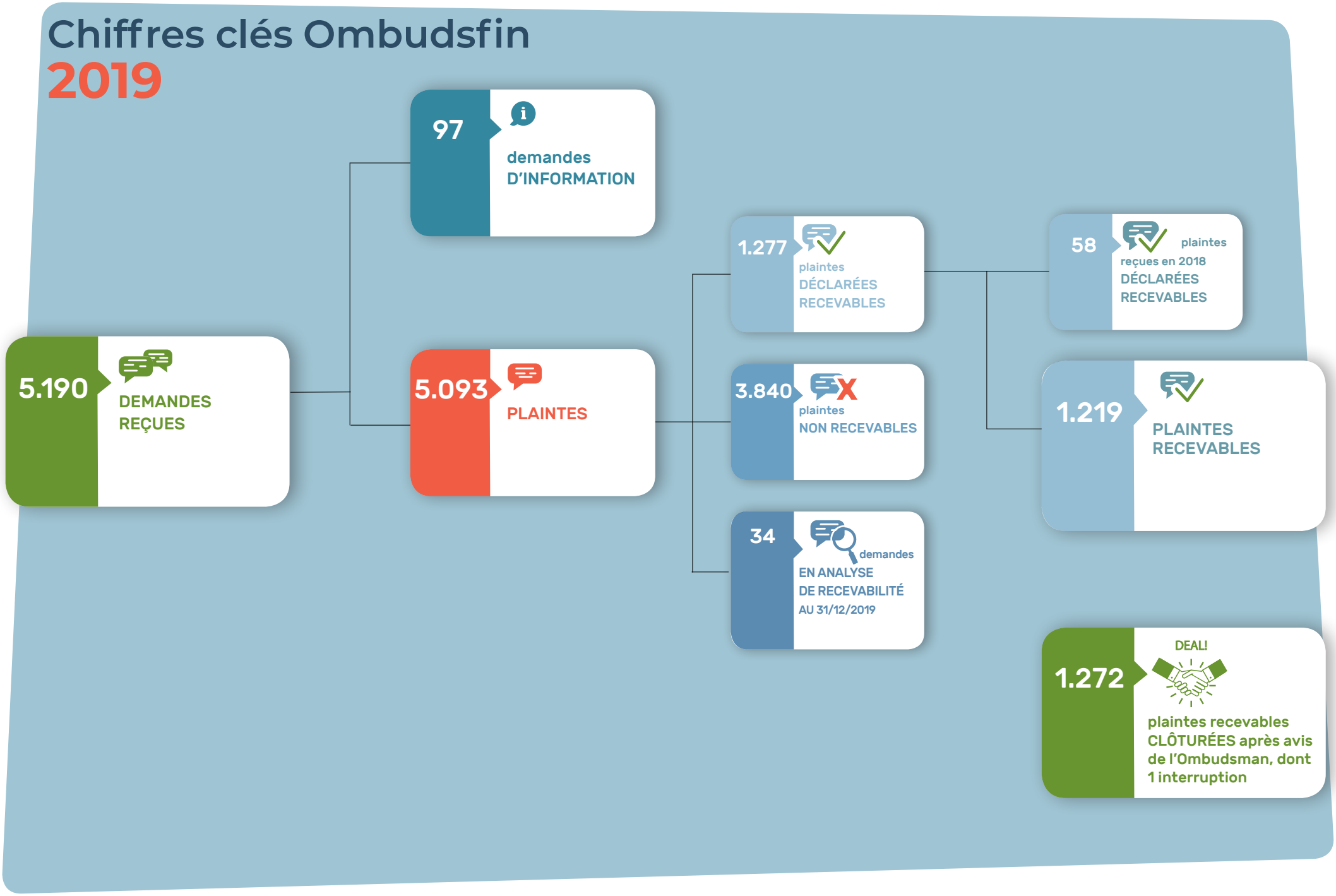
RAPPORT ANNUEL

2019

OMBUDSFIN

Chiffres clés Ombudsfin 2019



“ L’intervention de l’Ombudsman s’est conclue par un **résultat positif** dans **86,6%** des plaintes fondées déposées par les **consommateurs** et **51,5%** de celles des **entreprises** ”

4 890 DEMANDES de consommateurs

1 196 Plaintes RECEVABLES consommateurs

- **647** Paiements et comptes de paiement
- **289** Crédits
- **151** Investissements
- **93** Divers
- **16** Epargne

300 DEMANDES d’entreprises

81 plaintes RECEVABLES entreprises

- **1** Paiements internationaux
- **10** refus de remboursement anticipé
- **2** Divers
- **27** Funding Loss
- **13** Garanties
- **8** Dénonciation
- **2** Motivation refus de crédit
- **1** Devoir de s'informer et de conseil (responsible lending)
- **4** Difficultés (plan de remboursement)
- **5** Enregistrement BNB
- **3** Taux
- **4** Coûts
- **1** Procédure d'octroi de crédit (durée)

Table des matières

AVANT-PROPOS

STOP au phishing des données bancaires :

Ombudsfin lance un appel pour appuyer les campagnes de prévention contre les manipulations de fraudeurs qui parviennent encore trop souvent à détourner des fonds par ruse en profitant de la crédulité des victimes !

Ce rapport rappelle quelques consignes de sécurité pour ne pas se laisser piéger. Consulter régulièrement le site www.safeonweb.be

L'année 2019 est marquée par une augmentation frappante des plaintes qui portent sur des paiements contestés suite à une fraude internet. Ce rapport annuel y sera donc consacré. La lutte contre la fraude aux paiements en ligne doit prendre une place encore plus grande tant auprès de la clientèle des banques que des banques elles-mêmes. La digitalisation des paiements a fragilisé davantage une portion de la population moins avertie et donc plus sujette à la manipulation en raison d'une méconnaissance des mécanismes de paiement.

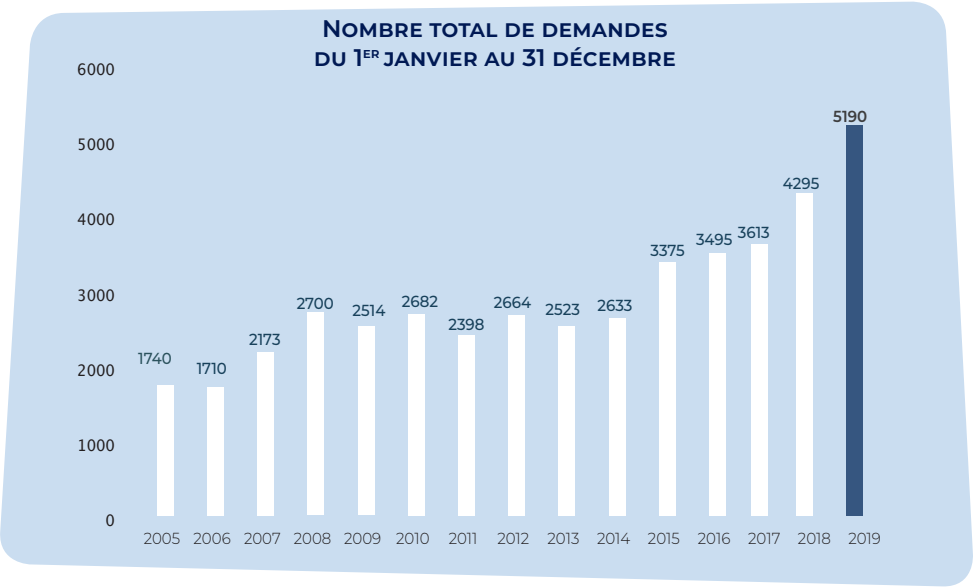
Ombudsfin encourage le secteur bancaire à renforcer la sécurité des paiements et, notamment, à mettre en place des procédures adéquates pour déceler et intercepter les fraudes dès constatation de celles-ci.

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 2019 s'élève à 5.190. Cela représente une augmentation de 895 dossiers ou 20,8 % par rapport à 2018.

Le tableau ci-dessous représente l'augmentation soutenue des cinq dernières années, avec une nouvelle hausse exceptionnellement forte en 2019.



Ces chiffres comprennent toutes les nouvelles demandes d'informations et plaintes écrites qui ont été soumises à Ombudsfin en 2019.

Dans chacun de ces dossiers, le client a reçu d'Ombudsfin une réponse à sa demande et 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

Comme mentionné ci-dessus, Ombudsfin a enregistré, en 2019, 5.190 nouvelles demandes de consommateurs et d'entreprises.

5.093 de ces demandes concernaient une plainte, 97 étaient des demandes d'information.

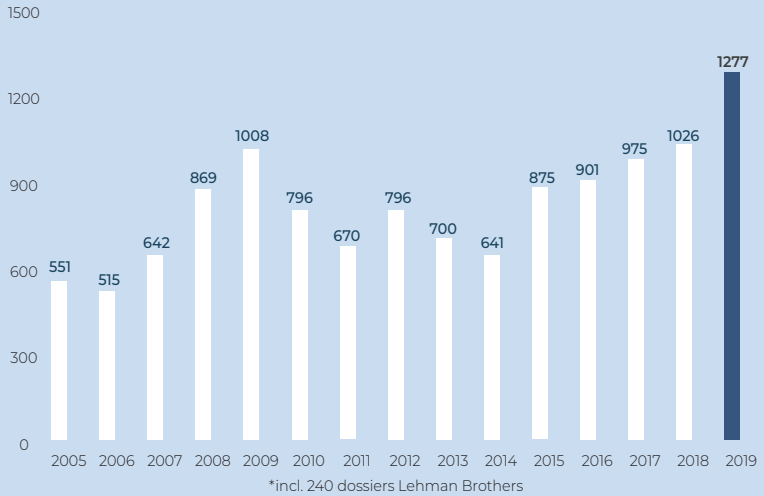
Ombudsfin a répondu au mieux aux demandes d'informations qui lui sont parvenues.

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.
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.

Parmi les 5.093 plaintes introduites en 2019, 1.219 (soit 24 %) ont été déclarées recevables.
En outre, 58 plaintes introduites en 2018 ont été déclarées recevables en 2019.
Au total, ce sont donc 1.277 plaintes qui ont été déclarées recevables en 2019, ce qui représente une augmentation de 24,5 % (soit 251 plaintes) par rapport aux 1.026 plaintes recevables de 2018.

Nombre total de dossiers recevables du 1er janvier au 31 décembre



*incl. 240 dossiers Lehman Brothers

1.2.3. Plaintes non recevables

Parmi les 5.093 plaintes introduites en 2019, 3.840 (soit 75,4 %) ne remplissaient pas les conditions de recevabilité.
Les requérants ont toujours été informés de façon étendue quant aux raisons de l'impossibilité d'accéder à leur demande.

Raison	Nombre
La plainte n'a pas encore été introduite auprès de l'institution financière	2.661
Le client ou l'institution n'est pas identifiable, l'objet de la demande n'est pas identifiable	448
Demande fantaisiste, vexatoire ou diffamatoire	0
Demande soumise il y a plus d'un an au service des plaintes de l'institution financière	4
Procédure judiciaire ou demande déjà traitée par une entité qualifiée	25
Le traitement de la demande porterait sérieusement atteinte au bon fonctionnement d'Ombudsfin	0
L'institution financière n'est pas affiliée chez Ombudsfin (p.e. bureaux de recouvrement, institutions financières étrangères)	168
Ombudsfin n'est pas compétent en la matière	464
Combinaison de causes mentionnées ci-dessus	70
TOTAL	**3.840**

Si un autre service était compétent ou si la première ligne n'avait pas encore été interpellée et que l'institution financière en question était connue, les coordonnées du service compétent étaient transmises au requérant.

En outre, à la fin de 2019, il y avait 34 demandes en attente d' analyse de recevabilité.

1.3. DÉLAIS DE TRAITEMENT DES PLAINTES RECEVABLES

Le délai moyen de traitement de toutes les plaintes recevables, clôturées en 2019 est de 45 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 2019, 100 dossiers ont été prolongés. Les parties ont été prévenues à temps de cette prolongation.

1.4. INTERRUPTION DE LA PROCÉDURE DE MÉDIATION

Dans 1 dossier recevable la procédure de médiation a été interrompue. La raison était un accord amiable atteint directement entre les parties.

1.5. LES INSTITUTIONS FINANCIÈRES CONCERNÉES PAR LES PLAINTES RECEVABLES

Ci-dessous, les catégories d'institutions financières concernées par les plaintes recevables en 2019, avec mention des chiffres et pourcentages précis :

Institutions financières concernées par les plaintes recevables	2019	
Banque	1090	85,36%
Société de crédit	127	9,95%
Établissement de paiement	25	1,96%
Courtier de crédit	11	0,86%
Prêteur social	8	0,63%
Société de bourse	7	0,55%
Asset Manager	3	0,23%
Société de leasing	3	0,23%
Etablissement de monnaie éléctronique	1	0,08%
Bureau de change	1	0,08%
Compagnie d'assurances	1	0,08%
TOTAL	**1277**	**100,00%**

1.6. ENQUÊTE DE SATISFACTION

1.6.1. Méthodologie

Au cours de l'année 2019, les clients avec une plainte recevable et réglée ont eu la possibilité d'exprimer, de façon anonyme, leur opinion sur Ombudsfin. Chaque requérant s'est vu remettre un code, 1 mois après l'envoi de l'avis, donnant accès à une enquête en ligne composée de 26 questions. Ce délai d'un mois se justifie par la volonté d'éviter les réactions « à chaud », donc moins objectives.

