OMBUDSFIN RAPPORT ANNUEL 25

SOMMAIRE

PREFACE

Jean Cattaruzza
Ombudsman

Dames en heren,

Mesdames et Messieurs,

Ombudsfin, le service de médiation en matière financière, a le plaisir de mettre à votre disposition son rapport annuel relatif à l'année écoulée.

Le premier fait marquant de l'année 2025 est l'augmentation sensible (plus de 10%) des dossiers recevables, soit 2.422, un chiffre jamais atteint par le passé.

Cette augmentation s'explique essentiellement par l'augmentation des dossiers de fraude, en particulier les scénarios de fraude qui impliquent une interaction entre le fraudeur et sa victime. Nous avons aussi connu l'an passé une importante vague de dossiers de crédits frauduleux, suivant un scénario immuable et très bien ficelé.

Le résultat global de nos médiations reste stable. Comme en 2024, 82,5% des plaintes fondées ont donné lieu à une médiation réussie.

Comme par le passé, ce chiffre cache une disparité importante entre le taux de réussite pour les dossiers fraude (58,3%, chiffre qui est toutefois en hausse par rapport aux dernières années), pour les crédits frauduleux (8,7%) et pour les autres types de dossiers (où nous franchissons pour la seconde année consécutive la barre des 95% de médiations réussies).

Vous trouverez dans le présent rapport toutes les statistiques utiles relatives à notre activité ainsi que des explications détaillées sur les différents thèmes qui ont fait l'actualité d'Ombudsfin en 2025.

L'année 2025 restera aussi dans les annales comme celle qui a vu l'extension des compétences d'Ombudsfin. La loi du 11 décembre 2025 a ainsi généralisé notre compétence pour les entreprises personnes physiques, les petites et micro-sociétés et les personnes morales poursuivant un but désintéressé. A l'instar des consommateurs, ces entités peuvent désormais s'adresser à Ombudsfin, quel que soit l'objet de la plainte émise à l'égard de leur institution financière. Il est également intéressant de noter que cette loi jette un pont entre l'ordre judiciaire et la médiation dans la mesure où il est désormais loisible au juge de suggérer aux parties à la cause de s'adresser à Ombudsfin avant qu'il se prononce sur le litige qui lui a été soumis.

Nul doute que les modifications apportées par cette loi à nos compétences se refléteront dans nos prochaines statistiques annuelles. 2026 marquera incontestablement pour Ombudsfin le début d'une nouvelle ère.

Je vous souhaite une intéressante lecture du présent rapport.

Jean Cattaruzza
Ombudsman

NOUVELLE MISSION **D'OMBUDSFIN**

Fin 2025, un nouveau chapitre VI – Règlement extrajudiciaire des litiges en matière financière – a été introduit dans la loi sur la surveillance financière[1] (loi du 2 août 2002 relative à la surveillance du secteur financier et des services financiers). Celui-ci définit la création, les missions et l'organisation d'Ombudsfin, le service de médiation en matière financière.

La mission et les compétences d'Ombudsfin ont ainsi été élargies depuis janvier 2026.

Pour notre mission jusqu'à fin 2025, nous vous renvoyons à notre rapport annuel 2024, p. 4.

En ce qui concerne notre nouvelle mission et nos nouvelles compétences, il est important de retenir ce qui suit :

Ombudsfin est une entité qualifiée, reconnue, indépendante et impartiale au sens du livre XVI « Règlement extrajudiciaire des litiges de consommation » du Code de droit économique et a pour mission principale de traiter les plaintes entre un client (potentiel) et son établissement financier, par la médiation ou en fournissant un avis afin de résoudre le litige.

En outre, Ombudsfin peut également formuler des avis et des recommandations généraux à l'intention des pouvoirs publics, des consommateurs, des entreprises et des institutions financières.

Qui peut introduire une plainte ?

Tout client (potentiel) d'un établissement de crédit (i.e. une banque), d'une entreprise d'investissement, d'un établissement de monnaie électronique, d'un établissement de paiement, d'un prêteur, d'un intermédiaire en services bancaires et d'investissement, d'un intermédiaire de crédit ou d'un gestionnaire de crédit[2] peut faire appel à Ombudsfin s'il n'a pas obtenu satisfaction auprès de son institution financière.

