base, indispensable pour leur permettre de fonctionner correctement.

Je formule évidemment le vœu qu'en 2022, certains des problèmes susmentionnés connaissent des évolutions positives et donnent, par conséquent, lieu à un nombre moins élevé de plaintes.

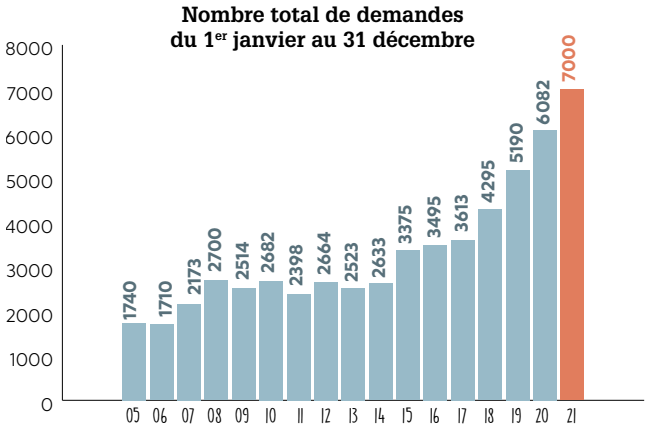
Jean Cattaruzza
Ombudsman

1. OMBUDSFIN EN CHIFFRES

1.1. Forte augmentation du nombre de demandes introduites

Le nombre total de demandes introduites par les consommateurs et les entreprises en 2021 s'élève à 7.000. Cela représente une augmentation de 918 dossiers (15,09%) par rapport à 2020.

Le tableau ci-dessous montre une augmentation soutenue au cours des sept dernières années, avec une accélération de cette tendance les trois dernières années.



Ces chiffres comprennent toutes les nouvelles demandes d'informations et les plaintes écrites qui ont été soumises à Ombudsfin en 2021.

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 7.000 nouvelles demandes introduites par les consommateurs et les entreprises, 6.859 concernaient une plainte et 141 étaient des demandes d'information.

1.2.2. Plaintes recevables

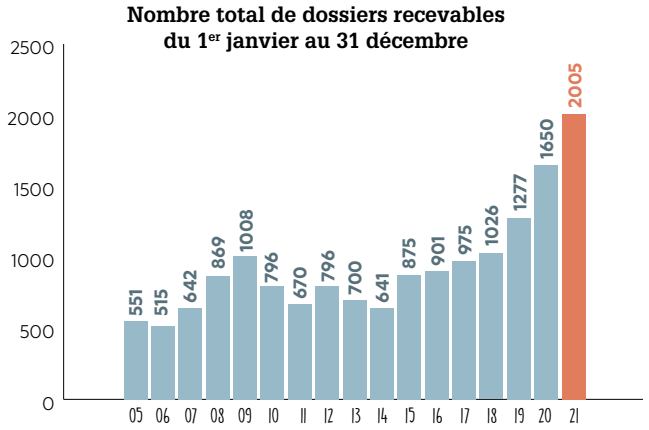
Les plaintes recevables sont celles pour lesquelles Ombudsfin est l'entité qualifiée compétente et qui remplissent toutes les conditions de recevabilité[1].

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.).

Parmi les 6.859 plaintes introduites en 2021, 1.882 (soit 27,4%) ont été déclarées recevables.

Par ailleurs, 2 plaintes déposées en 2018, 1 plainte déposée en 2019 et 120 déposées en 2020 ont également été déclarées recevables en 2021.

Au total, ce sont donc 2.005 plaintes qui ont été déclarées recevables en 2021, ce qui représente une augmentation de 21,5% (soit 355 plaintes) par rapport aux 1.650 plaintes recevables de 2020.



1.2.3. Plaintes non recevables

Parmi les 6.859 plaintes reçues en 2021, 4.968 (soit 72,4%) ne répondaient pas aux critères de recevabilité[2]. 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.

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

[2] *9 dossiers étaient encore en cours d'analyse de recevabilité au 31.12.2021.*

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

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 2021, est de 48 jours calendrier. En 2020, le délai moyen de traitement était de 43 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 2021, 199 dossiers ont été prolongés. Les parties ont été prévenues en temps utile de cette prolongation.

1.4. Interruption de la procédure de médiation

2 dossiers recevables ont été interrompus pendant la procédure de médiation à la demande du plaignant. Dans un dossier, la raison en était l'ouverture d'une procédure judiciaire. Dans l'autre dossier, une solution a été trouvée entre les parties.

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 2021, avec mention des chiffres et pourcentages respectifs.

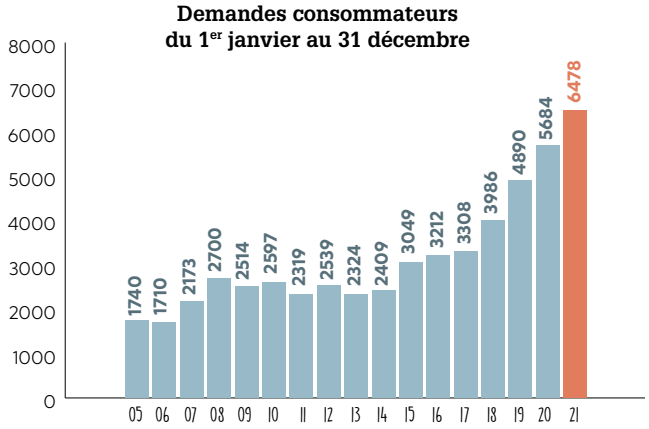
Banque	1766	88,08%
Société de crédit	101	5,04%
Etablissement de paiement	82	4,09%
Etablissement de monnaie électronique	42	2,09%
Courtier de crédit	3	0,15%
Prêteur social	2	0,10%
Asset Manager	1	0,05%
Société de bourse	0	0,00%
Société de leasing	5	0,25%
Bureau de recouvrement	0	0,00%
Bureau de change	0	0,00%
Intermédiaire en services bancaires et d'investissements	1	0,05%
Compagnie d'assurances	1	0,05%
Non-membre Febelfin	1	0,05%
Agent délégué	0	0,00%
TOTAL	**2005**	**100,00%**

2. DEMANDES INTRODUITES PAR LES CONSOMMATEURS

2.1. Forte augmentation du nombre de demandes

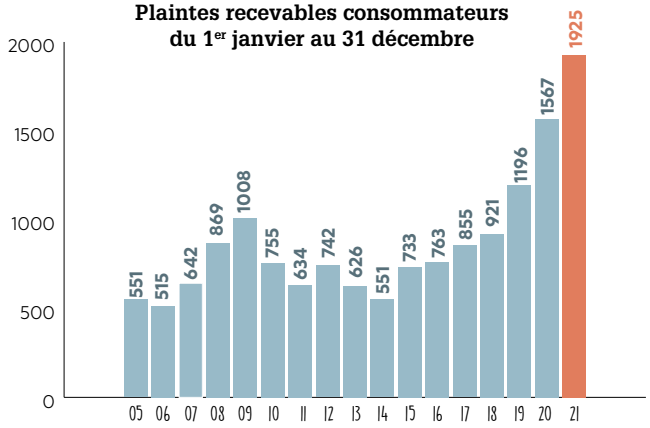
En 2021, Ombudsfin a reçu 6.478 demandes de consommateurs contre 5.684 en 2020, ce qui représente une augmentation de 794 dossiers (14%) par rapport à 2020.

6.377 demandes concernaient une plainte et 101 avaient trait à des demandes d'information.



2.2. Forte augmentation du nombre de plaintes recevables

En 2021, Ombudsfin a enregistré 1.925 demandes de consommateurs comme étant recevables (contre 1.567 en 2020), ce qui représente une augmentation de 358 dossiers (22,9%) par rapport à 2020.

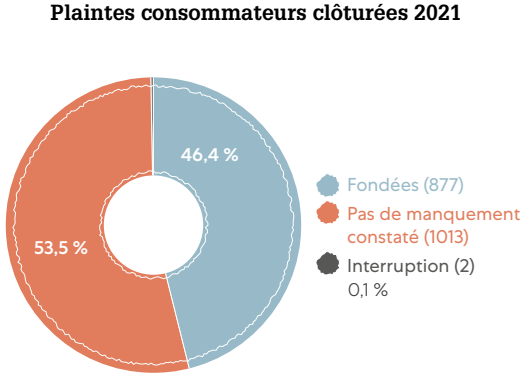


2.3. Résultats des plaintes recevables de consommateurs clôturées en 2021

Ces résultats concernent toutes les plaintes des consommateurs réglées en 2021. Certaines plaintes introduites avant 2021 auprès d'Ombudsfin sont donc aussi incorporées dans ces résultats.

1.892 dossiers ont été clôturés. Dans 46.4% des cas (soit 877 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 53,5% des cas (soit 1.013 dossiers), Ombudsfin n'a, en revanche, pas relevé de manquement 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[3].



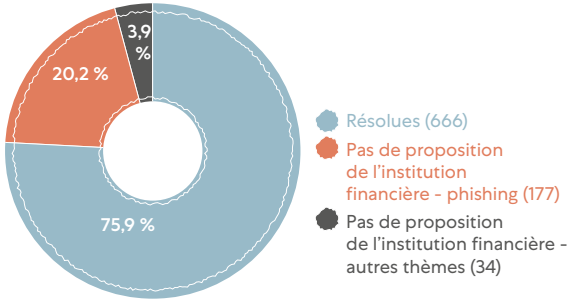
Des 877 plaintes considérées comme fondées par Ombudsfin, 75,9% (666 plaintes) ont été résolues. Ombudsfin regrette ce résultat insuffisant, qui est largement dû aux dossiers de fraude en ligne. Des 211 dossiers sans proposition de l'institution financière, 177 dossiers concernaient des cas de phishing. Donc 83,9% des dossiers non résolus sont liés aux dossiers phishing.

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 détectable ou non de la fraude est souvent perçu différemment par la banque et par Ombudsfin. Il en est de même en ce qui concerne la preuve de la négligence grave dans le chef du consommateur.

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 »).

[3] *Dans 2 dossiers, la procédure de médiation a été interrompue par le consommateur.*

Plaintes fondées consommateurs 2021



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 2021, 48 recommandations individuelles ont été formulées. Les institutions financières ont donné une suite favorable à 30 recommandations (62,5%). 10 recommandations (soit 20,8%) n'ont pas été suivies. Enfin, 8 recommandations (soit 16,7%) faisaient encore l'objet d'une enquête plus approfondie de la part de l'institution financière au moment de la rédaction du présent rapport.

[4] *Composition du collège, voir 14.2*

[5] *L'institution financière concernée est: Beobank.*

2.5. Collège des experts[4]

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

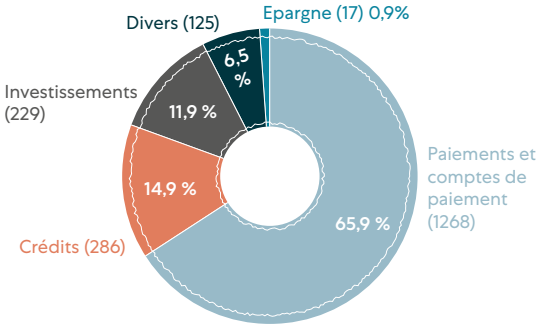
En 2021, 7 dossiers ont été soumis au Collège : 3 dossiers en matière de crédits hypothécaires, 2 dossiers en matière de paiements et comptes de paiements, 1 dossier en matière de crédits à la consommation et 1 dossier en investissements. 3 des 7 dossiers (43%) soumis au Collège ont été considérés fondés.

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.[5]

2.6. Thèmes des plaintes recevables des consommateurs

Les thèmes des plaintes recevables des consommateurs en 2021 étaient les suivants (évolution en nombre et en pourcentage depuis 2019):

Le principal thème de 2021 est, comme en 2020, de loin 'Paiements et comptes de paiement' avec 1268 dossiers. Ce thème, en augmentation constante ces dernières années, représente donc désormais près de deux tiers (65,9%) des plaintes recevables. Il englobe notamment les cas de fraudes et de rupture des relations, deux problématiques que nous développerons ci-dessous.



THEMES	2021	2020	2019	2021	2020	2019
	Nombre			%		
Paiements et comptes de paiement	1268	896	647	65,87	57,18	54,10
Crédits, dont	286	342	289	14,86	21,83	24,16
Crédits à la consommation	133	142	159	6,91	9,06	13,29
Crédits hypothécaires	153	200	130	7,95	12,76	10,87
Investissements	229	199	151	11,90	12,70	12,63
Autres	125	101	93	6,49	6,45	7,78
Epargne	17	29	16	0,88	1,85	1,34
TOTAL	**1925**	**1567**	**1196**	**100%**	**100%**	**100%**

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
Comptes à vue (généralités)	328
Découverts sur compte (non-autorisé)	11
Cartes	90
Guichets automatiques (Self)	28
Transactions guichet	15
Virements papier	2
Opérations à distance (PC, mobiles)	693
Domiciliations et ordres permanents	7
Paiements internationaux	66
Opération de change	3
Mobilité bancaire	6
Chèques	4
Service bancaire de base	15
Total	**1268**

Les dossiers concernant les opérations de paiement frauduleuses en ligne (phishing) se trouvent dans la rubrique 'opérations à distance (PC, mobiles)'. En 2021, 658 dossiers concernaient cette problématique.