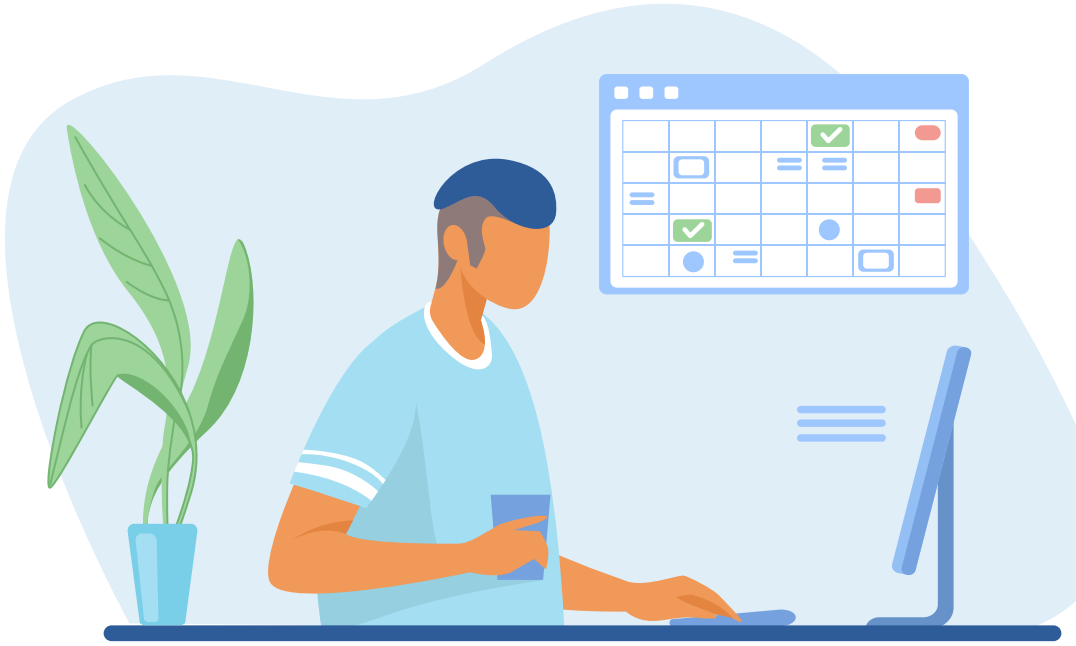
Les questions abordent l'ensemble des aspects du traitement des dossiers et visent à mesurer la satisfaction des requérants relativement à ces aspects.

Outre la satisfaction générale, sont notamment passés en revue l'opinion du requérant sur le premier contact, la façon dont il perçoit le traitement de son dossier, le délai de traitement, le soutien reçu pendant le traitement, la qualité rédactionnelle de l'avis reçu, l'impartialité du service ou encore l'utilité sociale du service. Une des questions porte aussi sur le résultat de l'avis reçu par le répondant à l'enquête afin d'établir une correspondance entre son opinion et le résultat de sa plainte. Il va en effet de soi que la perception qu'un requérant a du service est fortement influencée par l'issue réservée à sa requête.

Pour la plupart des questions, le requérant répond en cochant une case sur une échelle de 1 à 6, le 1 représentant un grand mécontentement et le 6 une grande satisfaction. D'autres questions demandent une réponse par oui ou par non. Une dernière série de questions permet aux gens de s'exprimer plus librement en rédigeant une courte réponse exprimant leur ressenti.

L'objectif de cette étude pour le service est d'évaluer l'efficacité de sa procédure vis-à-vis des requérants et d'identifier à la fois les points positifs qui doivent être consolidés et les points négatifs afin de tenter d'améliorer les aspects qui semblent poser problème et offrir un service qui corresponde mieux, dans la mesure du possible, aux attentes des requérants. En fonction de ces résultats, des mesures d'amélioration du service seront mises en place en 2020 pour pallier les manquements constatés. Ensuite, une nouvelle enquête de satisfaction sera lancée en 2020 afin de constater si les mesures prises auront eu l'effet escompté sur la perception qu'ont les requérants d'Ombudsfin.

En principe, Ombudsfin informe sur les résultats par le biais du rapport annuel tous les 2 ans.



1.6.2. Chiffres et enseignements

Taux de participation

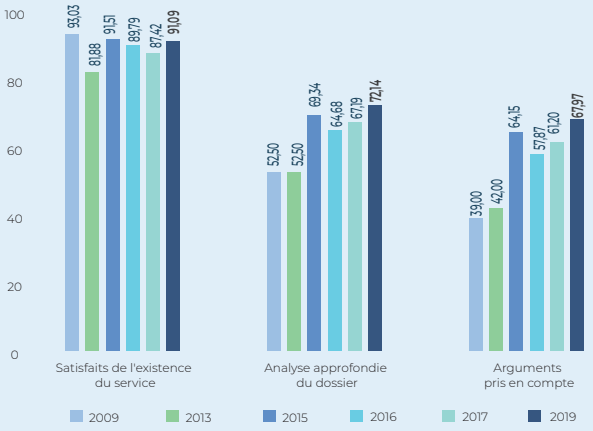
Le taux de participation en 2019 est de : 36,01%.

Au niveau de l'avis reçu, on observe que 43,73% des répondants ont reçu un avis positif et que 56,27% ont reçu un avis négatif. Cela indique qu'en 2019 les personnes ayant un avis négatif ont eu légèrement plus tendance à faire part de leurs impressions.

Les scores de satisfaction globale sont encore bons, même meilleurs que ceux des années précédentes.

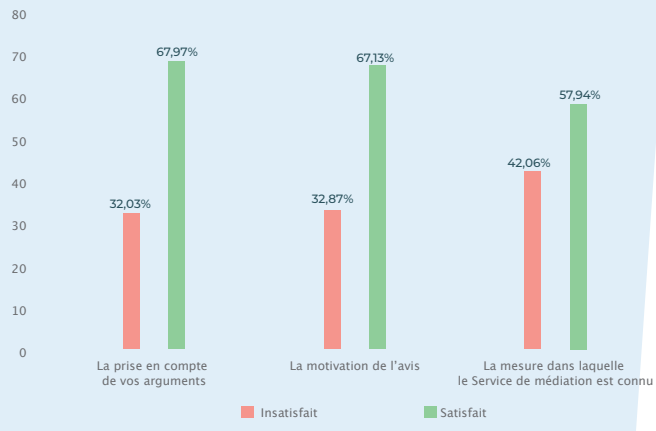
En général, Ombudsfin s'efforce d'obtenir un score minimum de 70% sur tous les aspects testés. Sur base de cet objectif minimal, une distinction est faite entre les aspects à consolider et ceux à améliorer.

Satisfaction générale



Aspects à consolider

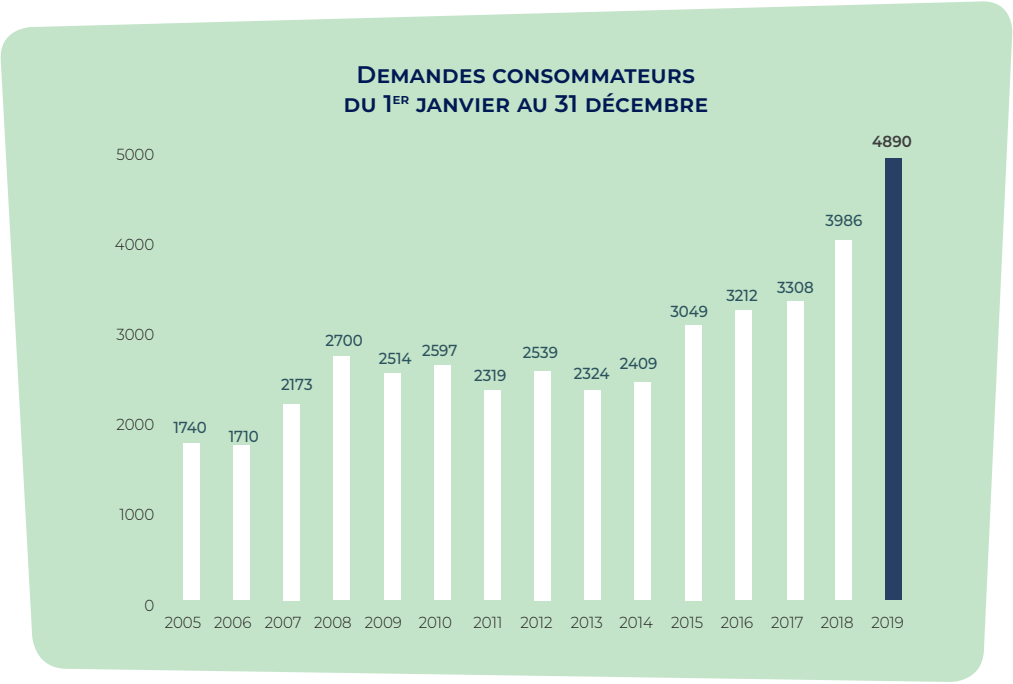
Aspects à améliorer



2. DEMANDES INTRODUITES PAR LES CONSOMMATEURS

2.1. FORTE AUGMENTATION DU NOMBRE DE DEMANDES

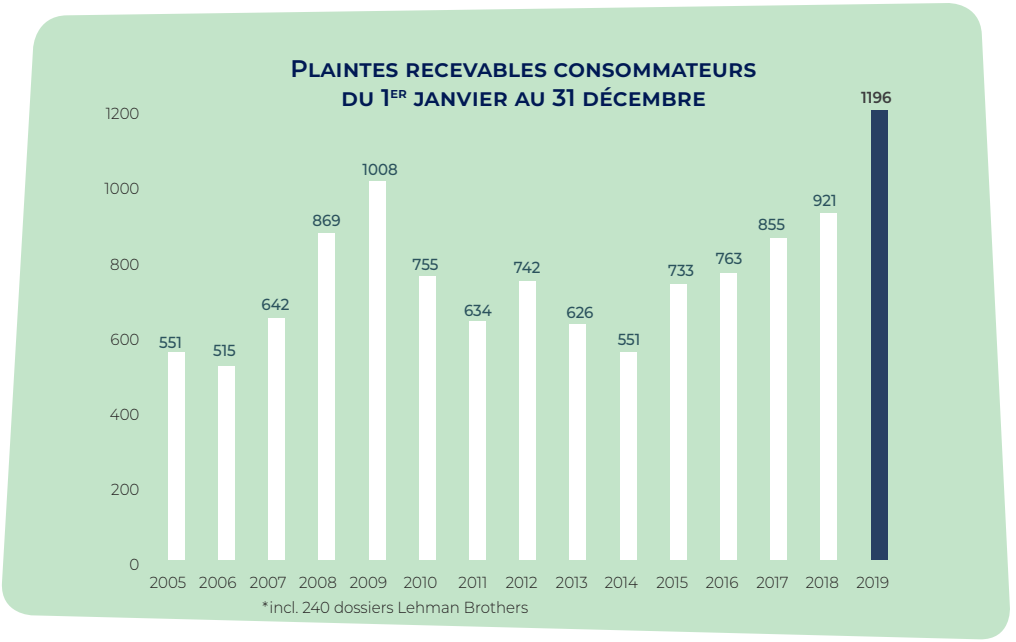
En 2019, Ombudsfin a reçu 4.890 demandes de consommateurs contre 3.986 en 2018, ce qui représente une augmentation de 904 dossiers ou 22,7% par rapport à 2018.



Ombudsfin a répondu au mieux à 96 demandes d'information. 4.794 demandes concernaient une plainte.

2.2. FORTE AUGMENTATION DU NOMBRE DE PLAINTES RECEVABLES

En 2019, Ombudsfin a enregistré 1.196 demandes de consommateurs comme étant recevables contre 921 en 2018, ce qui représente une augmentation de 275 dossiers ou 29,9% par rapport à 2018.



2.3. RÉSULTATS DES PLAINTES RECEVABLES DE CONSOMMATEURS CLÔTURÉES EN 2019

Ces résultats se rapportent à toutes les plaintes des consommateurs réglées en 2019. Certaines plaintes introduites avant 2019 auprès d'Ombudsfin sont donc aussi incorporées dans ces résultats.

On totalise 1.185 dossiers.

Dans 591 dossiers (soit 49,9%), Ombudsfin a considéré la plainte comme fondée sur la base de la législation, de dispositions contractuelles, de codes de conduite, de pratiques du marché, de codes déontologiques ou de tout autre élément utile à la résolution du conflit.

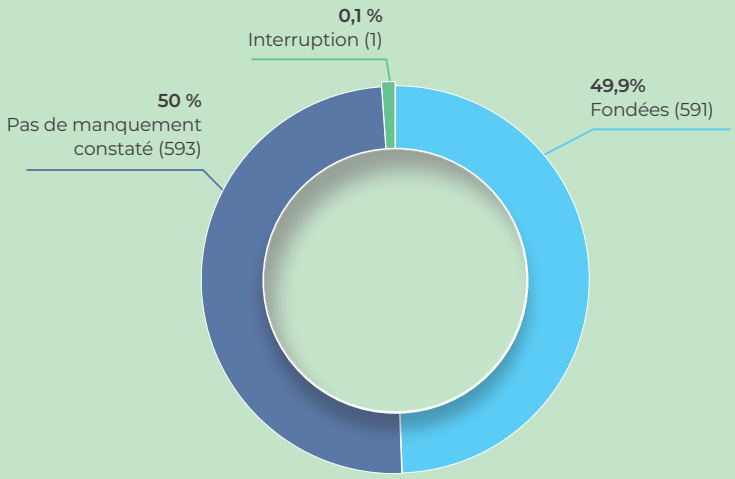
Pour 593 dossiers (soit 50%), Ombudsfin n'a pas pu établir de manquement dans le chef de l'institution financière. Dans ces dossiers, les informations et explications additionnelles nécessaires ont été données au client afin qu'il puisse comprendre pourquoi Ombudsfin est parvenu à cette conclusion et pourquoi une réparation ou indemnité de la part de l'institution financière ne pouvait être réclamée.

Dans 1 dossier restant (soit 0,1%) la procédure de médiation a été interrompue par le consommateur.