Seuls certains clients professionnels, plus précisément les sociétés qui ne répondent pas aux critères des micro-sociétés ou des petites sociétés[3] , sont soumis à certaines restrictions quant aux matières pour lesquelles Ombudsfin peut intervenir. Pour plus de détails, nous vous renvoyons au règlement de procédure publié sur notre site web.

Comment introduire une plainte ?

La plainte doit être introduite via le formulaire web sur le site www.ombudsfin.be[4], par e-mail ou par la poste 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 :

En ligne sur
www.ombudsfin.be

Par e-mail
ombudsman@ombudsfin.be

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

[1] *Via la loi du 11 décembre 2025 mettant en œuvre le règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) 1093/2010 et (UE) 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937, et le règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849 et portant des dispositions financières diverses, M.B. 24 décembre 2025.*
[2] *Ajout de la loi du 11 décembre 2025.*
[3] *Nouveauté de la loi du 11 décembre 2025.*
[4] *Les demandes de résolution extrajudiciaire des litiges (dans différents domaines) peuvent également être soumises via les plateformes en ligne suivantes : Belmed (jusqu'au 31 août 2026) et ConsumerConnect (au niveau belge).*

Gratuité

La procédure chez Ombudsfin est gratuite pour le demandeur.

Conditions de recevabilité principales[5]

- L'objet de la demande est clairement formulé et suffisamment documenté.
- Ombudsfin est compétent pour l'institution financière concernée.
- Il ne s'est pas écoulé une année depuis que la plainte a été introduite auprès de l'institution financière ou de l'intermédiaire financier.
- Le litige ne fait pas (n'a pas fait) l'objet d'une procédure judiciaire (sous réserve de l'application de l'article 1734, §1er/1, al. *in fine* du Code judiciaire) ou d'une procédure de règlement extrajudiciaire des litiges auprès d'Ombudsfin ou d'une autre entité qualifiée (par exemple : Ombudsman des Assurances).
- La demande ne concerne pas un surendettement pour lequel aucune faute de l'institution financière ne peut être établie.

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

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

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

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

Après examen de la plainte et des négociations, l'ombudsman constate qu'un accord existe entre les parties ou rend un avis.

Si le dossier remet en question un principe général ou si le dossier est plus complexe, celui-ci peut être 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 est libre de ne pas suivre cet avis et peut, le cas échéant, porter l'affaire devant un tribunal.

Collaborateurs et conseillers de l'ombudsman (au 1er avril 2026)

Assistants

Celia Grislain, Roham Hashemi, Serge Henris, Christel Speltens et Ingrid Vertenten (partiellement conseiller).

Conseillers

Vincent Chambeau, Charlotte De Braekeleer, Bérengère de Crombrugghe, Aurore Deckers, Jean Deschuijteneer, Clio Hans, Elke Heymans, Aline Umwali, Stéphanie Vaccaro et Leen Vandenbempt.

Collège d'experts

Reinhard Steennot (président), Johan Vannerom, Alain Guigui, Philippe D'Haen, Piet François, Erik Van den Haute et Mark Delanote (expert *ad hoc* dans les dossiers comportant des aspects fiscaux).

[5] *Changement important introduit par la loi du 11 décembre 2025 : le traitement préalable obligatoire de la plainte par le service de plaintes interne de l'institution financière n'est plus considéré comme une condition de recevabilité.*

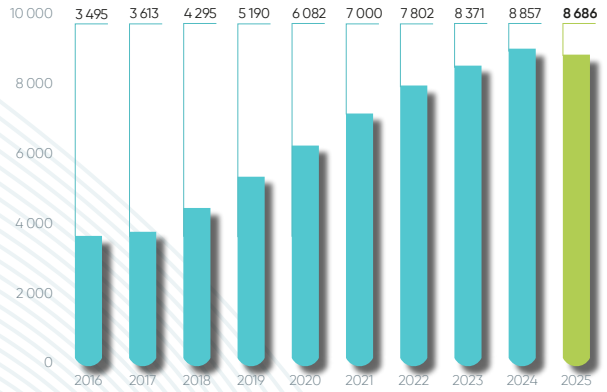
1. OMBUDSFIN EN **CHIFFRES**

1.1. Légère diminution du nombre de demandes introduites

Le nombre total de demandes introduites par les consommateurs et les entreprises en 2025 s'élève à 8.686. Cela représente une légère diminution de 171 dossiers (-1,93 %) par rapport à 2024.