Dans la rubrique 'Comptes à vue (généralités)' (189 dossiers), le blocage des comptes et la fin de la relation clientèle sont les thèmes les plus importants.

Dans la rubrique 'Cartes', on retrouve les dossiers relatifs aux transactions contestées concernant des cartes volées ou perdues (transactions physiques). En 2021, il s'agissait de 44 dossiers.

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 », Titre 3, 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 2021, Ombudsfin a reçu 15 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 2021:

Statistiques Service bancaire de base (SBB)	2021
Nombre de banques ayant enregistré une demande de SBB	11
Nombre de comptes SBB ouverts	12.771
Nombre total de comptes SBB existants	31.967
Nombre de refus d'ouverture d'un compte SBB	17
Nombre de comptes SBB résiliés (*)	3.893

** Ceci inclut les comptes SBB qui sont transformés en compte à vue régulier*

En 2021, 11 banques ont enregistré des demandes de services bancaires de base, soit 2 de plus qu'en 2020.

Le nombre de services bancaires de base ouverts en 2021 a augmenté de 35,3% pour atteindre 12.771. En 2020, il y a eu 9.442 ouvertures.

En 2021, 17 demandes d'ouverture de services bancaires de base ont été refusées en raison d'antécédents négatifs auprès de la banque (94,1%) et du fait que le demandeur était déjà titulaire d'un compte à vue (5,9%).

La principale raison d'une fermeture est la demande du titulaire (98,84%), suivi par:

- Compte courant dans une autre institution (0,79%)
- Autres produits non compatibles avec le service bancaire de base (0,17%)
- Antécédents négatifs à la banque (0,17%)
- Dépôts d'épargne et crédits à la consommation dont le montant cumulé est supérieur à 6.000 euros (0,03%)

2.7.2. Crédits

2.7.2.1. Crédits Hypothécaires

Crédits hypothécaires	Nombre de plaintes
Publicité	0
Formation du contrat	50
Exécution du contrat	79
Crédit pont	5
Mandat hypothécaire	3
Sûretés	2
Désolidarisation	12
Conditions générales (autres)	2
Total	**153**

Sous la rubrique 'Formation du contrat', les plaintes concernaient principalement la procédure d'octroi de crédit (21 plaintes) et la conclusion et contenu du contrat (13 plaintes).

Dans la rubrique 'Exécution du contrat', les plaintes concernaient principalement des difficultés de remboursement (20 plaintes) et le décompte (14 plaintes).

2.7.2.2. Crédits à la consommation

Crédits à la consommation	Nombre de plaintes
Publicité	0
Formation du contrat	28
Exécution du contrat	102
Conditions générales (autres)	3
Total	**133**

Sous la rubrique « Formation du contrat », les plaintes concernaient principalement le refus d'un crédit (12 plaintes) et la conclusion et contenu du contrat (9 plaintes).

Dans la rubrique « Exécution du contrat », les plaintes concernaient principalement le fichage négatif à la Banque nationale de Belgique (36 plaintes) et les difficultés de remboursement (17 plaintes).

2.7.3. Investissements

Investissements	Nombre de plaintes
Publicité et information à la souscription	3
Conseil et placement	10
Gestion de fortune	3
Achat et vente de titres (execution only)	98
Corporate action	15
Aspects fiscaux	20
Comptes titres	56
Fonds de pension/épargne-pension	14
Financial planning	0
Divers	9
Information sur tarif/coûts	1
Total	**229**

Sous la rubrique 'achat et vente de titres (execution only)', la plupart des plaintes concernaient l'achat en ligne d'actions (12 dossiers) et d'investissements alternatifs (72 dossiers). 65 de ces 72 dossiers concernaient des fraudes '*boiler room*' (voir point 6.6. ci-dessous).

2.7.4. Divers

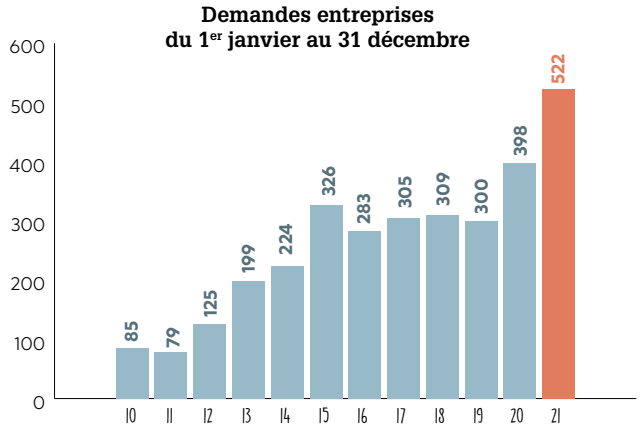
Divers	Nombre de plaintes
Coffres	6
Successions	54
Incapacité	15
Fraude employé	0
Garantie locative (aussi compte d'épargne)	19
Privacy	8
Discrimination	6
Divers	7
Know Your Customer	10
Produits d'épargne	17
Total	**142**

3. DEMANDES INTRODUITES PAR LES ENTREPRISES

3.1. Augmentation importante du nombre de demandes

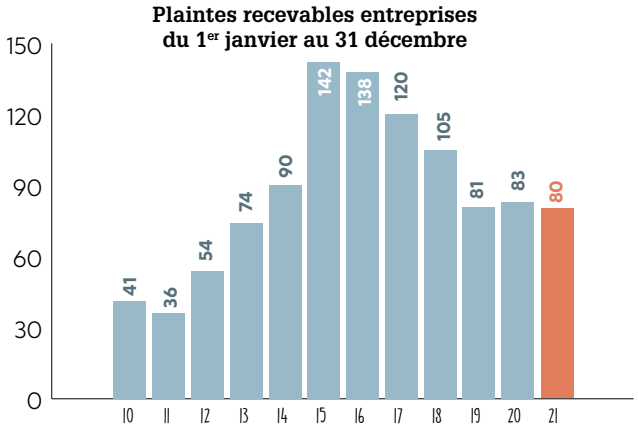
En 2021, Ombudsfin a reçu un total de 522 demandes écrites d'entreprises, contre 398 demandes en 2020. Cela représente une augmentation de 124 dossiers (31,9%). Cette évolution est notamment le résultat des nombreuses questions d'information qui ont été posées concernant le service bancaire de base pour les entreprises (voir ci-dessous).

482 demandes concernaient une plainte, tandis que 40 demandes concernaient une demande d'information.



3.2. Stagnation des plaintes recevables

En 2021, Ombudsfin a enregistré 80 demandes d'entreprises comme plaintes recevables, contre 83 demandes en 2020, soit une légère diminution de 3 dossiers (2,7%).



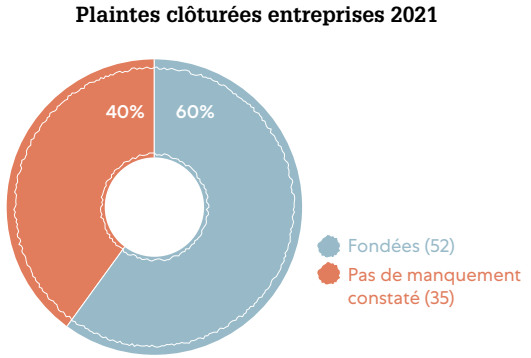
3.3. Résultats des plaintes des entreprises clôturées en 2021

Les résultats dont question ci-dessous concernent toutes les plaintes des entreprises qui ont été traitées et clôturées en 2021. Ces résultats comprennent également certaines plaintes qui avaient déjà été soumises à Ombudsfin en 2020, mais qui n'ont été traitées et clôturées qu'en 2021.

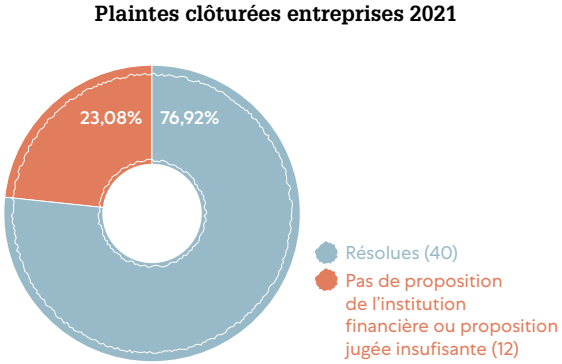
Au total, il s'agit de 87 dossiers.

Dans 52 dossiers (soit 60%), 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.

Dans 35 dossiers (soit 40%), 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.



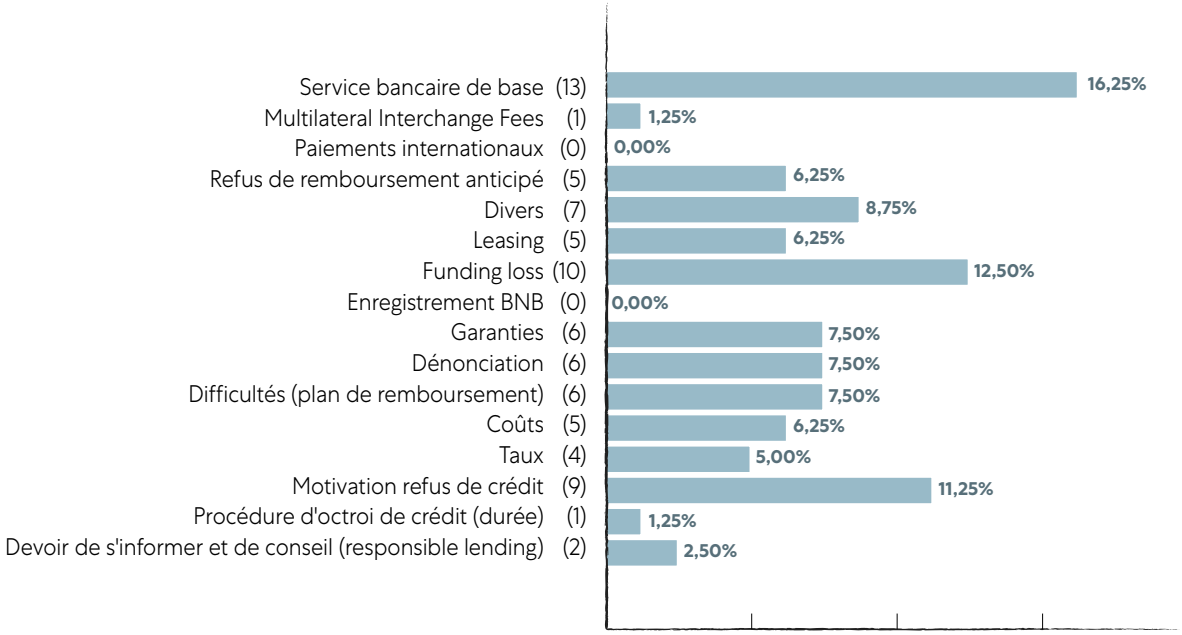
Dans les 52 dossiers qui ont été considérés comme fondés, Ombudsfin a poursuivi les négociations. Dans 40 dossiers (76,92% des plaintes fondées), cela a conduit à un règlement à l'amiable. En revanche, aucune solution n'a été trouvée dans 12 dossiers (23,08%).



Par rapport à 2020, il y a une augmentation de près de 15% des dossiers résolus. Il s'agit évidemment d'une évolution très positive.

3.4. Thèmes des plaintes recevables des entreprises

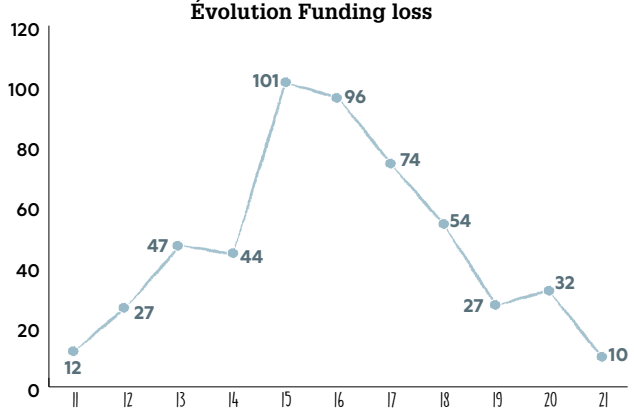
En 2021, les plaintes concernaient les thèmes suivants:



Pour la première fois, il y a une forte diminution du nombre de plaintes relatives au '*funding loss*'. Seuls 10 dossiers sur les 80 recevables avaient trait à cette problématique alors qu'en 2020, il s'agissait encore de 32 dossiers sur un total de 83.

Le graphique ci-contre montre l'évolution du nombre de plaintes concernant le '*funding loss*' qui ont été soumises à Ombudsfin ces 10 dernières années.

Évolution Funding loss



Jusqu'en 2020, le '*funding loss*[6] était le principal sujet de plaintes des entreprises.

En 2021, le nombre de plaintes à ce sujet a baissé de manière significative. Toutefois, cette tendance, déjà visible en 2019 et (dans une moindre mesure) en 2020, était à prévoir. En effet, de moins en moins de crédits octroyés avant l'entrée en vigueur de la loi du 21 décembre 2013, qui a réduit à 6 mois l'indemnité due en cas de remboursement anticipé, sont toujours en cours. Par ailleurs, le montant du 'funding loss' pour les crédits approchant de l'échéance finale diminue.