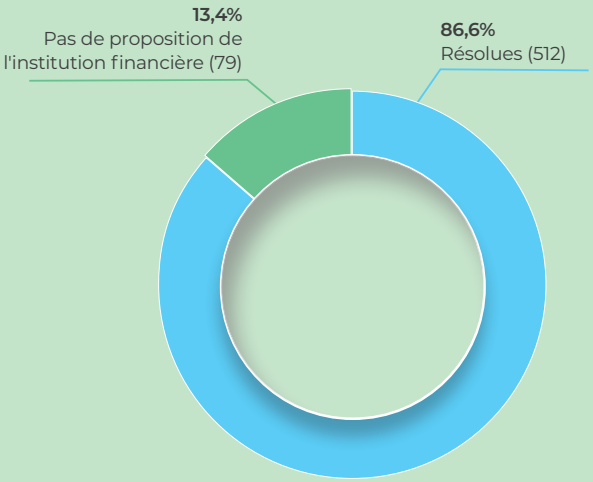
Des 591 plaintes considérées comme fondées par Ombudsfin, 86,6% ont été résolues.

Pour les dossiers de fraude en ligne, l'analyse de l'Ombudsman ne coïncide pas toujours avec celle des institutions financières.

PLAINTES CONSOMMATEURS CLÔTURÉES 2019



PLAINTES FONDÉES CONSOMMATEURS 2019



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.

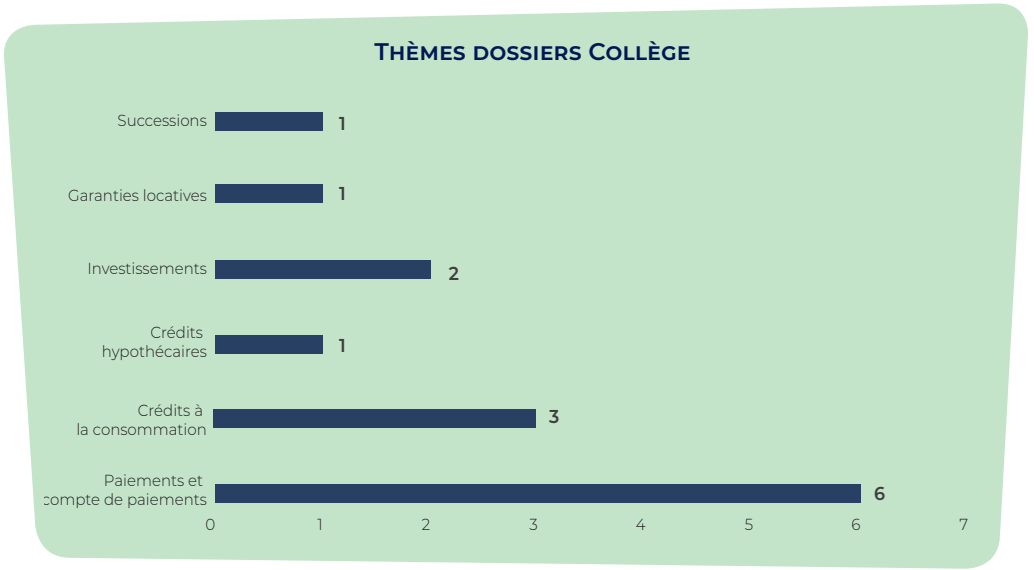
Ces recommandations sont soit formulées dans un cadre plus large comme une adaptation des procédures, des conditions générales ou de la liste des tarifs, soit portent sur une solution concrète limitée au cas examiné.

En 2019, 41 recommandations individuelles ont été formulées. Les institutions financières ont donné une suite favorable à 21 recommandations (51,2%). 12 recommandations (soit 29,3%) n'ont pas été suivies, l'institution en ayant expliqué les raisons. 8 recommandations (soit 19,5%) faisaient encore l'objet d'une enquête plus approfondie de la part de l'institution financière au moment de la rédaction du présent rapport.

2.5. COLLÈGE D'EXPERTS[1]

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

En 2019, 14 dossiers ont été soumis au Collège. Les thèmes étaient les suivants :



11 des 24 dossiers (78,6%) ont été jugés fondés.

Pour 4 de ces 11 plaintes (36,4%), une solution a été trouvée entre les parties. Dans 4 dossiers, les négociations sur une solution étaient encore en cours au moment de la rédaction du rapport annuel. 3 dossiers sont restés sans proposition de solution de la part de l'institution financière[2].

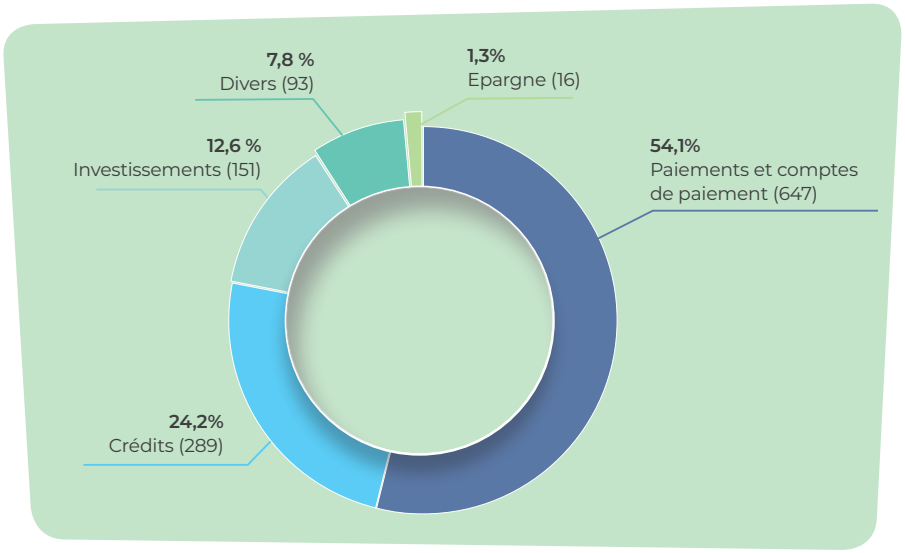
1 Le Collège est composé d'experts fixes indépendants. Composition du Collège d'experts en 2019 : Aloïs Van Oevelen (président), Nadine Spruyt, Johan Vannerom, Reinhard Steennot, Alain Guigui.
2 Les institutions financières concernées sont : ING, Banque Degroof Petercam, Belfius.

2.6. THÈMES DES PLAINTES RECEVABLES DES CONSOMMATEURS

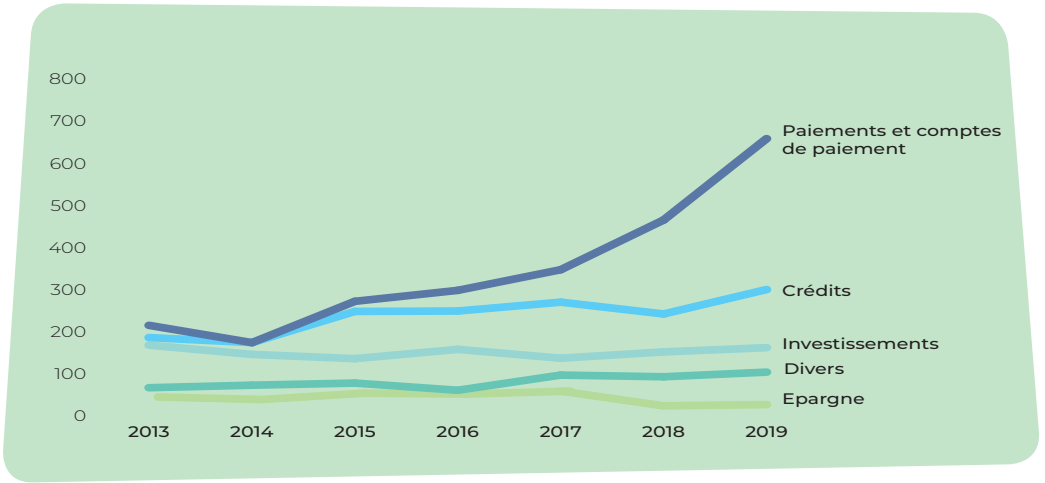
Les thèmes des plaintes recevables des consommateurs en 2019 étaient les suivants :

	2015	2016	2017	2018	2019	2015	2016	2017	2018	2019
THEMES	Nombre					%				
Paiements et comptes de paiement	261	287	336	454	**647**	35,61	37,61	39,30	49,30	**54,10%**
Crédits, dont	237	238	259	231	**289**	32,33	31,19	30,29	25,08	**24,16%**
Crédits à la consommation	*123*	*110*	*126*	*107*	**159**	*16,78*	*14,42*	*14,74*	*11,62*	**13,29%**
Crédits hypothécaires	*114*	*128*	*133*	*124*	**130**	*15,55*	*16,78*	*15,56*	*13,46*	**10,87%**
Investissements	125	147	126	141	**151**	17,05	19,27	14,74	15,31	**12,63%**
Autres	67	50	86	82	**93**	9,14	6,55	10,06	8,90	**7,78%**
Epargne	43	41	48	13	**16**	5,87	5,37	5,61	1,41	**1,34%**
TOTAL	**733**	**763**	**855**	**921**	**1196**	**100%**	**100%**	**100%**	**100%**	**100%**

Le principal thème de 2019 est, comme en 2018, à nouveau avec une grande avance, "Paiements et comptes de paiement" avec 647 dossiers. Ce thème représente un peu plus de la moitié (54,10 %) des plaintes recevables.



Le graphique ci-dessous indique une tendance claire dans l'évolution des différents thèmes. C'est le thème des "paiements et comptes de paiement" qui gagne clairement en importance. Cela est principalement dû au grand nombre de dossiers de fraude (contestation d'opérations de paiement frauduleuses).



2.7. UN APERÇU DES SOUS-THÈMES LES PLUS IMPORTANTS

Avant d'aborder le thème principal de 2019 (les opérations de paiement frauduleuses), un bref aperçu des sous-thèmes les plus importants de chaque thème principal est présenté :

Paiements et comptes de paiement		**647**
1.	Opérations à distance frauduleuses	221
2.	Opérations après vol ou perte de carte frauduleuses	95
3.	Fin relation bancaire	74
Crédits à la consommation		**159**
1.	Enregistrement Banque Nationale	48
2.	Conclusion et contenu contrat	20
3.	Décompte	18
Crédits hypothécaires		**130**
1.	Décompte	16
2.	Procédure octroi de crédit (durée,...)	14
3.	Refus	13
	Conclusion et contenu contrat	13
Investissements		**151**
1.	Comptes titres	41
2.	Achat et vente de titres (execution only)	34
3.	Aspects fiscaux	19
Divers		**93**
1.	Succession	50
2.	Garanties locatives	15
3.	Privacy	14
Epargne		**16**
1.	Clôture (comptes dormants)	7
2.	Comptes à terme	4
3.	Bons de caisse	1
	Parts de coopérateurs	1

Le service bancaire de base, un sous-thème de "Paiements et comptes de paiement" sur lequel Ombudsfin fait explicitement rapport chaque année.

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 2019, Ombudsfin a reçu 4 plaintes concernant le service bancaire de base.

Au cours de l'année 2019, Ombudsfin a eu des entretiens avec d'autres organismes compétents dans ce domaine (Unia, Myria, SPF Economie). Il semble qu'il y ait plus de plaintes relatives aux services bancaires de base que celles qui parviennent à Ombudsfin. En tant que service de médiation compétent qui fournit des avis contraignants en la matière, Ombudsfin ne peut que conseiller à tous les organismes qui recoivent des plaintes concernant l'application du service bancaire de base de transmettre les dossiers à Ombudsfin.

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 2019 :

Statistiques Service bancaire de base (SBB)	**2019**
Nombre de banques ayant enregistré une demande de SBB	10
Nombre de comptes SBB ouverts	9.224
Nombre total de comptes SBB existants	16.740
Nombre de refus d'ouverture d'un compte SBB	2
Nombre de comptes SBB résiliés (*)	1.825

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

En 2019, 10 banques ont enregistré des demandes de services bancaires de base, soit 2 de moins qu'en 2018.

Le nombre de services bancaires de base ouverts a augmenté de 39,4 % (9.224 en 2019). En 2018, il y a eu 1 868 ouvertures.

En 2019, deux demandes d'ouverture de services bancaires de base ont été refusées en raison d'antécédents négatifs auprès de la banque.

La principale raison d'une fermeture est la demande du titulaire (96,90%), suivi par

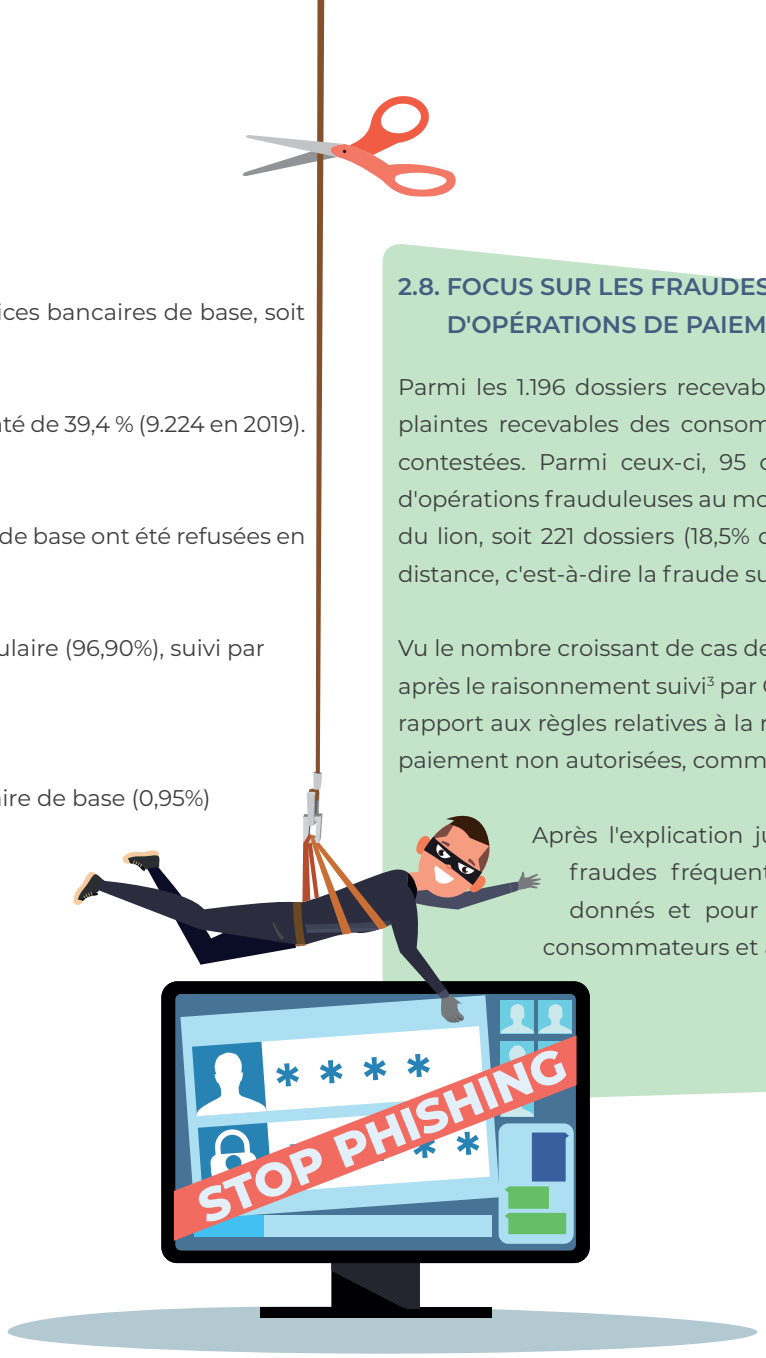
- Compte courant dans une autre institution (1,14%).
- Antécédents négatifs à la banque (1,01%)
- Autres produits non compatibles avec le service bancaire de base (0,95%)