C'est la première fois depuis dix ans qu'on constate une diminution, certes très faible, du nombre de dossiers introduits.

Nombre total de demandes
du 1er janvier au 31 décembre



Ces chiffres comprennent toutes les nouvelles demandes d'informations et les plaintes écrites qui ont été soumises à Ombudsfin au cours de l'année considérée.

Dans chacun de ces dossiers, le demandeur a reçu d'Ombudsfin une réponse à sa demande ou a été 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 8.686 nouvelles demandes introduites par les consommateurs et les entreprises, 8.595 concernaient une plainte et 91 une demande d'information.

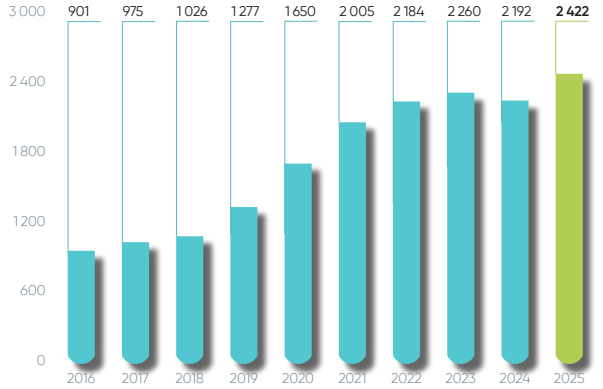
1.2.2. Plaintes recevables

Les plaintes recevables sont celles pour lesquelles Ombudsfin est l'entité qualifiée compétente et qui remplissent toutes les conditions de recevabilité[6].

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* 1.7.).

Parmi les plaintes introduites, seules 2.317 (26,96%) ont été déclarées recevables en 2025. Outre ces plaintes, 105 plaintes datant de 2024 ont également été déclarées recevables en 2025. Au total, 2.422 plaintes ont donc été déclarées recevables en 2025. Après la légère et exceptionnelle baisse de l'année dernière, nous avons atteint un nouveau record en 2025. Par rapport à 2024, nous notons une augmentation de 10,49% (soit 230 plaintes recevables en plus).

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



Par rapport à 2024, nous notons une augmentation de
10,49%
(soit 230 plaintes recevables en plus).

[6] https://www.ombudsfin.be/fr/procedure (nouvelle procédure depuis 2026).

1.2.3. Plaintes non recevables

Parmi les 8.595 plaintes reçues en 2025, 376 dossiers devaient encore être analysés à la fin de l'année et aucune décision définitive n'avait donc été prise quant à leur recevabilité. Parmi les 8.219 dossiers restants, 5.902 (soit 71,81%) ne répondaient pas à toutes les conditions de recevabilité. Les requérants ont toujours été informés de façon étendue quant aux raisons de l'impossibilité de traiter leur demande. Vous trouverez ci-dessous un récapitulatif des différentes raisons invoquées avec leurs nombres respectifs pour 2025, 2024 en 2023.

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

1.3. Délais de traitement des plaintes recevables

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 2025, 372 dossiers ont été prolongés. Dans 12 dossiers, la prolongation était due à la réception tardive ou à l'absence de position de l'institution financière ou de l'intermédiaire[7].

Le délai moyen de traitement de toutes les plaintes recevables, clôturées en 2025, est de 71,2 jours calendrier.