En 2021, le 'service bancaire de base pour les entreprises' est le nouveau thème principal.

Le présent rapport annuel consacre un chapitre distinct à ce thème (voir ci-dessous 10).

Il convient toutefois de noter que le nombre de plaintes consacrées à cette problématique (13 dossiers) reste assez limité par rapport au nombre de dossiers d'information qui ont été ouverts, à savoir 40 dossiers. Ombudsfin a également été contacté régulièrement par téléphone par des entrepreneurs qui ne pouvaient pas obtenir de compte bancaire. Cela montre clairement que le besoin d'un service bancaire de base pour les entreprises est réel dans certains secteurs.

[6] *Le 'Funding loss' est l'indemnité demandée par les banques en cas de remboursement anticipé d'une ouverture de crédit.*

4. CONSIDERATIONS GENERALES

Dans le contexte actuel de crise sanitaire et d'émergence de nouveaux modèles économiques bancaires suite au développement de la digitilisation, Ombudsfin relève que certaines problématiques sont récurrentes, quelle que soit la matière concernée par la plainte (crédit, comptes, ...).

En effet, plusieurs consommateurs ont rencontré en 2021 des difficultés avec leur banque par suite du manque de réactivité de cette dernière pour traiter leurs problèmes ou de l'absence de contact personnel, suite à la suppression des rendez-vous en agence liée à la crise sanitaire ou de la réduction structurelle du nombre d'agences. La nécessité de contacter, souvent plusieurs fois, un call center pour régler nombre de problèmes de base (transmission de documents, explication sur les frais imputés ...) engendre *des difficultés* de communication et *des retards* qui sont difficilement acceptables. Par exemple, lors de la demande d'un refinancement de crédit, il nous est arrivé d'observer, à plusieurs reprises, un délai de 8 mois pour obtenir une offre de refinancement alors qu'un délai de 4 mois nous semble devoir constituer, sauf circonstances exceptionnelles, un délai maximal. De même, pour l'ouverture de comptes bancaires qui nécessitent certaines formalités plus compliquées que la simple identification du client (par exemple pour les demandeurs d'asile, les administrateurs provisoires, ...), il est fréquent, malgré l'urgence, que les consommateurs doivent attendre plusieurs semaines, voire plusieurs mois, avant d'obtenir un rendez-vous pour procéder à l'ouverture desdits comptes.

L'évolution économique bancaire vers le numérique tend à l'exclusion des consommateurs en situation de rupture numérique. Cette exclusion a été accentuée par la crise sanitaire actuelle puisque les consommateurs ont un accès très limité dans le temps (horaire partiel des agences) et parfois géographiquement (suppression de nombreuses agences) aux services non numériques. De plus, il est manifeste que les banques *réduisent ou suppriment certains services traditionnels en faveur d'une solution numérique*. Par exemple, l'impression d'extraits de compte à un automate, possibilité utilisée par les personnes qui n'ont pas d'accès digital à leurs relevés, est de plus en plus limitée, payante ou carrément supprimée dans les packages offerts par les banques.

A cet égard, on doit donc se réjouir de la signature, par le gouvernement et le secteur bancaire, d'une Charte prévoyant l'obligation pour les banques de détail d'offrir à leurs clients, à partir du 1er janvier 2022, un service bancaire universel leur permettant (i) d'effectuer au minimum 60 opérations manuelles par an (par exemple: virements papier à remettre à l'agence et, si l'infrastructure de l'agence le permet, retraits d'espèces au guichet, etc.) et au moins 24 retraits d'espèces au guichet automatique de la banque propre et (ii) d'imprimer des extraits de compte aux guichets automatiques de la banque propre dans l'agence ou d'obtenir des retraits mensuels d'extraits au guichet (si le service est proposé par la banque) ou leur envoi mensuel à leur domicile à la demande du client. Ce package, qui comprend aussi l'octroi d'une carte de débit, doit être offert à un tarif compétitif (max. 60 €/an, hors frais « raisonnables »)[7].

En ce qui concerne le nombre de plaintes, Ombudsfin constate que la grande majorité des dossiers recevables en 2021 relève toujours (et même plus que jamais) du thème 'paiements et comptes de paiement'. Parmi les 2005 dossiers recevables, 702 plaintes[8] concernaient des contestations de transactions frauduleuses. Les dossiers de fraude (avec utilisation physique de la carte, mais surtout la fraude sur Internet) continuent donc d'être le thème le plus important. Un deuxième problème important sous la rubrique 'paiements et comptes de paiement' concernait la résiliation unilatérale de la relation clientèle (et le blocage du compte) par l'institution financière. En 2021, Ombudsfin a traité 189 plaintes à ce sujet.

Nous consacrerons évidemment une grande partie de ce rapport annuel à ces deux problématiques.

[7] *Pour plus de détails, voir https://www.febelfin.be/fr/article/un-service-bancaire-universel*

[8] *Dossiers sur les transactions frauduleuses tant avec des cartes physiques (44 dossiers) qu'en ligne (658 dossiers). Les dossiers relatifs à la fraude à l'investissement en ligne, 'boiler room', ne sont pas inclus dans ce nombre.*

5. Clôture de la relation clientèle

5.1. Généralités

Ombudsfin a eu à connaître, en 2021, de nombreux dossiers relatifs au blocage de comptes (5.2.) ou/et à la rupture unilatérale de la relation avec le client par l'institution financière (5.3.). Ombudsfin observe que ces deux mesures, de plus en plus utilisées par les banques et les institutions de paiement, constituent le plus 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 mais ce sont également des mesures que certaines banques implémentent dans d'autres circonstances, et notamment dans le cadre d'une politique de « derisking/ debanking » qui va plus loin que ce qu'exige la réglementation en vigueur (5.4.).

5.2. La mesure de blocage - article VII.37 §2 du Code de droit économique et conditions générales de la banque

Certaines plaintes portent sur le blocage pur et simple des comptes bancaires. Il s'agit d'une mesure de suspension de la relation, qui empêche le client d'utiliser son compte parfois pendant quelques mois.

L'article VII.37, §2 du Code de droit économique (ci-après « CDE ») prévoit cette faculté de blocage dans les termes et conditions suivants : « *Si le contrat-cadre le prévoit, le prestataire de services de paiement peut se réserver le droit de bloquer l'instrument de paiement et ce pour des raisons objectivement motivées ayant trait à la sécurité de l'instrument de paiement, à la présomption d'une utilisation non autorisée ou frauduleuse de l'instrument de paiement ou, s'il s'agit d'un instrument de paiement doté d'un contrat de crédit, au risque sensiblement accru que le payeur soit dans l'incapacité de s'acquitter de son obligation de paiement.*

Dans ces cas, le prestataire de services de paiement informe le payeur, de la manière convenue et sans préjudice de l'application de l'article VII.98, § 2, du blocage de l'instrument de paiement et des raisons de ce blocage et ce, si possible avant que l'instrument de paiement ne soit bloqué et au plus tard immédiatement après.

La fourniture des informations visées à l'alinéa précédent n'est pas requise si elle n'est pas acceptable pour des raisons de sécurité objectivement motivées ou interdite en vertu d'une autre législation. ».

Ombudsfin constate cependant que, dans de nombreux cas, le blocage du compte intervient souvent avant que le consommateur n'en ait été avisé de la manière convenue entre parties, ce qui le surprend et est très désagréable, d'autant que cette mesure se prolonge parfois pendant quelques mois.

Cette obligation d'information dans le chef des banques n'est toutefois pas sanctionnée par le Code de droit économique. Sur ce point, Ombudsfin ne peut donc pas se fonder sur cette absence d'information pour contraindre au déblocage ou pour obtenir une quelconque indemnisation.

Ombudsfin tente en revanche de vérifier si ces blocages sont objectivement motivés afin, soit d'obtenir la suppression de cette mesure s'il devait s'avérer qu'elle n'est pas justifiée (dans son principe ou sa durée[9]), soit d'obtenir les motifs de cette suspension (sécurité des cartes, débit non autorisé, ...) pour donner une explication compréhensible et satisfaisante au consommateur. Mais, comme le précise l'article VII.37 §2, alinéa 3 précité, les banques ne sont pas toujours tenues de fournir les informations demandées. Ombudsfin relève que ce refus de fournir les raisons d'un blocage par les banques est généralement fondé sur 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 (c'est généralement le cas en présence de money mule – voir infra - ou d'opérations suspectes).

5.3. La rupture de relation - conditions générales de la banque

En ce qui concerne les plaintes relatives à la résiliation de la relation avec le client, Ombudsfin observe que cette rupture de relation s'effectue parfois en deux étapes : dans un premier temps, la banque procède au blocage des comptes, comme expliqué ci-dessus et, dans un second temps, le client reçoit une « lettre de rupture de relation ». Dans d'autres cas, la rupture de relation est immédiate. Quel que soit le scénario utilisé, la rupture est le plus souvent liée à la prévention des opérations de blanchiment de capitaux et du financement du terrorisme même si, comme on le verra ci-dessous, d'autres considérations peuvent amener les banques à prendre une telle décision.

Dans les deux hypothèses, la lettre de rupture est adressée en application des conditions générales, par lesquelles les banques se réservent la possibilité de mettre fin à la relation avec le client, de manière unilatérale et sans motivation, moyennant le respect d'un délai de préavis (généralement deux mois) ou immédiatement (dans des cas extrêmement graves), avec motivation. Ce type de clause n'est valable que si le consommateur dispose également de cette faculté de mettre fin à ladite relation. Ombudsfin constate que les conditions générales bancaires prévoient généralement cette réciprocité.

[9] *Dans certains dossiers, nous avons dû constater que la mesure de blocage (par principe temporaire) était effective depuis plus de 3 mois lors de l'introduction de la plainte.*

La rupture d'une relation bancaire entraine évidemment de nombreux désagréments (transfert des avoirs; transfert des domiciliations; sort des produits « maison », par hypothèse difficilement transférables, et des crédits en cours, qui ne peuvent être dénoncés que dans les cas prévus par le contrat; notifications de changement de compte à l'employeur et aux fournisseurs divers...) et de l'incompréhension lorsqu'elle n'est pas motivée. Beaucoup de consommateurs s'interrogent dès lors sur la légalité de la rupture et souhaitent à tout le moins en connaître les motifs. Les consommateurs espèrent qu'Ombudsfin puisse rétablir cette relation ou, à tout le moins, connaître les motifs de la rupture.

Ombudsfin ne peut toutefois jamais forcer une institution financière à maintenir une relation avec un client existant[10]. Ceci a encore été rappelé récemment par le tribunal de Première Instance de Bruxelles, 3ème chambre, statuant en référé, dans un jugement du 6 décembre 2021 (NR 19/3281/A, p.11). L'intervention d'Ombudsfin se limite donc à vérifier si les formalités de résiliation (délai de préavis, mode de résiliation, etc.) stipulées dans les conditions générales de la banque ont bien été respectées. Dans certains cas spécifiques, Ombudsfin tente de faire valoir des circonstances spécifiques pour obtenir de la banque une révision de sa position. Si, dans certains cas, les banques acceptent de prolonger le délai de préavis pour donner au client la possibilité d'ouvrir un nouveau compte auprès d'une autre banque, elles ne sont en revanche guère enclines à revenir sur leur décision de mettre fin à la relation.

Par ailleurs, Ombudsfin veille au remboursement « pro rata temporis » des frais de compte déjà exposés et à ce que cette rupture de relation n'entraine pas de frais dans le chef du consommateur, par exemple en cas de transfert 'contraint' des avoirs à l'étranger, sans possibilité d'effectuer des virements SEPA (sans frais). En ce cas, Ombudsfin recommande aux institutions de prendre en charge les frais de virements « non SEPA ».

Enfin, Ombudsfin invite régulièrement les banques à lui transmettre les motifs de la rupture, qui peuvent être divers (perte de confiance, comportements inadéquats ou injurieux, agressivité à l'égard des employés, ...), mais les banques, si elles ont opté pour une rupture de relation sans motifs mais moyennant le respect d'un délai de préavis, refusent souvent de transmettre ces motifs ou se retranchent derrière 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 (money mule, opérations suspectes, ...). Ces dispositions imposent, en effet, aux banques, en cas de soupçons ou de motifs raisonnables de soupçons d'actes de blanchiment de capitaux/ financement du terrorisme, de suspendre ou rompre la relation et les banques doivent également immédiatement en référer à la Cellule de Traitement des Informations Financières (CTIF) mais sont tenues au secret et ne peuvent divulguer aux clients visés ou à des tiers les informations/ renseignements qui ont été ou seront transmises à la CTIF. Ombudsfin étant tiers, ces informations ne peuvent donc lui être communiquées, sous peine de sanction pour les banques.

Rappelons, pour clôturer ce chapitre, que les personnes qui, suite à la résiliation unilatérale de la relation bancaire, se retrouvent dépourvues de tout compte bancaire, peuvent demander de bénéficier d'un service bancaire de base (pour les conditions d'octroi : voir https://www.febelfin.be/fr/demander-le-service-bancaire-de-base).