2.8. FOCUS SUR LES FRAUDES - RÉPARTITION DE LA RESPONSABILITÉ EN CAS D'OPÉRATIONS DE PAIEMENT NON AUTORISÉES

Parmi les 1.196 dossiers recevables en 2019, 316 dossiers (26,4% du nombre total de plaintes recevables des consommateurs) concernaient les opérations frauduleuses contestées. Parmi ceux-ci, 95 dossiers concernaient la contestation « classique » d'opérations frauduleuses au moyen d'une carte de paiement volée ou perdue. La part du lion, soit 221 dossiers (18,5% du total), concernait la contestation des opérations à distance, c'est-à-dire la fraude sur Internet.

Vu le nombre croissant de cas de dossiers « fraude internet », ce rapport développe ci-après le raisonnement suivi[3] par Ombudsfin dans les cas concernés et notamment par rapport aux règles relatives à la répartition de la responsabilité pour les opérations de paiement non autorisées, comme le prévoit le livre VII du Code de Droit Economique.

Après l'explication juridique, suit une illustration de plusieurs types de fraudes fréquents (voir 2.9). Ensuite, quelques STOP-conseils sont donnés et pour conclure, suivent quelques recommandations aux consommateurs et au secteur (voir 2.10).



3 Compte tenu de la loi PSD II entrée en vigueur, le 9 août 2018, et de la Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les Directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le Règlement (UE) n° 1093/2010 et abrogeant la Directive 2007/64/CE, il existe à ce sujet une doctrine juridique très limitée.

2.8.1. Opérations de paiement autorisées

2.8.1.1. Distinction entre opérations de paiement autorisées et non autorisées[4]

Avant de pouvoir appliquer les règles relatives aux opérations de paiement non autorisées, il convient d'examiner si l'opération contestée peut être qualifiée d'autorisée ou non.

Le Code de Droit Economique prévoit qu'une opération de paiement n'est considérée comme autorisée que si le payeur a donné son consentement à l'exécution de l'ordre de paiement.[5] Sans le consentement (libre) du payeur, une opération de paiement est considérée comme non autorisée.

Pour Ombudsfin, on parle d'une opération de paiement autorisée uniquement si l'utilisateur y consent sciemment, c'est-à-dire si, au moment du paiement, il connaît le montant et le bénéficiaire ou le but de l'opération.

2.8.1.2. Charge de la preuve : l'opération est-elle autorisée ou non ?[6]

Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement exécutée ou affirme que l'opération de paiement n'a pas été correctement exécutée, le prestataire de services de paiement doit toujours fournir les quatre preuves suivantes:

- Preuve que l'opération de paiement a été authentifiée ;
- Preuve que l'opération de paiement a été dûment enregistrée ;
- Preuve que l'opération de paiement a été dûment comptabilisée ;
- Preuve que l'opération de paiement n'a pas été affectée par une déficience technique ou autre du service fourni par le prestataire de services de paiement.

En outre, la loi prévoit que l'utilisation d'un instrument de paiement telle qu'enregistrée par le prestataire de services de paiement, ne forme pas nécessairement la preuve suffisante du fait que l'opération de paiement a été autorisée par l'utilisateur de services de paiement ou que celui-ci a agi frauduleusement ou n'a pas satisfait intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent. Par conséquent, la fourniture par le prestataire de services de paiement des éléments de preuve susmentionnés n'implique pas automatiquement que l'opération contestée doit être considérée comme autorisée.

Une fois que le prestataire de services de paiement a fourni les preuves susmentionnées, l'utilisateur de services de paiement conserve le droit de rapporter de manière vraisemblable qu'il n'était pas conscient de l'opération qui a été autorisée. L'utilisateur de services de paiement n'est donc pas tenu de rapporter une preuve absolue. Ombudsfin est d'avis que, par le fait qu'un plaignant soit la victime d'un certain type de fraude[7] et qu'il soit en mesure de décrire en détail le mode opératoire du fraudeur, qu'il dépose plainte auprès de la police, et qu'il soumette une plainte à ce sujet à Ombudsfin, le plaignant, souvent sur la base de faits établis, rend vraisemblable le fait qu'il s'agit d'une opération de paiement non autorisée.

---

4 Les orientations de l'ABE concernant les exigences en matière de déclaration relatives à la fraude en vertu de l'article 96, paragraphe 6, de la Directive sur les services publics de télécommunications (PSD II) prévoient ce qui suit : " aux fins de la déclaration des données statistiques relatives à la fraude, conformément aux présentes orientations, le prestataire de services de paiement devrait prendre en compte, pour chaque période de déclaration : a.toute opération de paiement non autorisée effectuée, y compris à la suite de la perte, du vol ou de l'appropriation illicite de données de paiement sensibles ou d'un instrument de paiement, qu'elle soit détectable ou non par le payeur avant un paiement et résultant ou non d'une négligence grave du payeur ou exécutée en l'absence de consentement du payeur («opération de paiement non autorisée») ("opérations de paiement non autorisées")" ; voir https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2.

5 Art.VII.32 CDE.

6 Art.VII.42 CDE.

7 Cfr infra, 2.9. Focus sur Fraude - Scénarios de fraude et STOP-conseils.

2.8.1.3. Autorisation (consentir) ≠ authentification

Malgré la rédaction claire de la loi, Ombudsfin constate que diverses institutions financières assimilent l'autorisation (consentement) et l'authentification. Après avoir fourni les éléments de l'authentification, les institutions concernées affirment qu'il s'agit d'une opération de paiement autorisée et dès lors, qu'elles ne sont plus tenues de créditer[8] provisoirement le compte de paiement de la victime et considèrent qu'elles ne sont plus tenues de procéder à une analyse plus approfondie du dossier, par exemple d'apprécier l'existence d'une éventuelle négligence grave[9].

Ombudsfin relève que, dans ces dossiers, les institutions financières se raccrochent à leurs propres conditions générales bancaires. Ainsi, certains établissements financiers stipulent dans leurs conditions générales que si une opération est authentifiée selon la procédure convenue, ceci rapporte la preuve de l'identité du payeur et de son consentement à cette opération, sans préjudice de son droit d'apporter la preuve contraire. Bien que le payeur soit autorisé à apporter la preuve contraire, Ombudsfin constate souvent dans la pratique, que certaines institutions n'acceptent pas la preuve du contraire. En revanche, d'autres institutions financières vont plus loin en précisant, dans leurs conditions générales, que la banque ne peut être tenue responsable lorsqu'elle a fourni la preuve de l'authentification, de l'enregistrement correct, de la comptabilisation de la transaction et que l'opération de paiement n'a pas été affectée par une déficience technique ou autre défaillance des services offerts par le prestataire de services de paiement. Ici, le payeur n'a même pas la possibilité de fournir la preuve du contraire. Une telle disposition reprise dans les conditions générales est contraire à la loi et, par conséquent, nulle et non avenue.[10]

Certaines institutions financières invoquent également une disposition légale selon laquelle le consentement pour faire exécuter une opération de paiement ou une série d'opérations de paiement est donné sous la forme convenue entre le payeur et le prestataire de services de paiement et conformément à la procédure convenue.[11] Les institutions financières concernées font un usage fautif de cette disposition en déclarant que, si le fraudeur a respecté la procédure convenue (exemple : acheter sur internet au moyen du digipass, de la carte bancaire, introduire le code pin et générer des codes réponses), le titulaire de l'instrument de paiement a consenti à l'opération. Toutefois, cette disposition a pour seul but de prévoir que si le consentement est donné pour une opération, il ne peut l'être que conformément à la procédure convenue.

Une telle interprétation de la loi selon laquelle l'authentification équivaut à l'autorisation porterait atteinte presque totalement à la protection que le législateur européen et belge a voulu accorder au payeur.

8 Cfr infra, 2.8.2. Obligation de remboursement immédiat; art.VII.43 CDE
9 Cfr infra, 2.8.3.6. Négligence grave, fraude, et intention dans le chef du payeur; art.VII.44 CDE
10 Considérant 72 PSD II, art. VII.2, §4, al 2 CDE, art. VI.83, 21° CDE.

11 art.VII.32,§2 CDE.

2.8.2. Obligation de remboursement immédiat[12]

Le Code de Droit Economique prévoit qu'en cas d'opération de paiement non autorisée, le prestataire de services de paiement du payeur doit rembourser immédiatement au payeur le montant de l'opération de paiement non autorisée. Ce remboursement immédiat doit être effectué dès que le prestataire de services de paiement a eu connaissance de l'opération ou en a été informé. La loi prévoit que le remboursement doit être effectué au plus tard à la fin du premier jour ouvrable suivant.

L'obligation de remboursement immédiat susmentionnée ne s'applique pas si le prestataire de services de paiement a de bonnes raisons de soupçonner une fraude dans le chef du payeur et s'il communique ces raisons par écrit au SPF Économie. En conséquence, le prestataire de services de paiement a la possibilité d'effectuer une enquête à ce sujet dans un délai raisonnable, avant de rembourser le payeur.

Une fois qu'il est établi qu'il s'agit d'une opération de paiement non autorisée et qu'il n'existe aucune présomption de fraude dans le chef du payeur, le compte de paiement débité doit être remis dans son état initial, comme si l'opération de paiement non autorisée n'avait jamais eu lieu. La date valeur de ce crédit ne doit pas être postérieure à la date à laquelle le montant en question a été débité.

Ombudsfin constate que certaines institutions financières ne se conforment pas à cette obligation dans la pratique, du moins dans les cas traités par Ombudsfin. Sur la base, entre autre, de l'argument erroné selon lequel une opération authentifiée est également une opération autorisée, les institutions concernées estiment qu'elles ne sont pas tenues de rembourser immédiatement. Cette obligation de remboursement immédiat n'existe que dans le cas d'opérations non autorisées.

12 *art.VII.43 CDE.*

2.8.3. Répartition de la responsabilité[13]

2.8.3.1. Idée de base, telle qu'elle est reprise dans les travaux préparatoires de la loi du 19 juin 2019 modifiant et introduisant des dispositions relatives aux services de paiement dans différents livres du code du droit économique [14]

Le prestataire de services de paiement est tenu de mettre en place ou d'organiser au sein de son entreprise des structures permettant d'effectuer les opérations de paiement en toute sécurité. En principe, c'est donc le prestataire de services de paiement qui doit justifier en premier lieu du bon déroulement des opérations de paiement. On ne peut pas attendre du payeur moyen qu'il ait une connaissance complète de ce processus technique.

Dans les travaux préparatoires, il est expressément précisé qu'en cas de doute, cette règle doit être interprétée en faveur du payeur.

2.8.3.2. Contestation des opérations de paiement avant et après notification

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

2.8.3.2.1. Obligation de notification sans délai

L'utilisateur de services de paiement est tenu d'informer sans délai le prestataire de services de paiement ou l'entité désignée (la plupart du temps, Card Stop) par ce dernier de la perte, du vol, du détournement ou de l'utilisation non autorisée de l'instrument de paiement, dès qu'il l'a constaté.[15]

En outre, la loi prévoit que l'utilisateur de services de paiement ne pourra obtenir la rectification d'opération non autorisée que s'il notifie une telle opération au prestataire de services de paiement sans délai et au plus tard treize mois après la date-valeur du débit ou du crédit.[16] Cela signifie que l'utilisateur de services de paiement doit aviser

13 *Art.VII.44 CDE.*
14 *https://www.lachambre.be/FLWB/PDF/54/3131/54K3131001.pdf.*
15 *Art.VII.38 CDE.*
16 *Art.VII.41 CDE..*

son institution financière sans délai après la découverte de la fraude. Toutefois, s'il ne constate la fraude que 13 mois après le débit (ou plus tard), il ne pourra plus contester avec succès les opérations non autorisées à l'encontre de la banque en se fondant sur le livre VII du Code de Droit Economique. Et ce, pour autant que le prestataire de services de paiement ait rempli ses obligations légales en matière d'information, en particulier en fournissant en temps utile des informations exactes sur les opérations de paiement et le compte de paiement. Il est conseillé au payeur de vérifier, de manière régulière, ses extraits de compte et ses relevés de dépenses.

Ceci étant, Ombudsfin souligne que le prestataire de services de paiement est légalement tenu de veiller à ce que le payeur puisse effectuer cette notification à tout moment (24 heures sur 24, 7 jours sur 7)[17]. En outre, la loi prévoit que le payeur doit pouvoir effectuer cette notification gratuitement.[18] En pratique, le payeur n'a pas toujours la possibilité d'effectuer cette notification gratuitement.