1.4. Interruption de la procédure de médiation

En 2025, la procédure de médiation a été interrompue dans 24 dossiers (1,1% des plaintes clôturées). Dans 8 dossiers, le client nous a informés qu'il souhaitait interrompre la procédure, sans en donner la raison. Dans 3 dossiers, le client n'a pas répondu aux questions complémentaires pertinentes. Dans 3 autres dossiers, la plainte est devenue sans objet, car une solution avait été trouvée par une autre voie. Dans 3 dossiers, l'analyse de la plainte a révélé que le client ne s'était pas exprimé correctement dans sa plainte et qu'Ombudsfin ne pouvait pas intervenir (conflit avec un établissement financier étranger, dossier professionnel portant sur un thème pour lequel Ombudsfin n'était pas compétent, conflit entre un employé et son employeur). Dans 2 dossiers, une procédure judiciaire était en cours. Dans 2 dossiers, il s'agissait d'une procédure judiciaire. Dans 2 autres dossiers, le client est décédé et la plainte n'a pas été poursuivie par les héritiers. Par ailleurs, Ombudsfin s'est vu contraint de mettre fin à la procédure dans 2 dossiers en raison d'un manque total de réaction et de coopération de la part de la société concernée[8]. Enfin, dans 1 dossier, le client a déclaré que sa plainte avait entre-temps été résolue par l'établissement financier concerné.

Raison	Nombre 2025	Nombre 2024	Nombre 2023
La plainte n'a pas encore été introduite en première ligne auprès de l'institution financière	3.893	4.730	4.120
Le client, l'institution ou l'objet de la demande n'est pas identifiable	862	630	510
Ombudsfin n'est pas compétent en la matière	738	870	989
L'institution financière n'est pas affiliée chez Ombudsfin (p.e. bureaux de recouvrement, institutions financières étrangères)	329	333	274
Combinaison de raisons mentionnées dans ce tableau	41	91	132
Procédure judiciaire ou demande déjà traitée par une entité qualifiée	12	6	3
Demande soumise il y a plus d'un an au service des plaintes de l'institution financière	25	32	25
Demande fantaisiste, vexatoire ou diffamatoire	1	0	1
Le traitement de la demande porterait sérieusement atteinte au bon fonctionnement d'Ombudsfin	1	0	0
TOTAL	**5.902**	**6.692**	**6.054**

[7] Cela concerne les institutions financières suivantes (avec indication du nombre de dossiers) : Alpha Credit (1), American Express (1), BNP Paribas Fortis (1), EOS Aremas (1), EPI Company (WERO) (1), Intesa Sanpaolo Wealth Management (1), Lufthansa Airplus Service Karten (1), Moneygram (2), Saxo Bank (1), Sendwave (1), Worldremit (1).
[8] Concrètement il s'agit de : EPI Company (WERO) et Intesa Sanpaolo Wealth Management.

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 2025, avec mention des chiffres et pourcentages respectifs. On observera que les plaintes contre les sociétés de crédit ont quasiment doublé. Ceci est essentiellement dû à la vague de crédits frauduleux dont question au point 4.2. ci-dessous. En revanche, l'augmentation du nombre de dossiers contre les établissements de paiement, qui s'était manifestée en 2024, ne s'est pas poursuivie en 2025. La part des plaintes contre les établissements de paiement est restée stable. Cela ne les empêche toutefois pas de conserver la deuxième place, après les banques.

Catégorie	2025		2024	
	Nombre	%	Nombre	%
Banque	1.770	73,08	1.659	75,68
Etablissement de paiement	382	15,77	372	16,97
Société de crédit	221	9,12	125	5,70
Etablissement de monnaie électronique	17	0,70	15	0,68
Gestionnaire de crédit	9	0,37	0	
Société de leasing	6	0,25	6	0,27
Courtier de crédit	6	0,25	5	0,23
Prêteur social	5	0,21	6	0,27
Société de bourse	3	0,12	2	0,09
Compagnie d'assurances	2	0,08	0	0,00
Entreprise d'investissement	1	0,04	0	0,00
Bureau de change	0	0,00	2	0,09
Intermédiaires en services bancaires et d'investissement (autres qu'agents bancaires)	0	0,00	0	0,00
TOTAL	**2.422**	**100,00%**	**2.192**	**100,00%**

1.6. Résultats globaux

Ombudsfin a rendu un avis dans 2.164 dossiers de consommateurs et d'entreprises en 2025.

Parmi ceux-ci, 777 (soit 35,91%) ont été jugés fondés. Et dans 641 de ces dossiers fondés (soit 82,50%), le dossier a pu être clôturé à l'issue d'une médiation réussie.

Dans 1.363 dossiers (62,99%), Ombudsfin n'a pu identifier aucun manquement juridique ou aucune responsabilité de l'institution financière.

Enfin, il y a eu une interruption de la procédure de médiation dans 24 dossiers (1,1%) (voir *supra* 1.4.).