[10] *Sous réserve des articles VII.56/1 à VII.59/3 du livre VII du CDE relatifs au service bancaire de base*

5.4. Non-SEPA, de-risking, limitation du cash

Le « de-risking » (l'atténuation des risques) peut être défini comme l'ensemble des actes et décisions prises par les institutions financières pour « gérer » leurs risques conformément à l'approche prônée par les institutions européennes et internationales, telle le GAFI (Groupe d'Action Financière), dans la lutte contre le blanchiment d'argent, le financement du terrorisme et la limitation des espèces[11]. La cessation des relations commerciales avec des clients ou catégories de clients est un des outils utilisés à cette fin. Ceci dit, les institutions financières ont également recours au « de-risking » pour d'autres raisons, par exemple un souci de rentabilité, le respect de leurs obligations prudentielles, la gestion du risque de réputation, des considérations éthiques. Ceci amène certaines institutions financières à exclure des clients, particuliers ou entreprises, non parce que ceux-ci présenteraient un risque intrinsèque, mais tout simplement parce qu'ils appartiennent à une catégorie professionnelle ou sociologique avec laquelle l'institution financière ne veut plus traiter. Le « de-risking » ou « de-banking » constitue donc une approche globale et non au cas par cas, ce qui est pourtant préconisé par les institutions européennes et internationales[12].

Si le refus d'entrée en relation, le blocage des comptes et la rupture de relation sans motifs constituent donc des mesures individuelles fréquentes du « de-risking », Ombudsfin constate également que d'autres décisions prises par les institutions bancaires à l'encontre des consommateurs participent à cette stratégie de « de-risking » (même si elles s'apparentent davantage à une stratégie d'évitement qu'à une stratégie de gestion du risque proprement dit).

Ainsi par exemple, Ombudsfin relève que certaines banques suppriment purement et simplement leur service de 'dépôt cash', refusent à certains clients la possibilité de retirer de l'argent en espèces aux guichets ou le droit d'acquitter certaines obligations contractuelles en espèces, même si cette faculté est pourtant contractuellement prévue (par exemple le paiement des mensualités en espèces dans le cadre du remboursement d'un crédit.)

Certaines banques ont également décidé de limiter les services internationaux, en mettant fin aux transactions SWIFT. D'autres banques rompent systématiquement les relations bancaires avec les personnes résidant dans certains pays hors Europe (par exemple : la Thaïlande). Du fait de cette résidence à l'étranger, ces clients n'ont pas la possibilité de transférer le solde de leurs avoirs par virement SEPA (ce qui génère des frais importants) et sont alors contraints de récupérer leurs avoirs par transfert d'argent en espèces, à ouvrir un compte dans une autre banque (ce qui n'est évidemment guère aisé en ces temps de pandémie) ou à passer par le compte d'une personne de confiance dans une autre banque.

Enfin, nous devons noter les agissements peu corrects de certaines institutions de transfert d'argent qui bloquent les fonds reçus sur un compte général ou refusent de les remettre à leur bénéficiaire sans avertir le consommateur et sans analyse réelle des éléments du dossier, de manière apparemment purement potestative, en se fondant sur leurs conditions générales et le « de-risking », précité.

Ombudsfin remarque, dans le cadre de sa mission, à l'instar de nombreux observateurs, que si ce « de-risking » permet aux institutions financières de répondre à leur obligation de gestion des risques liée à la lutte contre le blanchiment d'argent, le financement du terrorisme et la limitation des espèces, la manière dont il est pratiqué mène, dans certains cas, à certaines mesures excessives et à l'exclusion financière de certains consommateurs.

Ombudsfin n'hésite pas, en pareil cas, à mettre les banques face à leurs responsabilités et à négocier des solutions plus équilibrées, qui permettent aux deux parties de s'y retrouver.

---

[11] *Le droit de l'Union repose sur la Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiée par la Directive 2018/843, ainsi que sur les 40 recommandations édictées par le GAFI;*
En Belgique, la Loi « anti-blanchiment » du 18 septembre 2017 compose, dans une large mesure, le cadre juridique applicable. Le Règlement de la Banque nationale de Belgique (« BNB ») du 21 novembre 2017 relatif à la prévention du blanchiment de capitaux et du financement du terrorisme, applicable aux institutions financières belges qui relèvent de sa compétence de contrôle complète la Loi anti-blanchiment.

[12] https://www.nbb.be/fr/supervision-financiere/prevention-du-blanchiment-de-capitaux-et-du-financement-du-terrorisme-81. *Voir plus particulièrement la circulaire NBB_2022_03 du 1er février 2022 sur les attentes prudentielles par rapport au phénomène de « de-risking ».*

6. DOSSIERS DE FRAUDE

6.1. Introduction

Comme en 2019 et 2020, la majorité des plaintes traitées par Ombudsfin en 2021 concernaient la contestation de transactions frauduleuses. Nous renvoyons à nos rapports annuels de 2019 et 2020 qui, d'une part, exposent le raisonnement suivi par Ombudsfin dans ces dossiers, notamment en ce qui concerne la réglementation sur la répartition de la responsabilité en cas d'opérations de paiement non autorisées, telle que prévue par le livre VII du Code de droit économique, et, d'autre part, expliquent les types de fraude les plus courants).

Ombudsfin constate que, tout comme en 2020, les résultats de la médiation dans les dossiers de fraude sont en 2021 moins positifs (seuls 40% des dossiers fondés aboutissent à une médiation positive). Ceci est dû au fait que la question de savoir si les banques sont légalement tenues ou non d'intervenir dans les dommages résultant d'opérations de paiement non autorisées dépend de la question de savoir si la fraude aurait pu être détectée à l'avance par la victime et de l'appréciation de la négligence grave dans le chef de la victime. Pour les deux appréciations, l'ensemble des circonstances de faits doit être pris en compte. Or, nous constatons que les banques évaluent actuellement souvent les faits d'une manière différente de celle d'Ombudsfin. Les discussions dans ces dossiers portent principalement sur la question de savoir si le client a fait preuve d'une négligence grave ou non. Ombudsfin constate que les banques utilisent une définition très large de la négligence grave.

Par souci d'exhaustivité, il convient de noter que tous les dossiers de phishing ne sont pas considérés comme fondés. Dans certains cas, nous retenons également l'hypothèse d'une négligence grave, dans d'autres cas, nous ne pouvons pas donner de réponse concrète parce que nous ne connaissons pas suffisamment les circonstances réelles de la fraude. Pour l'année 2021, nous avons clôturé 355 dossiers (soit 55%) comme non fondés et 293 dossiers (soit 45%) comme fondés.

6.2. Typologie

Ombudsfin constate que les scénarios de fraude utilisés par le fraudeur sont généralement restés les mêmes. Pour des conseils et des avertissements sur les scénarios de fraude les plus courants, nous vous renvoyons à safeonweb.be. Pour être complets, signalons que Safeonweb a également introduit une application mobile en novembre 2021. Vous pouvez en savoir plus à ce sujet en cliquant sur le lien suivant : https://www.safeonweb.be/fr/blog/lapplication-safeonweb-pourquoi-en-avez-vous-besoin

- Les fraudeurs approchent toujours leurs victimes par le biais de mails ou de SMS de phishing, provenant soi-disant (i) de leur banque, demandant par exemple à la victime de demander un nouveau lecteur de carte, (ii) du SPF Finances, indiquant par exemple à la victime qu'elle a toujours une dette impayée, (iii) du gouvernement flamand, indiquant à la victime qu'elle a droit par exemple à une prime corona, (iv) du fournisseur de télécommunications de la victime, indiquant à la victime qu'elle a toujours un arriéré de paiement, etc.

- La fraude à l'achat et à la vente via le site web 2ememain.be et d'autres sites similaires (Facebook, Marketplace, Vinted, etc.), où le fraudeur se fait passer pour un acheteur ou un vendeur intéressé, est également encore très courante (voir développements dans le rapport annuel 2020, page 23).

- De plus, Ombudsfin constate que le nombre de cas de 'whaling' continue d'augmenter. Dans ce type de fraude, les fraudeurs envoient souvent un message à leur victime via WhatsApp, en se faisant passer pour la fille ou le fils de la victime. Ils disent que leur GSM est tombé en panne 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 son compte.

- Un nombre non négligeable de dossiers de fraude concerne la fraude aux comptes de dépôt/la sécurisation des avoirs par téléphone sur un compte à sécurité renforcée (voir développements dans le rapport annuel 2020, page 24 et suivantes).

- Enfin, nous constatons de plus en plus de cas de fraude à l'investissement/boiler room, où les fraudeurs proposent des investissements très intéressants à leurs victimes, qui effectuent ensuite plusieurs virements pour investir, mais ne récupèrent jamais leur argent.

Dans chaque scénario, le fraudeur a toujours le même objectif : obtenir ou intercepter des codes générés avec la carte bancaire de la victime et un lecteur de carte via un site web frauduleux, par téléphone ou par tout autre moyen. Avec ces codes, le fraudeur peut ensuite se connecter au *'homebanking'* de sa victime ou installer une application mobile, liée aux comptes de la victime, sur son propre appareil (l'appareil du fraudeur). Le fraudeur peut alors utiliser ces canaux pour effectuer des transactions. Il arrive également que les fraudeurs utilisent les codes interceptés/acquis pour effectuer des paiements directement sur le site web d'un commerçant. Dans certains cas de fraude, les victimes sont manipulées et trompées de telle sorte qu'elles effectuent elles-mêmes les transactions contestées sur les instructions du fraudeur.

6.3. Développements

Bien que les scénarios de fraudes soient restés les mêmes, Ombudsfin constate cependant certaines évolutions. Ombudsfin remarque, entre autres, que les fraudeurs sont devenus de plus en plus professionnels. Les e-mails et les SMS frauduleux ne contiennent pratiquement aucune faute de grammaire ou d'orthographe. Les adresses électroniques utilisées semblent de plus en plus authentiques (voir par exemple: https://myebox.be/fr/news/myebox-be-des-e-mails-de-phishing-en-circulation). Les URL et les liens utilisés par les fraudeurs sont de plus en plus crédibles. Les faux sites web sont si bien construits qu'il est difficile de les distinguer des sites officiels et authentiques. En résumé, tout devient de plus en plus crédible et du danger se cache derrière chaque coin de l'environnement digital. Afin de brouiller les pistes et de rendre l'identification de la fraude plus malaisée, on notera également que le recours à des mules devient de plus en plus fréquent (voir point 6.4. ci-dessous).

Ombudsfin constate également que les fraudeurs font de petits ajustements à leur modus operandi. Par exemple, Ombudsfin a traité un certain nombre de dossiers en 2021 dans lesquels le fraudeur n'a pas effectué les transactions contestées par le biais de l'application mobile de la banque elle-même, mais par le biais d'Apple Pay, une application du « portefeuille mobile (Mobile wallet) » par laquelle les paiements peuvent être effectués par le biais des appareils Apple. Étant donné que les discussions sur la répartition de la responsabilité pour les transactions contestées utilisant Apple Pay sont très spécifiques et qu'elles ont quelque peu évolué au cours de l'année 2021, nous en parlerons plus en détail dans le présent rapport annuel (voir point 6.5. ci-dessous).

Tout comme en 2020, Ombudsfin note qu'en 2021, les banques prennent également en compte les recommandations d'Ombudsfin et adaptent en conséquence leurs processus de paiement, la manière dont leurs applications mobiles respectives et leurs mécanismes de détection des fraudes sont installés, etc. Vous pouvez en savoir plus sur ces évolutions positives ci-dessous.

6.4. Le phénomène des Money mules

6.4.1. Le mécanisme

Profitant de la crédulité de certaines personnes à qui ils promettent de gagner rapidement de l'argent sans effort, certains criminels utilisent des mules financières à des fins de blanchiment d'argent. Les proies des criminels sont souvent jeunes.

La mule va, consciemment ou non, permettre l'utilisation de son compte bancaire ou de ses instruments de paiement par des fraudeurs ayant besoin d'un compte bancaire intermédiaire pour y verser des fonds obtenus illégalement. Cet argent est ensuite rapidement transféré vers un autre compte ou bien retiré immédiatement à l'aide de la carte de la mule. En agissant de la sorte, les fraudeurs parviennent à dissimuler l'origine illicite des fonds. En jouant le rôle de mule, le titulaire du compte aide à blanchir de l'argent, ce qui est évidemment répréhensible au regard de l'article 505 du code pénal.

Ombudsfin tient à signaler l'initiative prise par Febelfin afin de mettre en garde les jeunes et leur entourage face au phénomène des mules. Febelfin a en effet publié des outils de sensibilisation pour les jeunes et leur environnement afin de lutter contre les fraudes commises par des mules. Vous pouvez accéder directement aux différentes brochures en suivant les liens mentionnés ci-dessous :

https://www.febelfin.be/sites/default/files/2021-11/Brochure_geldezels_jongeren_FR.pdf

https://www.febelfin.be/sites/default/files/2021-11/Brochure_geldezels_begeleiders_FR.pdf

Nous réitérons, pour notre part, aux jeunes consommateurs nos conseils publiés dans notre rapport annuel 2019 (page 29), à savoir : si vous êtes approché via les réseaux sociaux, à la porte de l'école ou sur le lieu de votre hobby par une tierce personne qui vous promet de l'argent en échange de vos coordonnées bancaires et de votre carte de banque, arrêtez immédiatement la conversation et ne donnez en aucun cas suite à une telle demande. Si vous coopérez, vous pouvez vous rendre coupable d'infractions pénales. En outre, les parents d'enfants mineurs peuvent également être tenus pour responsables.