En outre, Ombudsfin constate que l'entité désignée qui peut être jointe 24 heures sur 24 et 7 jours sur 7 n'est pas nécessairement celle qui peut prévenir d'autres fraudes (par exemple, dans le cas d'une installation frauduleuse d'une application mobile par le fraudeur).

2.8.3.2.2 Opérations de paiement non autorisées après notification

Le prestataire de services de paiement est tenu d'empêcher l'utilisation de l'instrument de paiement après la notification effectuée par le payeur.[19]

Le Code de Droit Economique prévoit expressément que l'utilisation de l'instrument de paiement perdu, volé ou détourné après la notification ne peut avoir de conséquences financières pour le payeur sauf si le prestataire de services de paiement prouve que ce dernier a agi frauduleusement. Par conséquent, le payeur ne peut jamais être tenu responsable des opérations qui ont eu lieu après la notification.

2.8.3.2.3. Opérations de paiement non autorisées avant la notification

En ce qui concerne la contestation des opérations de paiement non autorisées exécutées avant la notification, il convient de suivre les règles énoncées ci-après.

2.8.3.3 Authentification forte du client

2.8.3.3.1 Disposition légale

Lorsque le prestataire de services de paiement n'exige pas une authentification forte de la part du payeur, le payeur ne doit supporter aucune perte financière, sauf si le payeur lui-même a agi frauduleusement. Par conséquent, dans un tel cas, le payeur ne peut être tenu responsable de l'opération de paiement non autorisée.

L'authentification forte du client est définie par la loi comme "une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories "connaissance" (quelque chose que seul l'utilisateur connaît), "possession"(quelque chose que seul l'utilisateur possède) et "inhérence" (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification[20]. Dès que deux de ces facteurs sont combinés, on parle d'une authentification forte du client.

Ombudsfin constate que, depuis l'entrée en vigueur du Règlement délégué de la Commission du 27 novembre 2017 sur les normes techniques réglementaires relative à l'authentification forte des clients et les normes ouvertes, communes, et sécurisées de communication[21] presque toutes les opérations en ligne doivent être effectuées via une authentifiction forte (depuis le 14 septembre 2019[22]).

---

17 Art. VII.189 CDE prévoit que le prestataire de services de paiement reste responsable à l'égard de l'utilisateur de services de paiement, de toutes les conséquences résultant de l'usage d'un instrument de paiement par un tiers non autorisé en cas de non-respect par le prestataire de services de paiement de cette obligation.
18 Art.VII.39. 3° et 4° CDE.
19 Art.VII.39. 5° CDE.
20 Art.I.9.33/16° CDE.
21 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R0389&from=EN
22 L'ABE a prévu dans une Opinion du 16 octobre 2019 une "supervisory flexibility" jusqu'au 31 décembre 2020 ; voir https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment.

Le Règlement délégué prévoit un certain nombre de dérogations à l'authentification forte des clients. Parmi les exemples bien connus où une authentification forte des clients n'est pas requise, on peut citer, d'une part, les opérations de paiement électronique à distance d'un montant inférieur à 30 euros[23] pour lesquelles, par exemple, seuls le numéro de carte, la date d'expiration et le code CVV sont demandés et, d'autre part, les paiements sans contact d'un montant inférieur à 50 euros pour lesquels aucun code PIN n'est requis[24].

2.8.3.3.2 Application : installation frauduleuse d'une application mobile

Dans les différents types de fraude sur Internet, il est toujours possible pour un fraudeur de télécharger frauduleusement une application de la banque, liée à l'abonnement internet de la victime, sur son propre téléphone mobile. Après avoir intercepté les données ordinaires bancaires (comme le numéro de carte et le numéro de digipass), et également les codes générés avec le digipass, ou après que la victime les ait communiqués d'une manière ou d'une autre (consciemment ou non) à l'auteur de la fraude, ce dernier réussit à installer l'application liée au compte de la victime sur son propre téléphone mobile. L'installation de l'application se déroule donc bien avec l'authentification forte du client, mais sur le téléphone mobile du fraudeur.

Après l'installation de l'application mobile, le fraudeur choisit lui-même un code d'accès d'un certain nombre de chiffres. Ce code est donc connu du seul fraudeur et utilisable sur son seul téléphone. Ce code donne accès à l'application installée sur le téléphone mobile du fraudeur et est ensuite utilisé sans intervention de la victime pour effectuer des paiements via cette application mobile. La victime ne connaît donc pas ce code.

Après avoir téléchargé et installé l'application, le fraudeur reçoit l'accès aux comptes de sa victime. Grâce à l'application, il peut souvent adapter les limites applicables. Les applications de plusieurs banques permettent également d'effectuer des paiements en ligne simplement en scannant un code QR. Ombudsfin relève que le dommage dans ces dossiers peut souvent être très élevé. Une fois l'application installée, le fraudeur peut effectuer des transferts et des paiements à sa guise, jusqu'à épuisement des limites applicables.

Ombudsfin doute que pour les opérations de paiement que le fraudeur exécute après l'installation d'une application, il soit satisfait aux conditions d'authentification forte du client. En effet, le fraudeur utilise, pour l'initiation et la confirmation des transactions, une application installée sur son propre téléphone portable, qui n'a donc jamais été en possession de la victime, et un code créé par lui-même, qui n'est donc pas connu de la victime.

En marge, on peut mentionner que, dans de tels cas, Ombudsfin souligne toujours que l'installation d'une application mobile ne devrait pas se faire avec la même facilité que la confirmation d'une opération de paiement. Conformément au Règlement délégué relative à l'authentification forte des clients, le logiciel d'authentification doit d'abord être activé avant de pouvoir être utilisé.[25] Par conséquent, selon Ombudsfin, une application mobile ne pourrait être activée par la banque qu'après une action spécifique supplémentaire de son client, en s'assurant que c'est son client lui-même qui demande l'activation de l'application. Dans ce contexte, il peut également être fait référence à l'obligation de la banque, déjà évoquée, de mettre en place ou d'organiser des structures permettant d'effectuer les opérations de paiement en toute sécurité.

2.8.3.4 Règle de base : responsabilité du prestataire de services après la déduction d'une franchise de 50 euros

En ce qui concerne la répartition de la responsabilité en cas d'opérations de paiement non autorisées avant la notification et sans une authentification forte du client, la loi prévoit la règle de base suivante : en principe, le risque incombe au prestataire de services de paiement. Fondamentalement, le prestataire de services de paiement devrait supporter la perte.

23 Article 16 du Règlement délégué «Authentification forte»
24 Article 11 du Règlement délégué «Authentification forte»

25 Article 25 du Règlement délégué «Authentification forte».

La loi prévoit que jusqu'à la notification, le payeur ne doit supporter la perte qu'à concurrence d'un montant maximum de 50 euros pour toutes les opérations de paiement non autorisées résultant de l'utilisation d'un instrument de paiement perdu ou volé ou du détournement d'un instrument de paiement. Le payeur ne supporte donc ici qu'un risque limité, à savoir une franchise de 50 euros.

Cette règle de base ne s'applique que si aucun des cas évoqués aux points 2.8.3.5 et 2.8.3.6 n'est applicable.

2.8.3.5. Il n'est pas possible de détecter la fraude à l'avance

2.8.3.5.1 Disposition légale et application

Le Code de Droit Economique prévoit que le payeur ne doit supporter aucune perte jusqu'à la notification, et donc aussi aucune franchise de 50 euros si la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf si le payeur lui-même a agi frauduleusement. Cela signifie que si la victime d'une fraude n'a pas pu détecter à l'avance le détournement de son instrument de paiement, elle ne peut être tenue responsable de cette fraude.

Les travaux préparatoires de la loi[26] indiquent que cet article peut être appliqué, par exemple, dans les cas de piratage et d'hameçonnage (phishing) de données personnelles de sécurité ou de skimming de cartes. Il est en outre précisé que le "détournement" couvre également, par exemple, les cas où les données de paiement ont été volées alors que le payeur est toujours en possession de son instrument de paiement (par exemple, en cas de phishing ou de clonage de l'instrument de paiement).

La question de la possibilité d'une détection préalable d'un cas de fraude doit être appréciée en tenant compte de l'ensemble des faits. Il n'est donc pas exact qu'une victime d'hameçonnage, par exemple, peut automatiquement invoquer cette disposition de la loi et n'aura donc aucune perte à supporter. Compte tenu des circonstances spécifiques, il conviendra tout d'abord de déterminer si la disposition en question est applicable ou non. Si cette disposition ne devait pas s'appliquer, il y a lieu d'appliquer la règle de base et d'apprécier l'existence d'une éventuelle négligence grave[27].

2.8.3.5.2 Indépendamment d'une négligence grave

Sous 2.8.3.6, vous pouvez lire qu'il existe une exception à la règle de base pour les cas où il y a négligence grave dans le chef du payeur. En effet, la loi prévoit que le payeur doit supporter toutes les pertes liées aux opérations de paiement non autorisées si ces pertes résultent du fait qu'il n'a pas rempli certaines obligations à la suite d'une négligence grave.

Selon la doctrine juridique limitée disponible aujourd'hui, l'existence ou non d'une négligence grave dans le chef de la victime de la fraude n'est pas pertinente dans l'hypothèse où le payeur ne pouvait pas détecter la fraude au préalable. Cela signifie que lorsque l'article pertinent de la loi s'applique (article VII.44§1er alinéa 2 CDE), le payeur ne supportera aucune perte, même s'il a commis une négligence grave. Cette interprétation se déduit expressément du texte juridique, puisque la loi ne prévoit pas, dans cette hypothèse, d'exception explicite pour la négligence grave. Une autre interprétation viderait complètement de sens le contenu de cette disposition.

Ombudsfin constate que la manière dont l'article en question est rédigé dans la loi (ordre des différentes hypothèses) laisse malheureusement, dans la pratique, une marge d'interprétation et d'application différentes. Ainsi, Ombudsfin constate que les institutions financières n'appliquent pas l'alinéa adéquat de cet article de la loi si elles estiment que le client a été gravement négligent. En effet, elles estiment que la négligence grave peut s'appliquer comme une exception générale à toutes les dispositions concernant la répartition de la responsabilité. Ombudsfin estime que soit la jurisprudence devra apporter plus de clarté, soit la loi devra être révisée, soit les autorités de contrôle devront élaborer des directives d'interprétation supplémentaires. En tout état de cause, une telle application de la loi n'est pas conforme au principe déjà mentionné selon lequel, en cas de doute, la règlementation doit être interprétée en faveur du payeur.

26 https://www.lachambre.be/FLWB/PDF/54/3131/54K3131001.pdf.

27 *Cfr infra, 2.8.3.6. Négligence grave, fraude ou intention dans le chef du payeur ; art. VII.44 CDE.*

2.8.3.5.3 Application : installation frauduleuse d'une application mobile

Comme expliqué plus haut, dans de nombreux cas, les fraudeurs réussissent à installer frauduleusement une application mobile bancaire sur leur propre téléphone mobile, ce qui leur permet d'accéder aux comptes de la victime de la fraude.[28] En fonction de la manière et des circonstances dans lesquelles le fraudeur a intercepté les données de sécurité personnalisées bancaires personnelles de sa victime, la victime peut, le cas échéant, invoquer l'article de la loi selon lequel elle ne doit supporter aucune perte si elle n'était pas en mesure de détecter préalablement la fraude.

Nous avons déjà mentionné que, selon Ombudsfin, une application ne devrait être activée par la banque qu'après une action spécifique supplémentaire de la part du client, s'assurant que c'est le client lui-même qui demande l'activation de l'application. A cet effet, la banque pourrait, par exemple, envoyer un sms ou un e-mail avec un lien d'activation vers les coordonnées de contact du client connues de la banque. Ainsi, la victime serait toujours en mesure de détecter le détournement de son instrument de paiement avant les opérations de paiement non autorisées. Sans intervention active de la victime, le fraudeur ne serait pas en mesure d'effectuer des opérations via une telle application dans un tel cas.

Ombudsfin est d'avis qu'un mail ou un sms avec la simple communication indiquant qu'une nouvelle application a été installée et expliquant comment l'application en question peut être supprimée à nouveau, n'est pas suffisant.

2.8.3.6 Négligence grave, fraude et intention dans le chef du payeur

Si l'hypothèse évoquée sous 2.8.3.5 ne trouve à s'appliquer, il convient, alors, d'invoquer la règle de base. Comme indiqué précédemment, la règle de base prévoit une exception dans les cas de négligence grave dans le chef du payeur.

Si le payeur a subi des pertes à la suite d'opérations de paiement non autorisées du fait d'avoir agi frauduleusement ou de ne pas avoir respecté certaines obligations, que ce soit intentionnellement ou à la suite d'une négligence grave, contrairement à ce qui est prévu par la règle de base, il doit supporter toutes les pertes.

2.8.3.6.1 Appréciation de la négligence grave

Le Code de Droit Economique précise clairement les obligations auxquelles le payeur ne peut se soustraire à la suite d'une négligence grave afin d'éviter de devoir supporter toutes les pertes résultant d'opérations de paiement non autorisées :

- Le payeur doit utiliser l'instrument de paiement conformément aux conditions régissant l'émission et l'utilisation de l'instrument de paiement. Les conditions concernées sont fixées dans le contrat. Ces conditions doivent être objectives, non discriminatoires et proportionnées. Les travaux préparatoires de la loi[29] précisent que ces dernières concernent en particulier les dispositions relatives à la conservation des instruments de paiement et des données relatives à la sécurité des personnes.
- Le payeur est tenu d'informer sans délai le prestataire de services de paiement ou l'entité désignée dès qu'il a connaissance de la perte, du vol ou de toute utilisation non autorisée de son instrument de paiement.
- Afin de se conformer à ces obligations, l'utilisateur de services de paiement prend toutes les mesures raisonnables afin de préserver la sécurité de l'instrument de paiement et de ses données de sécurité personnalisées. Et ce, dès qu'il a reçu l'instrument de paiement.

28 Cfr supra, 2.8.3.3.2. Application : installation frauduleuse d'un application mobile.

29 https://www.lachambre.be/FLWB/PDF/54/3131/54K3131001.pdf.