6.4.2. L'attitude des banques

Lorsque les banques détectent sur un compte des

mouvements pouvant laisser penser à des pratiques frauduleuses (ou qu'elles reçoivent des informations d'une institution financière tierce laissant supposer qu'un compte a été utilisé afin de transférer de l'argent détourné dans le cadre d'une fraude dont a été victime un de ses clients), elles bloquent souvent le compte de la mule financière. Si ce compte est suffisamment provisionné, il arrive également que les banques retournent les fonds litigieux à la victime de la fraude, et ce même si le montant d'origine frauduleuse a déjà été retiré ou reversé entretemps sur un autre compte. La mule se voit ainsi financièrement pénalisée pour son intervention dans le processus de blanchiment.

Se pose évidemment la question de savoir si les banques ont le pouvoir d'agir de la sorte. En fait, cela dépend essentiellement de la manière dont les conditions générales sont rédigées. Celles-ci précisent habituellement que la banque se réserve le droit de bloquer les comptes pour des raisons objectivement justifiées liées à la sécurité, à la suspicion d'une utilisation non autorisée ou frauduleuse ou pour se conformer à ses obligations légales.

Cette pratique est conforme à l'article VII.37, §2 du CDE qui stipule que, si le contrat-cadre le prévoit, le prestataire de services de paiement peut se réserver le droit de bloquer l'instrument de paiement et ce pour des raisons objectivement motivées ayant trait à la sécurité de l'instrument de paiement ou à la présomption d'une utilisation non autorisée ou frauduleuse de l'instrument de paiement.

D'autres conditions générales octroient également à la banque une certaine marge de manœuvre et une possibilité d'action afin de débiter le compte de la mule financière pour reverser ensuite la somme litigieuse sur le compte de la victime initiale de la fraude.

En effet, certaines banques prévoient que le titulaire du compte autorise explicitement la banque à débiter son compte des montants qui auraient été crédités sur son compte par erreur ou à la suite d'une opération irrégulière, fausse ou falsifiée. Comme nous l'avons déjà indiqué ci-dessus, le fait que le montant crédité ait entretemps déjà été retiré du compte de la mule est sans incidence.

6.5. Apple Pay

Dans un certain nombre de dossiers de fraude soumis à Ombudsfin, le fraudeur a utilisé l'application Apple Pay. Dans ces dossiers, le fraudeur a réussi à lier une carte de débit et/ou de crédit de sa victime sur son propre appareil (Apple) à son application Apple Pay, et a ensuite pu exécuter des paiements frauduleux via cette application.

Ombudsfin se réjouit que les discussions avec les institutions financières impliquées dans ces dossiers ont connu une certaine évolution positive. Ces discussions étaient très spécifiques et concernaient principalement la question de savoir si Apple Pay était installé ou non sur l'appareil du fraudeur avec une authentification forte du client.

6.5.1. En quoi consiste Apple Pay ?

Apple Pay est une application de portefeuille mobile ('Mobile Wallet'), proposée par Apple (et non par la banque elle-même), qui permet d'effectuer des paiements via les appareils Apple (iPhone, iPad, Apple Watch ou Mac) sans que le payeur ait à utiliser sa carte de paiement. Pour cela, le payeur doit d'abord lier la ou les cartes de paiement souhaitées au portefeuille digital, l'application Apple Pay, sur son appareil. Une fois que cela a été fait, les paiements peuvent être effectués via cette application. Les paiements via Apple Pay sont possibles à la fois en ligne après confirmation par Touch ID (l'empreinte digitale enregistrée sur l'appareil) ou Face ID (reconnaissance faciale), et sans contact dans «le magasin» en tenant l'appareil sur lequel l'application est installée à quelques centimètres du terminal de paiement.

Vous pouvez trouver plus d'informations au sujet d'Apple Pay sur le site web d'Apple https://www.apple.com/befr/apple-pay/. Toutes les banques belges n'offrent pas Apple Pay. Le lien suivant vous permet de savoir quelles banques belges proposent déjà cette application: https://support.apple.com/fr-fr/HT206637

Apple Pay se distingue clairement des applications mobiles classiques proposées par les banques. Avec ces dernières, il n'est en effet pas uniquement possible d'effectuer des paiements. Les applications de banque mobile permettent également aux utilisateurs d'accéder au relevé de leur compte et à d'autres produits bancaires et leur permet d'effectuer des virements. La connexion à ces applications ne sont possible qu'en utilisant le code choisi lors de l'installation de l'application, par reconnaissance faciale ou par l'empreinte digitale enregistrée (cela varie d'une banque à l'autre). De cette manière, le payeur peut également effectuer des virements et des paiements. Toutefois, si le payeur souhaite utiliser son application bancaire mobile pour effectuer un virement dont le montant dépasse certaines limites, il devra toujours signer la transaction à l'aide de sa carte bancaire et de son lecteur de cartes (avec certaines banques, cela est également possible via itsme).

6.5.2. Authentification forte du client

Nous renvoyons à la page 20 de notre rapport annuel 2019 (titre 2.8.3.3.1.) où plus d'explications ont été fournies sur les règles concernant l'authentification forte du client. L'article VII.44, § 2 du Code de droit économique prévoit que, lorsque le prestataire de services de paiement n'exige pas une authentification forte de la part du payeur, le payeur ne doit pas supporter de pertes financières résultant d'opérations de paiement non autorisées, à moins que le payeur n'ait lui-même agi frauduleusement. Par conséquent, lorsqu'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 sera pas responsable même s'il a manqué à certaines obligations par suite de négligence grave.

Ombudsfin constate que, depuis l'entrée en vigueur, le 14 septembre 2019, du règlement délégué de la Commission du 27 novembre 2017 relatif aux normes techniques de

réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication[13], presque toutes les transactions en ligne doivent être effectuées via une authentification forte du client. Ce règlement prévoit certes un certain nombre de dérogations à cette obligation[14]. Mais même si le prestataire de services de paiement est exempté de l'obligation d'authentification forte du client en vertu du règlement délégué sur l'authentification forte du client, la banque sera responsable des dommages résultant d'opérations de paiement non autorisées sans authentification forte du client, conformément à l'article VII.44, § 2 du Code de droit économique.

Le terme «authentification forte du client» est défini à l'article I.9, 33/16° du Code de droit économique comme suit :

"*authentification forte du client: 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)*[15] *et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification*."

Une fois que deux des facteurs susmentionnés sont combinés, on obtient une authentification forte du client. Dans un avis du 21 juin 2019, l'Autorité bancaire européenne (ABE) a apporté des précisions sur l'interprétation de ces notions[16].

6.5.3. Façons dont Apple Pay peut être installée: authentification forte du client ou non ?

Nous constatons qu'il existe différentes manières d'installer Apple Pay et d'y lier une carte de débit ou de crédit. Cette procédure d'installation peut également varier d'une banque à l'autre. Dans les dossiers soumis à Ombudsfin, le fraudeur a utilisé l'une des procédures d'installation décrites ci-dessous.

6.5.3.1. Installation d'Apple Pay à partir de l'application bancaire mobile

Dans certains dossiers, Ombudsfin constate que l'application Apple Pay avait été installée à partir d'une application bancaire mobile installée frauduleusement sur l'appareil du fraudeur. Dans ces dossiers, le fraudeur a d'abord réussi à installer sur son propre appareil une application mobile liée aux comptes de sa victime. À partir de l'application bancaire mobile, les cartes peuvent ensuite être facilement ajoutées à Apple Pay.

L'application de banque mobile, proposée par la banque, ne peut être installée que sur base de certaines données bancaires du client et de plusieurs codes générés par la carte bancaire du client, son code PIN et un lecteur de carte. Certaines banques envoient également un e-mail avec un lien d'activation ou un SMS avec un code d'activation sans lequel l'application ne peut être utilisée activement (voir plus loin)[17]. Ainsi, avant que le fraudeur puisse installer l'application bancaire mobile, il doit d'abord intercepter ces données et ces codes (par exemple, via le phishing) ou les obtenir (par exemple, via vishing). En utilisant cette application bancaire mobile, le fraudeur peut ensuite ajouter des cartes à Apple Pay.

Ombudsfin constate que, dans ces cas, l'installation de l'application bancaire mobile, et donc d'Apple Pay, a bien lieu par une authentification forte du client. Ici, deux des facteurs mentionnés à l'article I.9, 33/16° du Code de droit économique sont combinés, à savoir la possession de la carte bancaire, de la puce électronique et des données de la carte et la connaissance du code PIN. Il n'y a pas eu de discussion avec la banque à ce sujet.

6.5.3.2. Installation d'Apple Pay sur base des données de la carte et d'un code d'activation envoyé par SMS

Une deuxième procédure d'installation d'Apple Pay utilisée par les fraudeurs consiste à lier les cartes de débit et de crédit sur base des données de la carte et d'un code d'activation envoyé par SMS (généralement au numéro de GSM de la victime, mais dans certains cas au numéro de GSM du fraudeur après qu'il ait changé le numéro de sa victime via, par exemple, la banque en ligne). Dans ces cas, la liaison de la carte de paiement à Apple Pay ne se fait pas via une application bancaire mobile, mais directement via le 'Wallet' (Il s'agit d'une application qui est installée automatiquement sur certains appareils Apple. Dans cette application, il est possible de lier non seulement des cartes de paiement, mais aussi, par exemple, des cartes d'identité, des tickets de transport, des tickets pour des événements, etc.)

Il s'agit de la procédure d'installation la plus souvent utilisée par les fraudeurs dans les dossiers soumis à Ombudsfin. Les discussions avec les banques ont principalement porté sur cette procédure d'installation.

Dans ces cas, Ombudsfin estime qu'Apple Pay n'a pas été activé avec une authentification forte du client. En effet, sur

[13] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R0389&from=NL.

[14] *Article 10 et suivants du règlement délégué : authentification forte du client.*

[15] *Par exemple, une empreinte digitale ou un scan de l'iris.*

[16] *Voir* https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

[17] *Point 6.5.3.2.*

la base de l'avis précité du 21 juin 2019 de l'ABE, Ombudsfin considère que tant les coordonnées de la carte de la victime de la fraude que le code d'activation envoyé par SMS constituent des éléments de possession.

Certaines banques suivent l'avis d'Ombudsfin à ce sujet et ont donc proposé une intervention. Dans plusieurs dossiers, d'autres banques ont décidé, après la mediation, de proposer une intervention commerciale par compréhension pour les arguments d'Ombudsfin mais sans y consentir explicitement. Ces banques n'ont pas encore pris de position juridique définitive sur cette problématique.

6.6. Fraude à l'investissement ou fraude 'boiler room'

6.6.1. Mécanisme

Certaines personnes cherchent en ligne des investissements intéressants. Grâce à des publicités attrayantes, elles entrent parfois en contact avec des entreprises qui semblent très professionnelles et promettent de bons rendements.

D'autres lisent, par exemple sur Facebook, qu'un homme politique bien connu ou une personnalité médiatique a gagné beaucoup d'argent en investissant dans des bitcoins par l'intermédiaire d'une société déterminée. Les personnes intéressées peuvent alors indiquer leurs coordonnées et sont ensuite contactées par téléphone par des collaborateurs de l'entreprise.

Dans les deux cas, les intéressés transfèrent de l'argent sur des numéros de compte fournis par la société d'investissement ou le conseiller présumé. Ombudsfin constate que les fraudeurs demandent souvent de transférer de l'argent vers différents numéros de comptes ouverts à l'étranger au nom de personnes ou de sociétés inconnues. Ils tentent ainsi, souvent avec succès, de contourner les mesures de protection prévues par les banques. En effet, aucune alarme ne se déclenche pour les noms qui ne figurent pas sur la liste d'alerte établie par les banques (voir ci-dessous).

Ensuite, il s'est évidemment avéré impossible de récupérer les fonds. Les entreprises n'existaient pas et l'argent avait tout simplement disparu.

Ces dernières années, il y a eu de nombreuses victimes de ces fraudes à l'investissement ou '*investment scam*' ('*scam*' signifie arnaque en anglais). Dans de nombreux cas, les victimes ont perdu de très grosses sommes d'argent.

Cette fraude est aussi généralement appelée 'fraude boiler room', car les fraudeurs font souvent pression sur leurs victimes pour qu'elles transfèrent de plus en plus d'argent.

Ombudsfin traite des plaintes relatives à des fraudes en matière d'investissement depuis plusieurs années, mais en 2021, le nombre de plaintes a considérablement augmenté. En 2021, 65 dossiers concernaient ainsi ce type de problème.

Les victimes demandent à leur banque d'intervenir dans le dommage parce qu'elles estiment que la banque aurait pu ou dû reconnaître la fraude et n'aurait pas dû effectuer les transactions. Elles invoquent le devoir de diligence qui incombe aux banques.

6.6.2. Le rôle d'Ombudsfin

Lors du traitement d'une telle plainte, Ombudsfin vérifie d'abord si la victime a effectué elle-même les transactions. Dans la plupart des dossiers, cela est effectivement le cas. La victime voulait faire les investissements et recevoir un beau rendement. Elle savait donc quels montants seraient transférés et vers quels comptes l'argent serait transféré.

Il s'agit donc 'd'opérations autorisées' (voir définition à l'article VII 32 du Code de droit économique). Dans ce cas, la loi ne prévoit pas l'intervention de la banque.

Ombudsfin examinera ensuite si le devoir de diligence des banques a été respecté ou non.

Le point de départ est que les banques sont tenues d'exécuter correctement les ordres de paiement de leurs clients. En principe, il leur suffit de regarder le numéro de compte du bénéficiaire. C'est ce que prévoit la loi (voir l'article VII 13, 1°, b du Code de droit économique). Le numéro de compte est 'l'identifiant unique'.

En principe, les banques ne doivent pas enquêter sur le titulaire du compte bénéficiaire. Certainement pas lorsque le bénéficiaire est un client d'une autre banque, dans un pays étranger de surcroît, comme c'est souvent le cas dans les fraudes à l'investissement. La banque ne doit même pas vérifier si le numéro de compte indiqué est réellement au nom du bénéficiaire communiqué. Ceci n'est pas toujours bien compris par les clients qui se demandent à juste titre pourquoi il faut alors indiquer les deux informations (numéro de compte et nom).

Ceci étant dit, dans le cadre de leur devoir de diligence, les banques assurent la sécurité des opérations de paiement en tenant à jour des listes de numéros de compte et de noms de personnes ou de sociétés impliquées dans des fraudes. Elles assurent également un monitoring systématique des transactions et lancent une alerte lorsqu'une transaction est jugée anormale ou frauduleuse.

La FSMA[18] publie sur son site des listes d'alerte avec les noms des entreprises impliquées dans des fraudes ou faisant l'objet de plaintes pour fraude. Les banques en tiennent évidemment compte mais, comme indiqué plus haut, les fraudeurs demandent souvent de transférer de l'argent vers différents numéros de compte à l'étranger ouverts au nom de personnes ou de sociétés inconnues, qui ne figurent pas sur la liste établie par les banques. Ceci explique qu'aucun signal d'alarme ne se déclenche.

[18] *En Belgique, la FSMA est l'autorité de contrôle des entreprises d'investissement. Le nom complet de la FSMA est l'Autorité des services et marchés financiers.*

Ombudsfin conseille de vérifier si la société avec laquelle le client est en contact (souvent uniquement en ligne ou par téléphone) est fiable avant de transférer des fonds à des fins d'investissement. Il est alors conseillé de vérifier les listes de mises en garde de la FSMA sur son site web. Les différents types de fraude y sont expliqués plus en détail.

Cependant, il arrive que les fraudeurs se servent du nom d'une entreprise existante et correcte. Dans ce cas, il est conseillé de contacter la vraie société et de vérifier quel numéro de compte cette société utilise avant d'effectuer un transfert.

Ombudsfin a également constaté que dans de nombreux cas, pour déposer plainte, les victimes sont épaulées par

une organisation qui offre une assistance aux victimes de fraude à l'investissement.

Sur son site web, la FSMA met toutefois en garde contre des organisations malhonnêtes qui, sous couvert 'd'aide', ne cherchent qu'à escroquer les victimes pour leur extorquer davantage d'argent.

6.6.3. Attitude des banques

Sur la base de l'analyse mentionnée ci-dessus, les banques refusent logiquement d'intervenir dans les dommages subis.

Cependant, elles doivent faire tout leur possible pour récupérer les fonds détournés. Lorsque les banques sont informées par un client qu'il a été victime d'une fraude, elles lui demandent de déposer immédiatement une plainte auprès de la police. Elles contactent ensuite la banque du bénéficiaire pour récupérer les fonds si les transactions sont très récentes. En revanche, lorsque la fraude n'apparaît qu'après quelques mois, ce qui est souvent le cas, les tentatives de récupération n'ont que peu de sens car les fraudeurs transfèrent ou retirent rapidement l'argent.

6.7. Procédures judiciaires

6.7.1. Jugements en première instance en faveur de la victime de la fraude

Le 16 février 2021, KBC a été condamnée par le tribunal de première instance d'Anvers à intervenir dans les dommages de la victime d'un cas de fraude par le biais de 2ememain.be. Le 23 mars 2021, KBC a également été condamnée par le tribunal de commerce de Louvain à intervenir dans le dommage subi par une victime de smishing (SMS + phishing), qui avait réagi à un SMS frauduleux prétendument envoyé par les services fiscaux. Les jugements en question ont été relayés par les médias (voir, par exemple: https://www.guide-epargne.be/epargner/actualites-generales-payer/les-banques-doivent-rembourser-les-dommages-causes-par-le-phishing.html?referrer=https%3A%2F%2Fwww.google.com%2F;
https://www.rtbf.be/info/economie/detail_les-banques-doivent-rembourser-les-victimes-de-phishing?id=10782744

Entre-temps, KBC a fait appel dans les deux dossiers. Par conséquent, les deux décisions de première instance ne sont pas définitives. La réaction de KBC aux reportages des médias concernant ces deux décisions peut être consultée via le lien suivant: https://www.kbc.com/content/dam/kbccom/doc/newsroom/pressreleases/2021/20210614_duiding_phishing_FR(2).pdf

Ombudsfin constate que plusieurs plaignants se sont appuyés sur ces jugements pour conclure que les banques sont tenues de rembourser le dommage subi dans tous les cas de phishing. Ombudsfin souligne que ceci n'est pas correct. La législation relative à la répartition de la responsabilité en cas d'opérations de paiement non autorisées prévoit comme règle de base que les banques sont tenues de supporter le préjudice, après déduction d'une franchise de 50 euros, sauf si la banque peut apporter la preuve que le payeur n'aurait pas rempli certaines obligations à la suite d'une négligence grave. Le Code de droit économique prévoit également un certain nombre d'exceptions à cette règle de base, dont l'une est toujours pertinente dans les cas de phishing: si la victime n'a pas pu détecter la fraude à l'avance, la banque est obligée de supporter la totalité du préjudice (indépendamment du fait que la victime ait fait preuve d'une négligence grave). Le Code de droit économique ne prévoit donc pas de règle générale sur la base de laquelle les banques devraient intervenir dans tous les cas de phishing ou de smishing.

Tant l'évaluation de la détectabilité préalable de la fraude que celle d'une éventuelle négligence grave de la part de la victime doivent être effectuées sur la base de tous les faits. Ombudsfin remarque que pour cette raison, chaque dossier de fraude doit être examiné de manière individuelle. Bien que plusieurs cas de fraude soient souvent similaires, Ombudsfin constate que chaque dossier de fraude a ses propres caractéristiques et circonstances de fait.

6.7.2. « Action collective » contre Argenta

En novembre 2021, les médias ont rapporté que plusieurs victimes de fraude (vishing, voice + phishing) avaient entamé une action collective contre Argenta. Vous pouvez en savoir plus à ce sujet en cliquant sur les liens suivants : https://www.rtbf.be/info/economie/detail_des-victimes-de-phishing-lancent-une-procedure-collective-contre-argenta?id=10885815;

https://geeko.lesoir.be/2021/11/26/la-banque-argenta-poursuivie-par-des-victimes-de-phishing/

En 2021, Ombudsfin a été confronté à plusieurs reprises à la question de savoir s'il était utile ou non pour les victimes concernées de se joindre à cette action collective. Ombudsfin n'a toutefois pas pour habitude de donner de conseils dans les cas de fraude pour savoir s'il faut ou non entamer une procédure judiciaire. Comme l'appréciation de l'ensemble des circonstances de fait dans les dossiers de fraude est souvent déterminante, Ombudsfin ne peut jamais garantir qu'un tribunal suivra son avis. Les personnes concernées ont toujours été prévenues que chaque dossier de fraude a ses propres caractéristiques (les faits ne sont jamais identiques), comme expliqué ci-dessus[19]. Aux plaignants qui décideraient de se joindre à cette action collective, il est donc recommandé de veiller à ce que les caractéristiques propres à leur dossier soient suffisamment prises en compte.

6.8. Evolutions générales

6.8.1. Codes de validation ou d'activation supplémentaires par SMS

Ombudsfin se réjouit de voir que les banques prennent en compte les recommandations de l'Ombudsman dans les dossiers de fraude. Ombudsfin constate en effet que de plus en plus de banques travaillent avec des codes de validation supplémentaires ou des liens d'activation qui sont envoyés par e-mail ou par SMS à l'adresse e-mail ou au numéro de GSM connus du client. De cette manière, les banques introduisent une étape supplémentaire lorsque, par exemple, des applications mobiles sont installées et que l'on effectue des opérations de paiement. Cette procédure présente plusieurs avantages. Ainsi, si un fraudeur réussit à installer une application mobile liée aux comptes de sa victime, sur base des données interceptées par un mail de phishing, il ne pourra pas utiliser activement cette application tant que celle-ci n'est pas activée via le lien ou le code d'activation envoyé au client. Par ailleurs, au moyen de ces SMS et e-mails envoyés par la banque, l'attention du client est attirée, au cours du processus de fraude, sur le fait qu'il effectue par ses actes une action spécifique mentionnée dans le SMS/e-mail. Enfin, les banques s'assurent, par le biais de ces SMS et e-mails, que c'est le client lui-même qui effectue les actions concernées.

Ombudsfin a également constaté qu'une banque en particulier a choisi de travailler avec un système de détection de fraude dans lequel les transactions suspectes (basées sur des paramètres définis par la banque) sont arrêtées et un SMS contenant un code supplémentaire pour confirmer la transaction est envoyé au numéro de GSM connu du client.

Ombudsfin encourage ces adaptations dans les systèmes de détection des fraudes, les processus de paiement et les procédures d'installation. Malheureusement, Ombudsfin constate que les fraudeurs tiennent également compte de ces adaptations et modifient leur modus operandi en conséquence. Les fraudeurs adaptent leur scénario et manipulent leurs victimes afin d'obtenir ou d'intercepter également ces codes d'activation auprès de leurs victimes. Toutefois, cela ne change rien au fait que l'utilisation d'un code ou d'un lien d'activation supplémentaire offre une sécurité et un contrôle additionnels lors de l'installation d'une application mobile.

Ombudsfin observe également qu'après avoir installé l'application mobile ou s'être connectés au système bancaire en ligne de certaines banques, les fraudeurs parviennent à changer le numéro de GSM de la victime et de renseigner leur propre numéro de GSM. Les codes d'activation et de confirmation requis sont alors envoyés au numéro de GSM du fraudeur. Le fraudeur peut arriver à faire cette substitution en utilisant un ou plusieurs codes générés par la carte bancaire et le lecteur de carte de la victime. Ombudsfin est d'avis qu'à cause de ce fait, il y a une faille dans le mécanisme de sécurité que constitue l'envoi d'un code d'activation ou de confirmation supplémentaire par SMS. Selon Ombudsfin, l'utilité d'un SMS avec un code supplémentaire est que la banque puisse s'assurer que le client effectue lui-même une opération ou installe une application mobile. On observe en effet que le fraudeur aura souvent pu tromper sa victime dans la première phase de la fraude et l'inciter à introduire les codes générés, par exemple, sur un faux site web avec un lecteur de cartes. Il sera donc, à notre sens, plus facile pour le fraudeur d'amener sa victime à introduire des codes supplémentaires générés par le lecteur de carte par l'intermédiaire de ce site web que de convaincre la victime d'introduire un code, qu'elle reçoit par SMS et où le SMS indique clairement qu'il s'agit d'un code d'activation qui ne peut pas être partagé avec quiconque. Ombudsfin recommande donc aux banques concernées de prendre les mesures nécessaires pour éviter de réduire à néant l'utilité de l'envoi de ce SMS en cas de changement du numéro de GSM du client concomitant avec l'installation d'une nouvelle app et de vérifier au moins la légitimité du nouveau numéro de GSM avec le client.

Dans les cas où le fraudeur parvient néanmoins à installer l'application mobile liée aux comptes de sa victime, parce qu'il a intercepté ou obtenu les codes d'activation envoyés ou que la victime a cliqué sur le lien d'activation, il n'y aura, selon nous, pas toujours automatiquement une négligence grave de la part de la victime ou une fraude détectable

[19] *Voir point 6.7.1.*

à l'avance. Cela devra toujours être évalué sur base de l'ensemble des circonstances de fait. Le contexte dans lequel la fraude a pris place, la plausibilité de l'histoire racontée par le fraudeur et le déroulement de la fraude seront toujours d'une importance cruciale. Sur la base de ces appréciations, il conviendra ensuite de déterminer si la banque est obligée ou non d'intervenir dans le dommage.