Si, à la suite d'une négligence grave, le payeur ne respecte pas une ou plusieurs des obligations susmentionnées, il supportera intégralement la perte subie occasionnée par les opérations de paiement non autorisées.

Le Code de Droit Economique fournit également des explications supplémentaires à propos de la notion de "négligence grave". Ainsi, la loi prévoit que, pour l'appréciation de la négligence, il doit être tenu compte de l'ensemble des circonstances de fait.

En outre, la loi prévoit que sont notamment considérées comme négligences graves, les comportements suivants :

- Le fait, pour le payeur, de noter ses données de sécurité personnalisées, telles que son numéro d'identification personnel ou tout autre code, sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement ou sur un objet ou document que le payeur conserve ou emporte avec lui avec l'instrument de paiement.
- le fait pour le payeur de ne pas avoir notifié au prestataire de services de paiement, ou à l'entité désignée par celui-ci, la perte ou le vol de l'instrument de paiement.

Il convient d'établir une distinction entre la négligence et la négligence grave. Les considérants de la Directive PSD II précisent expressément que la négligence grave devrait impliquer plus que de la simple négligence. Le comportement en question doit comporter un défaut de vigilance caractérisé.

2.8.3.6.2 Charge de la preuve

Le Code de Droit Economique prévoit que la charge de la preuve en matière de fraude, d'intention ou de négligence grave incombe au prestataire de services de paiement. Par ailleurs, la loi précise que l'utilisation du moyen de paiement avec le code connu du seul utilisateur de services de paiement ne constitue pas une présomption suffisante de la négligence dans le chef de ce dernier. Comme mentionné ci-avant, la loi prévoit que l'utilisation d'un instrument de paiement, telle qu'enregistrée par le prestataire de services de paiement, ne suffit pas nécessairement en tant que telle à prouver que l'opération de paiement a été autorisée par le payeur ou que ce dernier a agi frauduleusement ou n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent.[30] En outre, depuis le 9 août 2018, le prestataire de services de paiement doit fournir des preuves à l'appui afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement.[31]

30 Cfr supra, 2.8.1.2. Charge de la preuve: l'opération est-elle autorisée ou non?
31 Art.VII.42 CDE.

2.9. FOCUS SUR LES FRAUDES - SCÉNARIOS DE FRAUDE ET STOP-CONSEILS

2.9.1. Microsoft

2.9.2 2EMEMAIN.BE

Kim met un aspirateur en vente sur 2ememain.be pour 150 EUR et est immédiatement contactée par un acheteur intéressé John.

John envoie un message à Kim:

je voudrais acheter votre aspirateur pour 150 EUR, ou même 175 EUR. Pour l'encaissement et le paiement, je préfère travailler par l'intermédiaire du service de colis. J'effectue le paiement immédiatement. Vous recevrez un e-mail du service de colis afin de pouvoir recevoir le paiement.

Kim est devenu victime du phishing dans une première phase et du vishing dans une seconde phase.

Kim est enthousiaste parce qu'elle a trouvé si rapidement un acheteur qui veut donner le prix ou même plus. Elle trouve l'intervention du service de colis un peu bizarre, mais continue quand même. Elle reçoit un e-mail du service de colis.

Le service de colis dispose maintenant, grâce aux coordonnées bancaires introduites via le lien et aux codes de réponse transmis, de suffisamment de données pour effectuer des paiements à partir du compte de Kim.

le service de colis envoie :

un paiement vous attend. Pour recevoir le paiement, vous devez créer un compte.

Veuillez remplir vos coordonnées via le lien afin que nous puissions créer un compte à votre nom.

Kim suit les instructions données par le service de colis.

Pour finaliser la création du compte, vous devez effectuer quelques actions supplémentaires avec votre digipass. Nous vous donnons les chiffres que vous devez entrer dans votre digipass et vous nous donnez les chiffres qui apparaissent sur votre digipass.

Kim clique sur le lien et remplit les données bancaires (données du compte et de la carte de paiement) ainsi que les données personnelles. Après avoir rempli les données, Kim est appelée par le service de colis.

CODE

WARNING!

CONSEILS

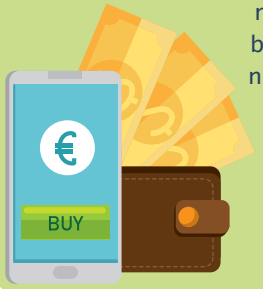
- **Ne vendez rien sur un site 2ememain à un acheteur qui souhaite organiser la livraison et le paiement via Fedex, DPD, UPS ou tout autre service de colis.**
- **Ne vendez rien non plus à un acheteur qui veut vérifier votre fiabilité en utilisant votre digipass.**
- **Un acheteur sur 2ememain qui veut immédiatement offrir plus que le prix devrait éveiller vos soupçons.**

2.9.3. Remplacement lecteur de carte/ digipass

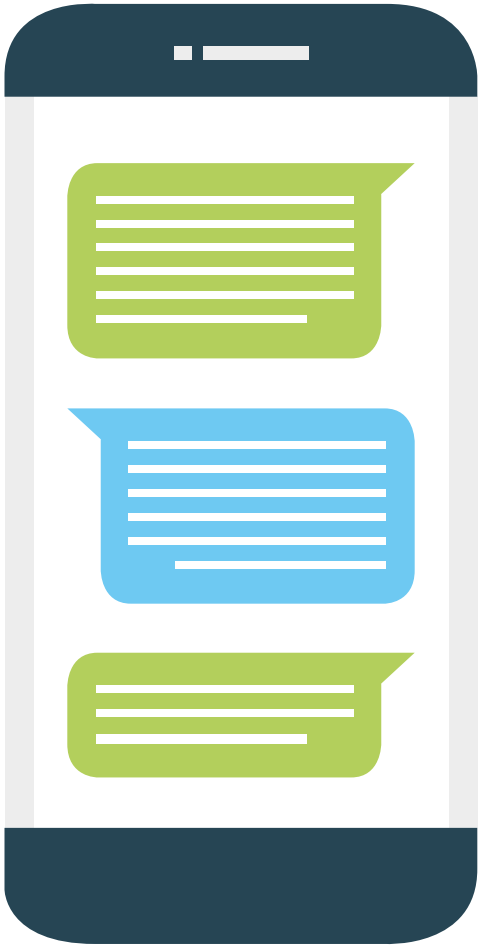
Bob reçoit un SMS de la banque l'invitant à remplacer son lecteur de carte. Bob peut immédiatement faire le nécessaire en suivant un lien.

Bob est étonné de recevoir un SMS parce que la banque ne connaît pas son numéro de téléphone portable, mais clique quand même sur le lien de peur de ne plus pouvoir effectuer ses opérations bancaires en ligne s'il ne suit pas les instructions.

Ce qu'il ne réalise pas, c'est qu'il s'agit d'un faux site web et que ses données sont interceptées en arrière plan par un fraudeur. Le fraudeur réussit à installer sur son propre téléphone portable une application de banque mobile, liée aux comptes de Bob, sur base des données récupérées.



Le fraudeur est ensuite en mesure d'utiliser l'application de banque mobile pour effectuer de nombreuses transactions à partir de différents comptes.



Bob est devenu victime du phishing, avec des conséquences très importantes (suite à l'installation de l'application de banque mobile).

Bob suit le lien et se retrouve sur la plateforme de banque en ligne de la banque - ou du moins c'est ce qu'il pense.

Il remplit les données demandées sur son lecteur de carte et utilise son lecteur de carte pour générer un ou plusieurs codes, comme demandé à l'écran.

Conseils:

- Supprimez immédiatement les e-mails ou SMS reçus d'une banque dont vous n'êtes pas client.
- Ne réagissez jamais aux demandes de renouvellement de cartes bancaires, de lecteurs de cartes, de mise à jour de données, etc. par e-mail ou par SMS. Effacez immédiatement le message et/ou contactez votre banque.
- Lorsque vous recevez un message concernant une domiciliation établie, ne suivez jamais un lien dans ce message pour le contester.

2.9.4. Facture payée en double

Kim reçoit un SMS de son fournisseur l'informant qu'elle a payé deux fois une facture. Si elle suit un lien, elle peut remplir quelques données bancaires pour recevoir 1 paiement en retour.

Kim ne se souvient pas d'avoir payé une facture deux fois, mais ne vérifie rien, suit le lien et remplit les données détaillées.

Ensuite, Kim reçoit un appel téléphonique de son fournisseur, John.

John: Merci de remplir vos données pour le remboursement de ce montant. Cependant, je vois ici que, malheureusement, quelque chose a mal tourné. Allons-nous suivre la procédure ensemble ? Prenez votre carte et votre digipass.

Kim: : D'accord. Nous allons le faire ensemble.

John donne des instructions à Kim pour qu'elle sache quoi insérer dans son digipass.

John: Vous y arrivez ? Vous pouvez me donner les chiffres qui figurent sur votre digipass.

Kim: OK.
Voici les chiffres 123 456.

John: Merci. Oups, je reçois un autre message d'erreur. Il faut que nous le fassions à nouveau. Alors tout se passera bien.

Kim trouve un peu bizarre que cela n'ait pas fonctionné, mais elle accepte de réessayer. Elle suit à nouveau les instructions et transmet le code obtenu à John.

John: Merci. Oups, on a été trop vite. Nous allons encore une fois recommencer. Vous pouvez éventuellement essayer une autre carte?

Kim accepte d'essayer une autre carte et transmet le code reçu du digipass à John.

John: Ok, maintenant cela semble correct. Vous verrez bientôt le montant apparaître sur vos comptes. Passez une bonne journée.

Ensuite, Kim vérifie ses comptes et constate que plusieurs montants ont disparu de ses comptes. Elle n'a reçu aucun montant. La facture payée en double était une astuce d'un fraudeur.

Elle est devenu victime de phishing dans une première phase et de vishing dans une seconde.

Conseils:

- **Pour recevoir un paiement, l'utilisation d'un digipass n'est jamais nécessaire ! Si quelqu'un vous demande quand même, arrêtez immédiatement vos actions ou la communication.**
- **Lorsque vous recevez un e-mail ou un sms de votre fournisseur ou d'une agence gouvernementale concernant une facture doublement payée ou impayée, ne suivez jamais un lien ou n'utilisez jamais votre digipass.**

2.9.5. Mules

Kim 16 ans, est approchée via Facebook par une personne John qui influence Kim pour lui faire gagner de l'argent rapidement et sans trop d'efforts. La seule chose que Kim doit faire, c'est donner son numéro de compte, sa carte bancaire et son code pin à John. Ceci serait suivi par le paiement du "salaire" promis.".

Kim y va ; elle aimerait bien ce petit supplément d'argent.

Une fois que John a la carte en main, il dissimule frauduleusement de l'argent sur le compte du mineur. Soit il continue à transférer des montants à partir de ce compte, soit il retire les montants en espèces avec la carte bancaire du mineur.

ALERT!

CONSEILS

Si vous êtes approché par une tierce personne sur Facebook/Instagram, à la porte de l'école ou à l'endroit de votre hobby qui vous promet de l'argent supplémentaire en échange de vos coordonnées bancaires et de votre carte bancaire, arrêtez immédiatement la conversation. Ne répondez pas à cette question. Si vous coopérez, vous pouvez vous rendre coupable d'infractions pénales.

2.10. FOCUS SUR FRAUDE - RECOMMANDATIONS GÉNÉRALES AUX CONSOMMATEURS ET AU SECTEUR

Recommandations générales anti-fraude aux consommateurs:

- Consultez régulièrement le site safeonweb.be. Vous y trouverez de nombreux conseils et avertissements utiles sur toutes les pratiques de fraude connues sur Internet.
- Vérifiez toujours l'adresse électronique complète ou l'URL complet d'un site web. La moindre erreur d'écriture ou l'utilisation de noms de domaine ou d'adresses électroniques atypiques sont le signe d'une fraude.

Au moindre doute, arrêtez vos actions ou communications et faites les vérifications nécessaires par des recherches supplémentaires.

- Quand quelque chose semble trop beau pour être vrai, alors c'est probablement trop beau pour être vrai et c'est donc une fraude. Ne vous laissez pas séduire et arrêtez la communication ou les actions.
- Lorsque vous utilisez votre digipass, vous effectuez par définition une action ou une transaction sur votre compte.
- Grâce à des codes (créés par votre digipass), un fraudeur à distance peut effectuer des paiements, effectuer des virements via votre homebanking ou même installer votre application bancaire sur son smartphone personnel. Ne communiquez donc jamais les codes créés par votre digipass à un tiers.
- N'utilisez jamais votre digipass lorsque vous devez recevoir un paiement. Vous n'aurez jamais besoin d'un digipass pour cela.
- Les touches et le texte de votre digipass vous en disent déjà beaucoup sur les actions que vous entreprenez. Les boutons disent "Acheter", "Signer", "Identifier", "M1 = Identifier = Appli 1", "M2 = Signer = Appli 2" pour une raison. Soyez conscient de ce que vous faites et lisez également le texte qui peut apparaître sur votre digipass.