Enfin, Ombudsfin remarque que les SMS et les e-mails ne sont pas toujours clairement rédigés (par exemple, les SMS sont envoyés avec un code d'activation, sans préciser à quoi sert ce code). Cet aspect doit également être pris en compte dans la détermination d'une éventuelle négligence grave dans le chef du client et de la détectabilité de la fraude. Ombudsfin recommande dès lors aux banques de toujours rédiger les SMS et les e-mails concernés de façon aussi claire que possible.

6.8.2. Un système pour bloquer à la fois la carte bancaire, le compte et l'application mobile

Dans le rapport annuel de 2020 (p. 26), Ombudsfin a déjà souligné la nécessité de faire plusieurs notifications dans un même dossier de fraude afin que tous les instruments de paiement soient bloqués. Par exemple, si le fraudeur a réussi à installer une application mobile liée aux comptes de sa victime, il ne suffira pas toujours de bloquer la carte de paiement via Card Stop. Dans certaines banques, le fraudeur ne pourra alors plus utiliser les données de la carte mais il pourra toujours effectuer des opérations frauduleuses via l'application nouvellement installée. Une notification additionnelle à la banque sera donc nécessaire. Cela n'est pas toujours pratique pour la victime car elle n'a pas toujours une connaissance complète de la procédure et des instruments de paiement installés par le fraudeur. Dans le rapport annuel de 2020, Ombudsfin a toutefois déjà noté que plusieurs banques, lorsqu'elles bloquent la carte de paiement via Card Stop, bloquent aussi automatiquement l'application installée frauduleusement. Ceci doit évidemment être encouragé.

Fin 2021, la secrétaire d'État à la protection des consommateurs, Eva De Bleeker, a annoncé que d'ici l'été 2022, les banques devront offrir un système simple grâce auquel le payeur pourra bloquer sa carte bancaire, son compte bancaire et son application bancaire en un clic de souris ou un appel téléphonique. Un plan en deux étapes est prévu :

1) Tout d'abord, il a été convenu avec les banques que d'ici fin 2021, Card Stop devrait toujours préciser que le simple blocage de la carte ne suffit pas mais qu'il faut également faire bloquer son compte et son application par la banque. D'ici là, les banques devront également être accessibles 24 heures sur 24 ou proposer un système permettant aux clients de bloquer immédiatement leur compte et leur application.

2) Dans une deuxième phase, pour l'été 2022, les banques devront fournir un système simple permettant au payeur de bloquer sa carte bancaire, son compte bancaire et son application bancaire en un clic de souris ou un appel téléphonique.

Vous pouvez en savoir plus à ce sujet dans un article de L'Echo via le lien suivant : https://www.lecho.be/entreprises/banques/phishing-eva-de-bleeker-demande-un-plan-d-action-clair-au-secteur-bancaire/10346434.html

A titre complémentaire, nous tenons à signaler que le numéro de téléphone de Card Stop a changé. Card Stop est désormais joignable au 078/170 170 et il n'y aura plus de frais d'appel à payer. Pour assurer une transition facile vers le nouveau numéro, l'ancien numéro de téléphone (070/344 344) restera toutefois actif pendant quelques années encore mais lorsque vous utilisez ce numéro de téléphone, vous devrez toujours payer les frais d'appel. Vous pouvez en savoir plus à ce sujet en cliquant sur le lien suivant : https://www.rtbf.be/info/economie/detail_un-nouveau-numero-card-stop-pour-eviter-les-frais-supplementaires-est-active-des-lundi?id=10911723

6.8.3. Blocage de la carte : aucune utilisation physique de la carte n'est possible

Comme précisé ci-dessus, Ombudsfin a constaté que le blocage de la carte bancaire via Card Stop n'empêchait pas toute utilisation de la carte physique. Dans ces dossiers, la carte bloquée par Card Stop pouvait encore être utilisée pour générer des codes à l'aide du lecteur de carte afin de se connecter à la banque en ligne et de faire des virements. Dans les dossiers concernés, le blocage de la carte pour se connecter à la banque en ligne et effectuer des virements n'a en effet pas été traité immédiatement, mais seulement par lots.

Une carte bloquée via Card Stop ne devrait plus pouvoir être utilisée physiquement, pas même pour générer des codes à l'aide du lecteur de carte pour ensuite initier des virements en ligne. Si la carte de paiement avait été bloquée correctement et traitée immédiatement, les dommages causés après le blocage de la carte de paiement auraient pu être évités dans ces dossiers.

Il convient toutefois d'observer que dans ces dossiers, les banques sont toujours intervenues pour tous les dommages survenus après le blocage de la carte.

6.8.4. Vérification du nom de l'IBAN selon le modèle des Pays-Bas ?

Ombudsfin constate que certaines banques aux Pays-Bas travaillent avec une vérification du nom de l'IBAN. Cela signifie que lorsqu'un payeur a introduit le numéro de compte IBAN et le bénéficiaire dans son application bancaire en ligne ou mobile, le nom du bénéficiaire est automatiquement vérifié avant l'exécution du virement. Si une irrégularité est détectée, par exemple parce que le nom introduit diffère légèrement du nom connu pour le numéro de compte, le payeur reçoit un avertissement. Le payeur peut alors décider lui-même s'il souhaite toujours effectuer le virement ou non. Vous pouvez en savoir plus à ce sujet sur le site web suivant : https://www.bnnvara.nl/kassa/artikelen/wat-moet-je-weten-over-de-iban-naam-check.

La Belgique travaille également sur une proposition pour instaurer ce contrôle du nom IBAN. Vous pouvez en savoir plus à ce sujet en cliquant sur le lien suivant : https://www.test-achats.be/argent/payer/presse/iban-naamcheck

https://www.test-aankoop.be/geld/betalen/pers/iban-naamcheck#:~:text=Een%20nieuw%20wetsvoorstel%20van%20Micha%C3%ABl,informeert%20of%20die%20wel%20overeenkomen.

La vérification du nom de l'IBAN a pour but de contribuer à la prévention des cas de fraude. Ombudsfin souligne que cette vérification du nom de l'IBAN ne peut être utile que dans les cas de fraude où la victime de la fraude effectue elle-même le virement. Par exemple, il existe des cas de 'fraude à la facture', où les fraudeurs interceptent une facture et modifient le numéro de compte qui y figure. Un autre exemple est la fraude au compte de dépôt sécurisé, où le fraudeur se fait passer pour un employé de la banque par téléphone et conseille à la victime de transférer son argent sur un compte soi-disant nouvellement ouvert au nom du client ou sur un compte de dépôt sécurisé interne de la banque. Dans ces cas de 'fraude à la facture' et de fraude au compte de dépôt sécurisé, une vérification du nom de l'IBAN pourrait être utile. Dans les cas classiques de phishing, où un fraudeur intercepte les données bancaires et les codes générés par la carte bancaire et le lecteur de carte via un faux site web afin d'effectuer lui-même des virements et des paiements, la vérification du nom de l'IBAN ne sera en revanche d'aucune utilité.

6.8.5. Campagnes de lutte contre la fraude

Ombudsfin constate que jamais auparavant la fraude en ligne n'a reçu autant d'attention dans les médias. On peut penser à de nombreuses campagnes de sensibilisation (FSMA, Safeonweb, Febelfin, etc.). Ombudsfin encourage évidemment toutes ces initiatives mais regrette que de telles campagnes soient régulièrement utilisées par les banques contre les consommateurs pour juger d'une négligence grave de la part de la victime de la fraude. Selon Ombudsfin, cela ne peut pas être l'objectif de ces différentes campagnes de lutte contre la fraude.

6.8.6. Signaler la fraude à la banque : permanence

Bien souvent le consommateur se trouve démuni, lorsque victime d'une fraude, il essaye en vain de contacter sa banque en soirée ou un week-end afin de signaler la fraude ou un transfert en cours qu'il souhaiterait bloquer.

En effet, les services de fraude concernés (de la banque de la victime et/ou de la banque du bénéficiaire) ne sont malheureusement pas accessibles 24 heures sur 24, 7 jours sur 7, ce qui signifie évidemment une perte de temps précieux pour le processus de récupération. Dans son rapport annuel relatif à l'année 2019, Ombudsfin recommandait aux banques de mettre en place un système permettant de prendre immédiatement connaissance de ces signalements de fraude.

Ombudsfin est heureux de constater qu'il existe désormais des permanences dans certaines banques et que cela a un impact positif quant à la possible récupération des transferts frauduleux lorsque le client et la banque agissent rapidement. Cela augmente en effet considérablement la probabilité de récupération des fonds.

En effet, si la transaction n'est pas un transfert instantané ou s'il s'agit d'un virement interne vers un compte au sein de la même banque, une réaction rapide permet dans un certain nombre de cas de bloquer la transaction litigieuse ou de récupérer les fonds ou une partie d'entre eux avant le retrait par le fraudeur.

Ombudsfin attire toutefois l'attention du consommateur sur le fait que la mise à disposition d'une permanence par la banque de la victime de la fraude, ne signifie malheureusement pas que les fonds seront automatiquement récupérés étant donné que le succès de la procédure dépend également de la banque bénéficiaire qui est, dans certains cas, établie à l'étranger. L'absence actuelle d'une réglementation sectorielle et européenne ne facilite donc pas la communication rapide entre banques et les chances de récupération.

Ombudsfin recommande enfin aux banques de mettre au point des procédures de notification, de blocage et de récupération adaptées à la vitesse à laquelle les transactions sont actuellement effectuées.

6.8.7. Recommandations

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

- Consultez régulièrement safeonweb.be. Vous y trouverez de nombreux conseils et avertissements utiles sur toutes les pratiques frauduleuses connues sur l'internet.
- Vérifiez toujours l'adresse électronique complète ou l'URL complète d'un site web. Les petites fautes d'orthographe ou l'utilisation de noms de domaine ou d'adresses électroniques atypiques indiquent une fraude. Si vous avez le moindre doute, arrêtez vos actions ou votre communication et faites les vérifications nécessaires par 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 vous laissez pas tenter et arrêtez la communication ou les actions entreprises.
- À l'aide de codes (créés par votre lecteur de carte), un fraudeur peut effectuer des paiements à distance, effectuer des virements via votre homebanking ou même installer votre application bancaire sur son smartphone personnel. Ne communiquez donc jamais à un tiers les codes générés par votre lecteur de cartes.

- N'utilisez jamais votre lecteur de cartes lorsque vous devez recevoir un paiement. Pour cela, un lecteur de cartes n'est jamais nécessaire.

- Les touches et le texte de votre lecteur de cartes vous en disent déjà beaucoup sur les actions que vous entreprenez. Les touches ne disent pas « Acheter », « Signer », « Identifier », « M1 = Identifier = Appli 1 », « M2 = Signer = Appli 2 » par hasard. Soyez conscient de ce que vous faites et lisez également le texte qui peut apparaître sur votre lecteur de cartes.

6.8.7.2. 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 rende toute utilisation physique ultérieure de cette carte complètement impossible. Il n'est pas logique qu'il soit encore possible de se connecter en ligne et d'effectuer des virements avec une carte bloquée.

- Ombudsfin conseille aux banques de rendre leurs SMS plus clairs après avoir créé l'application mobile et d'informer les clients des actions qu'ils peuvent entreprendre pour bloquer l'application mobile, si le client ne l'a pas installée lui-même.

- Les banques informent les clients de la création d'une application mobile en leur envoyant immédiatement un SMS. Toutefois, aucune activation de l'application mobile n'est demandée au client concerné. Ombudsfin a déjà conseillé aux banques de demander au client une activation supplémentaire d'une application nouvellement installée. Cela pourrait empêcher la fraude dans de nombreux cas.

- Afin de renforcer la sécurité des opérations de paiement, la banque devrait adapter son système de surveillance et veiller à ce qu'une alarme se déclenche lorsqu'une nouvelle application est installée et que le numéro de GSM du client est modifié peu de temps après. Le deuxième SMS de la banque contenant le code d'activation peut donc ne pas parvenir au client. Dans cette situation, le client doit être contacté directement avant que toute transaction puisse avoir lieu.

- Ombudsfin se réjouit que des banques demandent désormais au client d'activer lui-même l'application. Toutefois, il est regrettable que le deuxième SMS contenant le code d'activation ne précise pas clairement qu'il s'agit du code d'activation de l'application nouvellement installée. "SMS 2 - Info [Banque]. Votre code est xxxx. Ce code est valable pendant 10 minutes. Ne pas partager avec des tiers ! SMS Gratuit." Le SMS est trop concis et ne fournit pas les informations nécessaires au client.

7. LES GROUPES VULNÉRABLES

Au cours de l'année 2021, Ombudsfin a reçu de nombreux signaux 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 d'un service bancaire adapté à leurs besoins.

Les personnes peuvent se trouver dans une position vulnérable en raison de leur situation financière difficile, parce qu'elles ne connaissent pas les langues nationales, parce qu'elles ont un réseau social très limité, parce qu'elles ne disposent pas des appareils électroniques ou des connaissances techniques nécessaires pour suivre les évolutions digitales et/ou en raison de leur statut spécifique (par exemple, demandeur d'asile).

Ces organisations sociales ont soulevé un certain nombre de problèmes et ont formulé les points d'action suivants: développer une offre de services adaptée, compréhensible et à un prix raisonnable pour ces personnes, plus d'accessibilité physique et de services de la part des banques et une bonne diffusion de l'information au groupe cible et à toutes les organisations sociales impliquées qui soutiennent ce groupe cible.

Ombudsfin a pris note des signaux qui lui ont été adressés. Ombudsfin est conscient de ce problème mais ne peut toutefois le confirmer en tant que tel à partir de ses propres activités.

Nous devons en effet constater que, même en 2021, 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 souhaitons rappeler aux CPAS et aux autres institutions de soutien

qu'ils peuvent soumettre une plainte à Ombudsfin au nom et pour le compte des personnes qu'ils aident, après avoir préalablement soumis la plainte au service des plaintes compétent de la banque en question.

Un exemple de dossier traité par Ombudsfin en 2021 est un dossier où des comptes ont été ouverts pour certains réfugiés mineurs non accompagnés par un tuteur. Le dossier a clairement montré que le suivi et la communication de la banque avaient été insuffisants et tardifs, ce qui a eu pour conséquence que certaines formalités n'étaient plus en ordre et que les comptes ne pouvaient de facto pas être utilisés. Ombudsfin a recommandé à la banque concernée d'adapter ses procédures internes.

Enfin, il semble utile de se référer au « service bancaire universel[20] », récemment introduit, ainsi qu'au service bancaire de base existant (réglementé par le Livre VII du Code de droit économique) qui, en principe, peut offrir une réponse partielle à la problématique susmentionnée des groupes vulnérables.

8. CREDITS

Comme les années précédentes, Ombudsfin a traité en 2021 un certain nombre de plaintes relatives à des crédits aux consommateurs: à la fois des crédits hypothécaires et des crédits à la consommation. Aucun problème spécifique n'est toutefois apparu en 2021 et la tendance à la baisse du nombre de plaintes relatives à ce thème s'est poursuivie (voir les statistiques ci-dessus : points 2.6 et 2.7.).

Dans un certain nombre de dossiers, des recommandations au secteur ont été formulées:

8.1. Recommandations au secteur

- Nous recommandons aux prêteurs de bien clarifier les clauses du document de « demande de crédit » afin que les clients aient des attentes correctes après l'avoir signé.

- Nous recommandons aux prêteurs de communiquer les contrats de crédit à la Centrale des crédits aux particuliers (volet positif) lorsque le contrat est effectivement conclu (signé par les deux parties), et non lorsque l'offre de crédit est établie.

- Nous recommandons aux prêteurs de rédiger des décomptes plus clairs, détaillant tous les éléments pris en considération.

9. DIVERS

Comme le montrent les statistiques, Ombudsfin a également traité un grand nombre de dossiers de succession en 2021. La question de la vie privée a également été abordée de manière occasionnelle dans les dossiers.

Ces dossiers ont donné lieu aux recommandations suivantes :

9.1. Recommandations au secteur

- Nous rappelons aux institutions financières, lorsqu'elles sont informées d'un décès, l'obligation de transmettre cette information à toutes les divisions de la même entité juridique. Il doit y avoir un échange de ces informations entre ces différentes divisions afin que les héritiers reçoivent un aperçu global et complet des avoirs par l'intermédiaire de cette seule institution financière.

- Nous recommandons aux institutions financières d'indiquer clairement quels fichiers elles peuvent consulter pour se conformer à leurs obligations en matière de lutte contre le blanchiment d'argent (identification).

[20] *Voir point 4. Considérations générales*

10. SERVICE BANCAIRE DE BASE POUR LES ENTREPRISES

10.1. Introduction

Les entreprises ont besoin d'un compte bancaire pour fonctionner correctement. Elles doivent être en mesure de recevoir et d'effectuer des paiements, elles doivent tenir une comptabilité et elles ont des obligations envers différentes autorités, telles que le fisc, l'ONSS, etc. Le fait d'avoir un compte est également une condition pour être inscrite à la BCE (Banque-Carrefour des Entreprises).

Cependant, certaines entreprises rencontrent actuellement de sérieux problèmes pour ouvrir un compte bancaire. Parfois, ce problème est même sectoriel, comme dans le secteur du diamant, les ambassades et les secteurs où beaucoup d'espèces circulent (par exemple, les casinos).

En 2021, notre service a reçu environ 70 demandes écrites d'entreprises rencontrant des problèmes parce qu'elles n'avaient pas de compte bancaire, et ce n'est évidemment que la partie émergée de l'iceberg.

Suivant ce qui existe déjà pour les consommateurs depuis 2003[21], le législateur a voté, en 2020, une loi pour aider les entreprises confrontées à une exclusion bancaire.

10.2. La loi du 8.11.2020 prévoit un droit à un service bancaire de base pour les entreprises

La loi du 8.11.2020 prévoit, sous certaines conditions, un droit à un « service bancaire de base pour les entreprises ». Cette loi a introduit les articles VII 59/4 à VII 59/8 dans le livre VII du Code de droit économique.

La loi susmentionnée est entrée en vigueur le 1.05.2021. Toutefois, à cette époque, les préparatifs de la chambre des services bancaires de base prévue par le SPF Economie n'étaient pas encore terminés, de sorte que l'arrêté d'exécution n'a pas pu être pris à temps.

Et ce n'est toujours pas le cas au moment de la rédaction de ce rapport annuel[22]. Par ailleurs, la loi elle-même doit être réécrite, entre autres pour tenir compte de la problématique du RGPD.

Entretemps, l'État belge a été condamné par un jugement pour le retard dans l'application de la loi[23]. Apparemment, il faudra encore attendre l'été 2022 pour que la loi soit effectivement appliquée et que les entreprises puissent obtenir un service bancaire de base, ce qui est évidemment regrettable.

10.3. Principaux aspects de la procédure prévue par la loi pour obtenir un service bancaire de base.

Pour obtenir un service bancaire de base, une entreprise doit d'abord faire face au refus de 3 banques différentes de lui ouvrir un compte bancaire avec des services de base. Elle peut ensuite soumettre une demande pour un service bancaire de base à la « Chambre des services bancaires de base », qui est chargée de désigner le prestataire de services[24]. Comme mentionné ci-dessus, cette Chambre n'a pas encore été créée par le SPF Economie.

La loi stipule que la Chambre contacte la Cellule de Traitement des Informations Financières (CTIF). Il s'agit de vérifier si l'entreprise n'a pas fait l'objet d'une déclaration de soupçon au titre de la législation anti-blanchiment. Si la CTIF est d'accord (ou si aucune réaction n'est reçue de sa part dans un délai de deux mois), la Chambre peut, après avoir examiné les autres conditions, décider d'obliger une banque systémique[25] à ouvrir un service bancaire de base pour entreprises.

Outre le service bancaire de base imposé à une banque, la loi prévoit également la possibilité pour les banques d'offrir ce service de manière spontanée. Dans ce cas, la banque qui souhaite le faire doit indiquer clairement ce «service» sur son site web, avec les conditions, les caractéristiques et les coûts qui y sont liés. A ce jour, Ombudsfin ne connaît aucune banque qui offre ce service spontanément.

[21] *Loi du 24.03.2003 instaurant un service bancaire de base.*

[22] *Le 10 mars 2022.*

[23] *Jugement du 6.12.2021 du tribunal de première instance néerlandophone de Bruxelles (réf 19-3281-A) . L'Etat belge a fait appel de ce jugement.*

[24] *Dans le cas du «service bancaire de base pour les consommateurs», la loi prévoit qu'Ombudsfin peut désigner une banque qui doit ouvrir le service bancaire de base. Sa décision est contraignante à cet égard. Ce n'est pas le cas pour le service bancaire de base pour les entreprises.*

[25] *En Belgique, il y a actuellement 8 banques systémiques, à savoir BNP Paribas Fortis, KBC Group, Belfius Banque, ING Belgique, Argenta, Axa Bank Belgium, Euroclear et The Bank of New York Mellon. Cependant, il nous semble peu probable que les deux dernières soient un jour désignées, compte tenu de leurs activités spécifiques.*

10.4. Le rôle d'Ombudsfin en cas de refus ou de résiliation d'un service bancaire de base

La loi du 8 novembre 2020 stipule qu'Ombudsfin est compétent pour intervenir en cas de refus ou de résiliation d'un service bancaire de base (indépendamment du fait que ce service soit offert par une banque spontanément ou à la demande de la Chambre).

En effet, la loi prévoit que même si une banque est désignée par la Chambre, elle peut toujours invoquer quelques arguments (limitativement définis) pour refuser d'ouvrir ou résilier un service bancaire de base. Ombudsfin procédera alors à un examen approfondi des motifs invoqués et, si ces motifs ne sont pas fondés, annulera la décision de l'établissement financier. La décision d'Ombudsfin est contraignante pour la banque.

Comme il n'y a actuellement aucune banque qui soit obligée d'offrir un service bancaire de base, ni aucune banque qui offre ce service spontanément, Ombudsfin n'a pas encore été sollicité à cet égard.

Par conséquent, en 2021, notre service s'est limité à informer les entreprises concernées de la situation juridique concernant le service bancaire de base.

Dans certains cas, au cours de la procédure de médiation, nous avons demandé à la banque qui avait mis fin à la relation bancaire avec l'entreprise de poursuivre temporairement cette relation, afin de donner à l'entreprise suffisamment de temps pour trouver une autre banque, étant donné que l'entreprise ne pouvait pas encore obtenir un service bancaire de base. Plusieurs banques ont accueilli favorablement notre demande et ont accordé cette prolongation temporaire dans l'intérêt de l'entreprise.

11. FIN-NET : PLAINTES TRANSFRONTALIÈRES

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

11.1. 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. Dans certains pays, il existe différents organismes de règlement alternatif des litiges, dont la compétence est fonction du type de litige ou du statut de l'établissement financier concerné. Il peut également arriver que certains médiateurs ne fassent pas partie du réseau FIN-NET. En ce cas, Ombudsfin essayera tout de même d'orienter le requérant vers l'organisme compétent.

11.2. Exemples concrets

En 2021, Ombudsfin a reçu 4 dossiers dans le cadre desquels la procédure FIN-NET a été utilisée. 3 dossiers concernaient des institutions espagnoles, un dossier concernait une institution maltaise.

Les problématiques soulevées étaient : l'impossibilité de clôturer un compte à distance (2 dossiers), l'impossibilité de consulter le compte (plus accès à la banque en ligne) et le blocage d'un compte.

12. COLLABORATION

12.1. BELGIQUE

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 4/04/2014 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.

12.1.2. CPMO

L'ombudsman fait partie de la « Concertation permanente des Médiateurs et Ombudsmans », la CPMO. Celle-ci 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 sur la CPMO sont disponibles sur le site www.ombudsman.be

12.1.3. 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

12.2. EUROPE

12.2.1. 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".

12.2.2. ODR

La plateforme ODR est une plateforme lancée en 2016 par la Commission européenne et destinée aux consommateurs et aux professionnels effectuant des transactions 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)

12.3. 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.

13. MOYENS FINANCIERS

Au moment de la publication de ce rapport annuel 2021, les comptes annuels de l'exercice comptable d'Ombudsfin asbl de 2021 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 2021:

	Budget 2021
Revenus	
Cotisation fixe membres Ombudsfin asbl	601.775,00
Cotisation variable membres Ombudsfin asbl	601.775,00
Revenus totaux	**1.203.550,00**
Dépenses ordinaires	
Frais de personnel + honoraires	1.149.000,00
Frais de fonctionnement	129.550,00
Dépenses ordinaires totales	**1.203.550,00**
Dépenses extraordinaires, prélevées de la réserve	*75.0000*

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.

14. OMBUDSFIN – À VOTRE SERVICE

14.1. INTRODUIRE UNE PLAINTE AUPRÈS D'OMBUDSFIN

Qui peut introduire une plainte ?

Chaque client d'une banque, d'un intermédiaire en services bancaires et en services d'investissements, d'une société de crédit, d'un intermédiaire de crédit, d'un établissement de paiement, d'une société de Bourse ou d'un conseiller en placement, agissant comme personne physique dans le cadre de ses intérêts privés, peut faire appel à Ombudsfin quand il n'a pas obtenu satisfaction.

Ombudsfin est également compétent pour certaines plaintes des entreprises.

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 (au sein de l'Union Européenne) 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 comme suit :

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

Par 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.

Il existe un résumé de toutes les conditions de recevabilité dans le Règlement de procédure, publié sur le 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, il est pris contact 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.

14.2. COLLABORATEURS ET CONSEILLERS OMBUDSMAN

Pour le traitement des demandes, l'ombudsman est entouré de 3 assistants et de 5 conseillers :

Assistants

Serge Henris, Christel Speltens et Ingrid Vertenten (conseiller à temps partiel).

Conseillers

Christine Buisseret, Vincent Chambeau, Bérengère de Crombrugghe, Brent De Waele et Elke Heymans.

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 2021: Françoise Sweerts (présidente – à partir de mai 2021), Nadine Spruyt, Johan Vannerom, Reinhard Steennot, Alain Guigui, Philippe D'Haen.

Collège d'experts pour les plaintes concernant les crédits aux entreprises

Ce Collège est composé d'une présidente indépendante : Françoise Sweerts, 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.

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

ombudsman@ombudsfin.be

www.ombudsfin.be