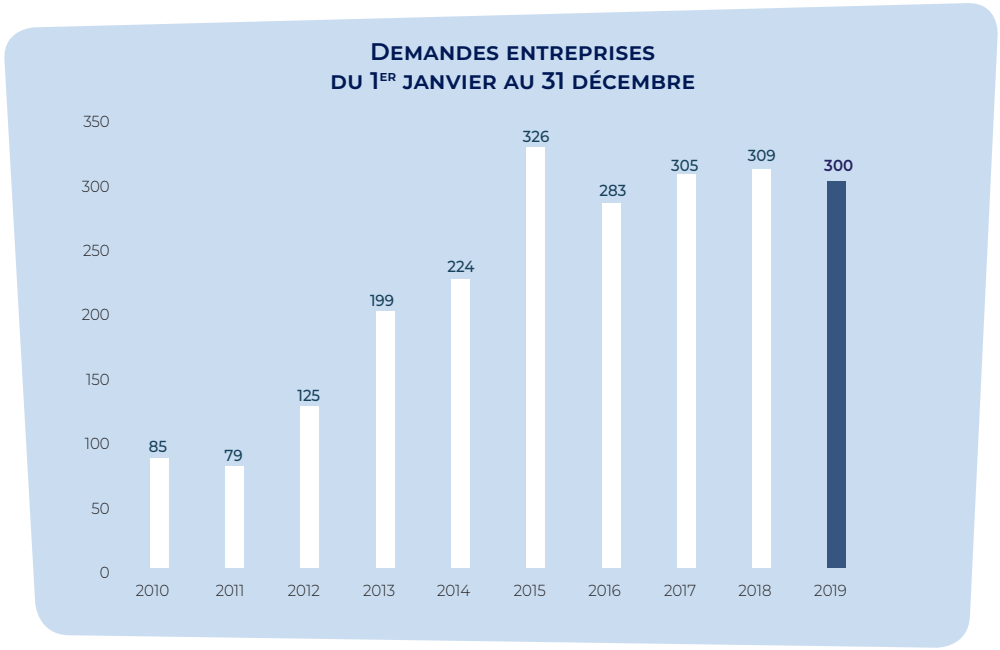
Recommandations générales anti-fraude au secteur:

- Prévoir des procédures de notification, de blocage et de recouvrement adaptées à la vitesse à laquelle les opérations sont actuellement effectuées.
- Après un constat de fraude, prenez immédiatement les mesures nécessaires pour essayer de récupérer les fonds..
- Mettre en place des systèmes de contrôle adéquats pour intercepter et arrêter les transactions frauduleuses.
- Prévoir une action supplémentaire du client pour activer l'application, comme une étape supplémentaire après l'installation de l'application mobile banking.
- Expliquer aux clients comment fonctionne le mécanisme de paiement et quel est l'impact de l'utilisation du digipass.

3. DEMANDES INTRODUITES PAR LES ENTREPRISES

3.1. LÉGÈRE DIMINUTION DU NOMBRE DE DEMANDES

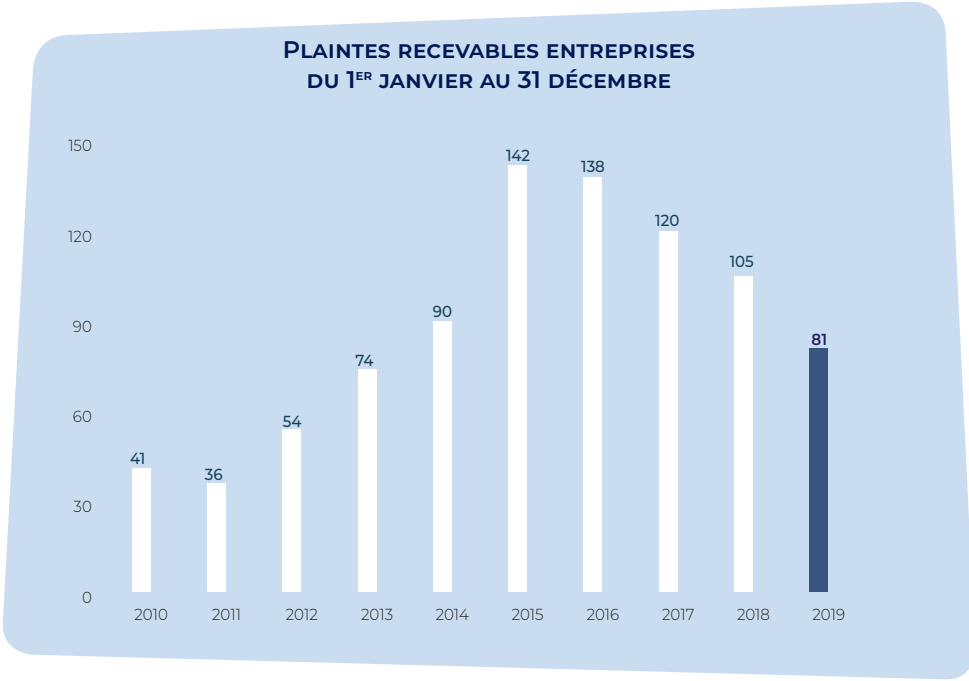
Au total, Ombudsfin a reçu 300 demandes écrites d'entreprises en 2019, contre 309 demandes en 2018. Cela représente une diminution de 9 dossiers ou 2,9%.



299 demandes étaient des plaintes, 1 demande était une simple demande d'information.

3.2. LA DIMINUTION DU NOMBRE DE PLAINTES RECEVABLES SE POURSUIT

En 2019, Ombudsfin a enregistré 81 demandes d'entreprises comme étant recevables, contre 105 demandes en 2018. Ceci représente une diminution de 24 dossiers ou 22,9%.

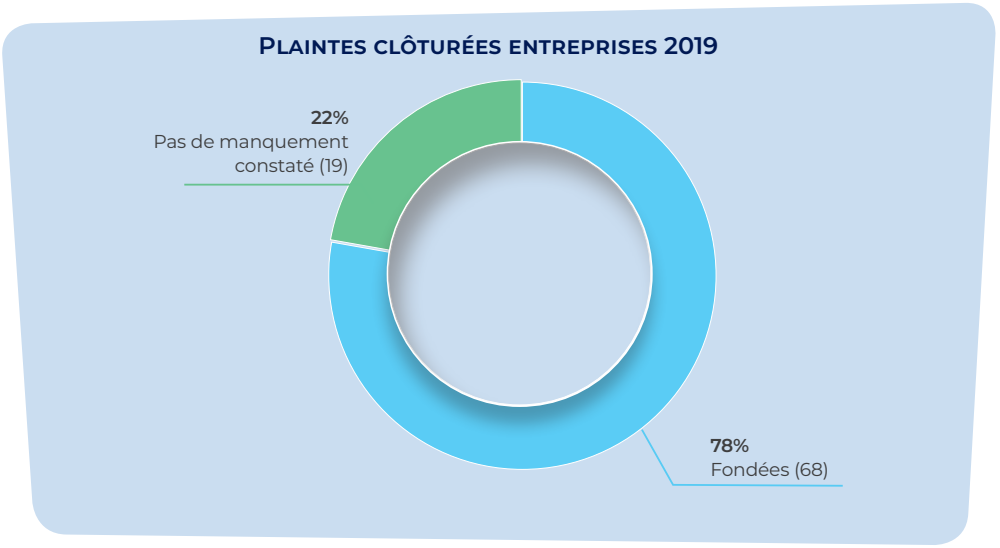


3.3. RÉSULTATS DES PLAINTES VENANT D'ENTREPRISES ET CLÔTURÉES EN 2019 : AUGMENTATION DU NOMBRE DE DOSSIERS RÉSOLUS !

Les résultats analysés ci-après se rapportent à toutes les plaintes venant d'entreprises et ayant été traitées et clôturées en 2019. Certaines plaintes introduites en 2018 chez Ombudsfin sont donc également incluses dans ces résultats, mais elles n'ont été traitées et clôturées qu'en 2019.
Au total, il s'agit de 87 dossiers.

Pour 68 dossiers (soit 78,5%), Ombudsfin a considéré la plainte comme fondée (c'est-à-dire sujette à négociation) sur la base de la législation, des dispositions contractuelles, des codes de conduite ou des pratiques du marché.

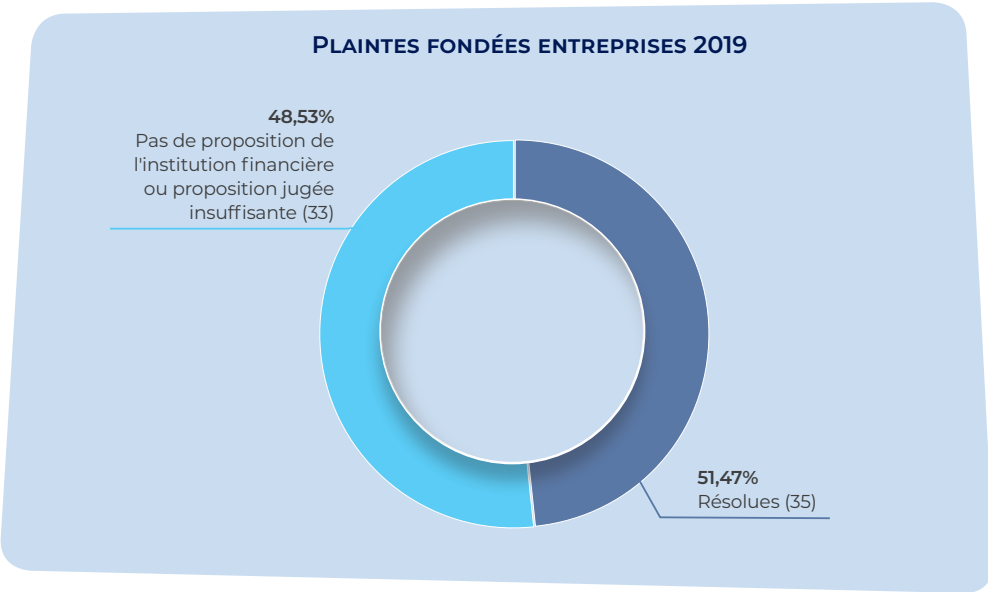
Pour 19 dossiers (soit 21,8%), Ombudsfin n'a pas pu établir de manquement dans le chef de l'institution financière. Dans ces dossiers, les explications adéquates ont été transmises à l'entreprise afin qu'elle comprenne pourquoi Ombudsfin est arrivé à cette conclusion et pourquoi il ne pouvait être demandé d'indemnisation ou de rectification de la part de l'institution financière.



Pour les 68 dossiers (78,2%) considérés comme fondés, Ombudsfin a poursuivi les négociations. 35 dossiers (soit 51,5% des plaintes fondées) ont abouti à une solution à l'amiable. À l'inverse, 33 dossiers (48,5%) n'ont pas trouvé de solution.

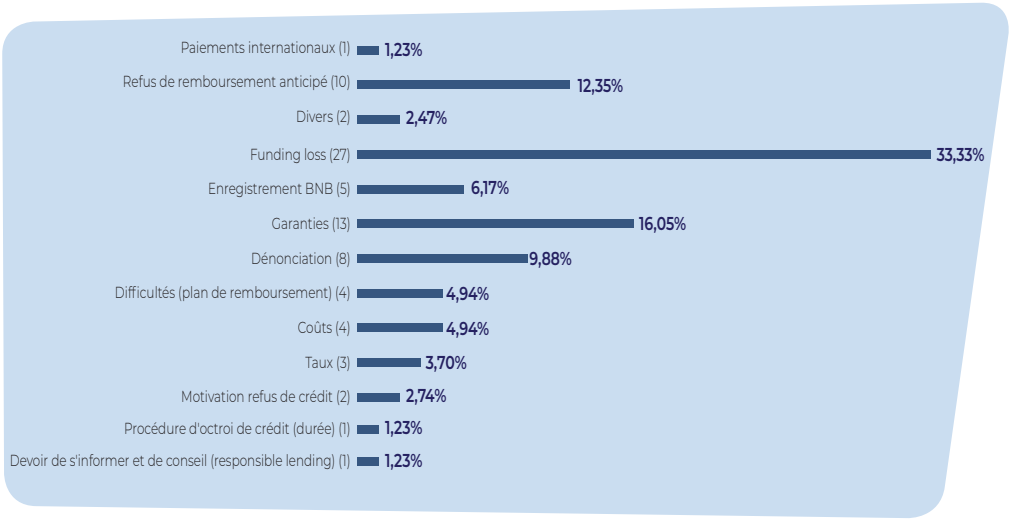
Cela représente une augmentation du nombre de dossiers résolus par rapport à 2018 ! Ceci est une évolution positive.

Comme les années précédentes, en 2019, la majorité des plaintes portait sur la problématique du remboursement anticipé et celle du *funding loss*. L'analyse d'Ombudsfin des conventions de crédit diffère de la vision des banques. En 2019, il a été possible de parvenir à un accord entre les parties dans un plus grand nombre de cas.



3.4. THÈMES DES PLAINTES RECEVABLES DES ENTREPRISES

En 2019, les plaintes étaient réparties, par thème, de la façon suivante :



La plupart des dossiers recevables étaient liés au *funding loss* : 27 dossiers (soit 33,33%) sur les 81 dossiers recevables.

Cependant, il convient aussi d'ajouter les dossiers ayant pour thème le « remboursement anticipé non autorisé », étant donné qu'il s'agit de la même problématique, à savoir le remboursement anticipé d'un crédit professionnel. Il est question ici de 10 dossiers (12,35 %). On totalise donc ici 37 dossiers (45,68%).

Par rapport à 2018, le nombre de dossiers relatifs à ces 2 thèmes a presque diminué de moitié : 37 dossiers contre 67 en 2018. Une explication pourrait être que les banques négocient davantage avec les emprunteurs afin de parvenir à une solution.

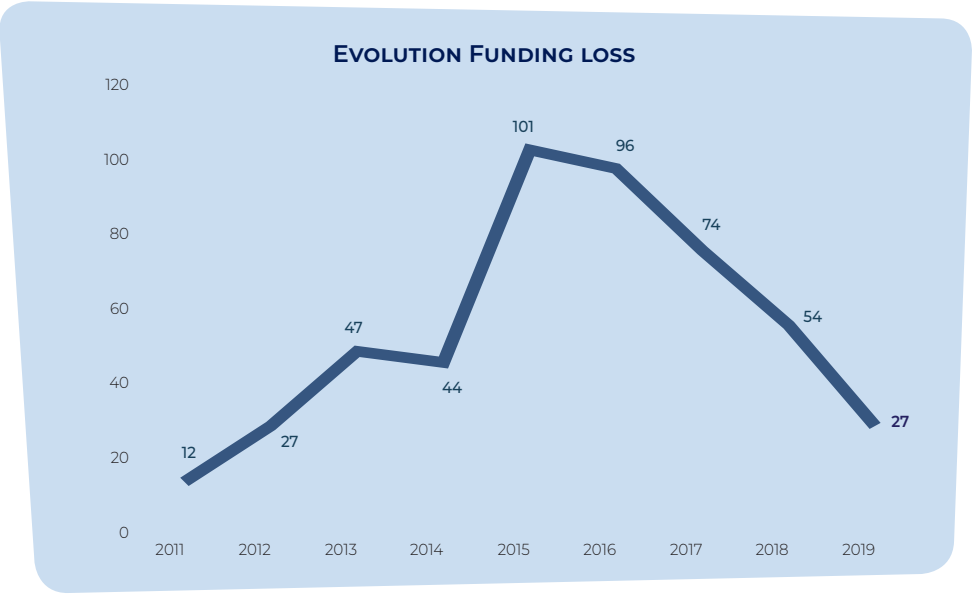
Le nombre de plaintes concernant le *funding loss* est en baisse depuis environ trois ans. La tendance à la baisse se poursuit en 2019. Néanmoins, cela reste le thème le plus important des plaintes des entreprises.

Un autre thème plus vaste reste celui des garanties.

> « Le nombre de plaintes concernant le *funding loss* a diminué de moitié. »

Diminution importante des plaintes sur le *funding loss*

Le graphique ci-dessous indique l'évolution du nombre de plaintes en rapport avec le *funding loss* soumises à Ombudsfin. En 2019, il y a eu à nouveau une diminution du nombre de dossiers pour ce thème.



Les résultats des dossiers traités sur les thèmes de *funding loss* et du remboursement anticipé non autorisé.

En 2019, 33 dossiers relatifs au *funding loss* ont été traités et clôturés par Ombudsfin. De ces dossiers, 1 n'était pas fondé. 32 dossiers ont été considérés par Ombudsfin comme étant fondés.

Dans 6 des 32 dossiers fondés (19%), un accord à l'amiable a été conclu, mais dans 26 dossiers (soit 81%), il n'y a pas eu de proposition de la banque pour limiter le funding loss, ou une proposition a été jugée insuffisante par l'entrepreneur.

En ce qui concerne les dossiers relatifs au remboursement anticipé non autorisé, les résultats sont pareils : sur les 10 dossiers traités, 2 ont été résolus et les 8 autres ne l'ont pas été.

Conclusion :

Il existe une évolution claire dans le nombre de plaintes relatives à ce sujet. Celui-ci est retombé en 2019 à environ la moitié du nombre de dossiers en 2018. Toutefois, les résultats des plaintes traitées sont toujours en ligne avec la tendance précédente : dans la grande majorité des dossiers traités, aucun accord à l'amiable n'a pu être trouvé entre les parties.

Analyse d'un certain nombre de thèmes

1-Funding loss

Le *funding loss* correspond à l'indemnité de remploi demandée à l'emprunteur en cas de remboursement anticipé d'un crédit d'investissement. Le *funding loss* est la différence actualisée entre la somme de tous les intérêts prévus contractuellement qui auraient dû être payés jusqu'à la fin normale du crédit et les intérêts créditeurs sur le montant du remboursement anticipé calculés généralement à un taux d'intérêt interbancaire, majoré ou diminué d'une marge. Vu le taux d'intérêt interbancaire très bas ces dernières années, le montant du funding loss peut être très élevé.

Aussi en 2019, la plupart des plaintes concernaient le problème du remboursement anticipé d'un prêt d'investissement et /ou l'imputation d'un *funding loss*.

La discussion juridique concernant le *funding loss* qui traîne depuis des années concerne l'application de l'article 1907bis du Code civil (BW). Cet article stipule qu'en cas de remboursement anticipé d'un prêt à intérêt, il n'est pas permis de réclamer une indemnité de remploi d'un montant supérieur à 6 mois. Selon les institutions financières, les crédits d'investissement professionnels ne peuvent être considérés comme des prêts, mais sont des ouvertures de crédit auxquelles l'article précité ne s'applique pas.

La jurisprudence actuelle confirme que les crédits d'investissement peuvent être qualifiés comme des prêts sur intérêts lorsqu'elles présentent les caractéristiques d'un prêt. Une caractéristique importante pour qualifier un crédit comme un prêt est le "manque de liberté" laissée à l'emprunteur. À cet égard, la liberté de prélever les fonds et de rembourser le capital est principalement prise en considération.

Dans le cas d'un prêt d'investissement, les fonds doivent souvent être prélevés au cours d'une période de prélèvement limitée. Une période standard est souvent de 9 mois, mais la période prévue peut également être plus courte ou plus longue en cas de travaux de construction ou de rénovation d'une propriété. Les fonds ne peuvent être utilisés que pour l'objectif déclaré du crédit.

L'emprunteur doit rembourser le capital et les intérêts par des paiements périodiques conformément à un tableau de remboursement établi par la banque.

Dans toutes ces situations, les juges ont tendance à qualifier les crédits comme des "prêts", vu le manque de liberté de l'emprunteur. Dans ce cas, l'article 1907bis du code civil peut s'appliquer.

En 2019, le nombre de plaintes concernant le *funding loss* a fortement diminué.

Dans plusieurs banques, les conditions de crédit prévoient que le remboursement anticipé n'est pas autorisé. Pendant de nombreuses années, ces banques n'ont pas invoqué cette interdiction et ont accepté un remboursement anticipé, sous réserve du paiement d'un *funding loss*. Afin d'éviter la discussion sur l'imputation d'un *funding loss*, certaines banques ont décidé de respecter à l'avenir l'interdiction contractuelle de remboursement anticipé. S'il n'y a pas de remboursement anticipé, aucun *funding loss* ne sera imputé.

Un certain nombre d'emprunteurs ont critiqué cette décision des banques et estiment qu'elle peut être considérée comme un abus de droit.

Avant la loi du 21.12.2013 sur le financement des PME, les banques pouvaient encore prévoir contractuellement une interdiction de remboursement anticipé. La loi précitée prévoit désormais un droit de remboursement anticipé, de sorte que depuis le 10.01.2014, il n'est plus possible d'interdire le remboursement anticipé.

Dans les cas où une société avait été autorisée à rembourser de façon anticipée il y a quelques années (sous réserve du paiement d'un *funding loss*) et ne l'est plus aujourd'hui, Ombudsfin estime que la banque a "renoncé à son droit" d'invoquer l'interdiction de remboursement anticipé.

2 - Garanties

Le deuxième thème important reste celui des garanties liées à des crédits professionnels.

Certaines de ces plaintes concernaient des demandes de libération d'une garantie. Depuis l'adaptation de la loi sur le financement des PME en 2017, les banques sont obligées de motiver par écrit chaque refus de libération d'une garantie. Dans ces cas, Ombudsfin examine, entre autre, la situation concrète en matière de crédit, c'est-à-dire les garanties qui existent par rapport aux crédits qui sont encore en cours.

Un dossier concernait la situation où la banque avait initialement 3 garants, mais au fil du temps avait libéré 2 des 3 garants, ne laissant qu'un seul garant. Le garant restant pensait que l'action de la banque l'avait mis dans une situation pire et a demandé à être libéré lui aussi. L'Ombudsman a confirmé que le garant pouvait invoquer l'article 2037 du Code civil, qui stipule que le garant est libéré lorsqu'il ne peut plus être subrogé dans les droits, hypothèques et privilèges de ce créancier en raison des actions de ce dernier. La banque n'a pas suivi cette analyse.

De plus, il y a eu de nouveau des plaintes concernant la conversion d'un mandat hypothécaire en une inscription hypothécaire. Les plaintes sont souvent dues au fait que la décision de convertir le mandat n'est pas communiquée au client à l'avance. Dans ces cas, le débit des coûts de conversion est ressenti comme très agressif par le client. Ombudsfin est favorable à une consultation plus ouverte avec l'emprunteur, afin d'éviter une surprise aussi désagréable.

4. FIN-NET : PLAINTES TRANSFRONTALIÈRES

4.1. FIN-NET

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

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

De plus amples informations sur FIN-NET sont disponibles sur le site de la Commission européenne : https://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.

4.2. PROCÉDURE

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

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

4.3. EXEMPLES CONCRETS

En 2019, Ombudsfin a reçu 3 dossiers dans le cadre desquels la procédure FIN-NET a été utilisée. Dans les dossiers, des institutions hollandaise, portugaise et espagnole étaient concernées..

5. COLLABORATION

5.1. BELGIQUE

5.1.1. Service de Médiation pour le Consommateur

L'Ombudsman en conflits financiers 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.

5.1.2. 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

5.1.3. 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

5.2. EUROPE

5.2.1. 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 4 : « FIN-NET : plaintes transfrontalières ».

5.2.2. 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)

5.3. 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.

En 2019, Ombudsfin a participé à la conférence INFO qui avait lieu en Afrique du Sud. Le programme:

Day 1 – Monday 30 September 2019:

- The fundamental principles of Ombud schemes: critical evaluation & application of the effective approaches
- The new approach to consumer protection and regulation of Ombuds schemes in SA
- Hot topics – discussing the latest hot topics per industry sector
- Learnings from Ombud schemes that went through a merger / consolidation process: A panel discussion with Ireland & Australia
- Consumer financial education
- Communication for Ombud schemes – Expert speaker & panel discussion

Day 2 – Tuesday 1 October 2019:

- Hot topic: the challenges affecting established schemes / the challenges faced by new schemes
- The advent of 'Robo-advice' & the impact on Ombuds & complaints
- The benefits of different structures to resolve complaints i.e. small groups / triage system / panel decisions / teams / single case handler from start to end
- Bench-marking performance for an Ombudsman
- Expert advice on what to expect from innovation in the Fintech space
- Complaints arising from the application of Fintech – What are the implications for Ombud schemes?

Day 3 – Wednesday 2 October 2019:

- Second breakaway session – Hot issues per industry sector
- Applying fairness in Ombudsman rulings: challenges & successes
- An external view of the importance of Facilitation & Mediation in ADR

6. MOYENS FINANCIERS

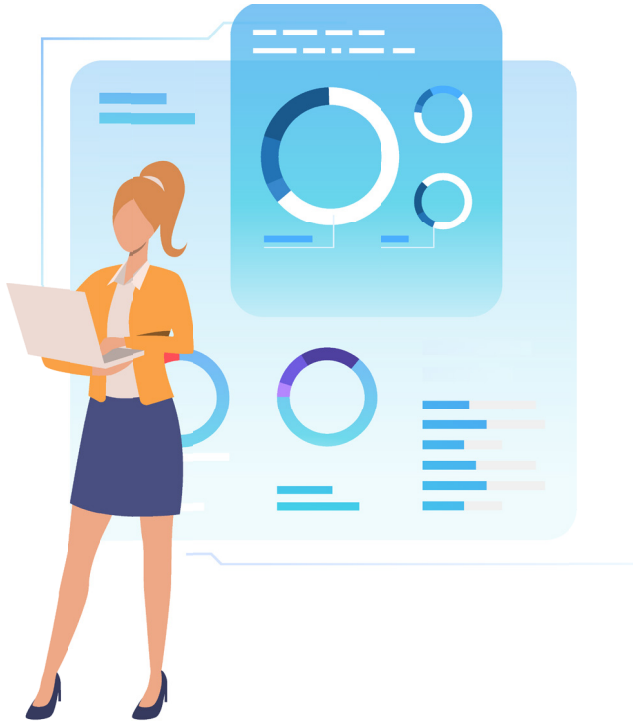
Au moment de la publication de ce rapport annuel 2019, les comptes annuels de l'exercice comptable d'Ombudsfin asbl de 2019 n'ont pas encore été approuvés par l'assemblée générale. Dès que ceux-ci auront été approuvés, les grandes lignes en seront publiées sur le site web d'Ombudsfin sous la forme d'un addendum au rapport annuel (www.ombudsfin.be – Publications – Rapports annuels).

Il est toutefois possible de donner un aperçu du budget établi pour 2019 :

	Budget 2019
Revenus	
Cotisation fixe membres Ombudsfin asbl	523.668,00
Cotisation variable membres Ombudsfin asbl	523.668,00
Revenus totaux	**1.047.336,00**
Dépenses	
Frais de personnel + honoraires	909.000,00
Frais de fonctionnement	138.336,00
Dépenses totales	**1.047.336,00**

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

Le budget nécessaire est demandé aux membres d'Ombudsfin asbl au moyen d'une cotisation fixe et d'une cotisation variable, 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.



7. OMBUDSFIN – À VOTRE SERVICE

7.1. 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 d'un montant maximum de 50 000 € ou de plaintes concernant MIFs (les frais d'interchange facturés dans le cas d'opérations de paiement par carte).

Comment introduire une plainte ?

Votre plainte doit être introduite par écrit, par la poste, par fax, 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
Per e-mail
ombudsman@ombudsfin.be
En ligne sur
www.ombudsfin.be
Par fax au numéro
02 545 77 79

Gratuit

La procédure chez Ombudsfin est gratuite pour le demandeur.

Conditions de recevabilité principales

L'institution financière contre laquelle vous avez une plainte doit être affiliée auprès d'Ombudsfin. La liste des institutions affiliées avec leurs services compétents est disponible sur le site.

Vous avez déjà introduit une plainte par écrit auprès du service compétent de l'institution financière et vous n'avez pas obtenu satisfaction ou vous n'avez pas reçu une réponse dans un délai raisonnable (1 mois).

Votre 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. Votre litige n'a pas non plus été traité par une autre entité qualifiée (ex. : Ombudsman des Assurances).

Le litige ne vise pas à régler un surendettement. Ombudsfin ne fait pas de la médiation de dettes.

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

Comment se déroule le traitement d'un dossier recevable concrètement ?
Ombudsfin envoie d'abord le dossier à l'institution financière pour s'informer de sa position dans l'affaire.

Si des informations complémentaires sont requises, 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.

7.2. COLLABORATEURS OMBUDSMAN

Pour le traitement des demandes, l'Ombudsman est entouré de 2 assistants et de 5 conseillers :

Assistants

Serge Henris, Christel Speltens, Ingrid Vertenten (depuis octobre 2019).

Conseillers

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

OMBUDSFIN

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

ombudsman@ombudsfin.be

www.ombudsfin.be