Plus loin dans ce rapport annuel, les résultats des plaintes des consommateurs, d'une part, et des plaintes des entreprises, d'autre part, sont abordés plus en détail.

1.7. Recommandations individuelles

L'Ombudsman peut adresser des recommandations individuelles aux institutions financières. Ombudsfin leur demande alors de répondre à la recommandation dans un délai de 30 jours.

Ces recommandations sont généralement formulées dans un cadre plus large, comme une adaptation des procédures, des conditions générales ou des listes de tarifs, et ont pour objectif d'éviter que des plaintes similaires à celle qui a fait l'objet de la recommandation soient introduites à l'avenir.

En 2025, 42 recommandations individuelles ont été formulées.

35 recommandations (soit 83,3%) ont fait l'objet d'une action positive de la part des institutions financières. 5 recommandations (soit 11,9 %) n'ont pas été suivies. Dans ces cas, l'institution nous a expliqué les raisons de sa décision. 2 recommandations (4,8%) n'ont pas encore reçu de réponse concrète de la part des institutions financières concernées.

1.8. Collège d'experts[9]

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

En 2025, 3 dossiers ont été soumis au Collège. Ces dossiers concernaient tous des crédits à la consommation (fichage à la Banque nationale, conclusion frauduleuse de contrats et prescription).

2 des 3 dossiers traités (66,67 %) ont été jugés fondés. Dans ces dossiers, Ombudsfin a pu obtenir une solution partielle de la part des institutions financières concernées.

2 questions de principe ont également été soumises au collège d'experts (application de l'article VII.55/2, §3 du Code de droit économique et libération de la garantie locative d'un agent diplomatique sur base d'un jugement).

Vous trouverez les avis du collège sur le site web d'Ombudsfin[10].

[9] Composition du Collège, voir *supra* Mission Ombudsfin – Collaborateurs et conseillers de l'ombudsman
[10] https://www.ombudsfin.be/nl/publicaties/adviezen-college

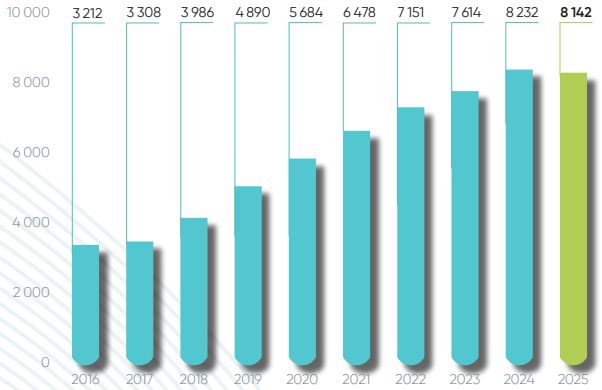
2. DEMANDES INTRODUITES PAR LES **CONSOMMATEURS**

2.1. Légère diminution du nombre de demandes

En 2025, Ombudsfin a reçu 8.142 demandes de consommateurs contre 8.232 en 2024, ce qui représente une diminution de 90 dossiers (-1,09%) par rapport à 2024.

8.057 demandes concernaient une plainte et 85 avaient trait à une demande d'information.

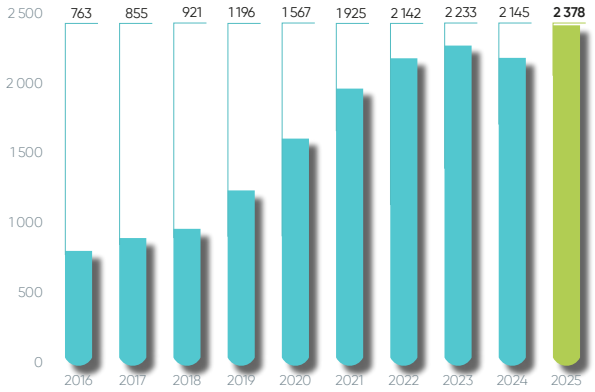
Demandes consommateurs
du 1er janvier au 31 décembre



2.2. Augmentation du nombre de plaintes recevables

En 2025, Ombudsfin a déclaré recevables 2.378 plaintes de consommateurs, contre 2.145 en 2024, ce qui représente une augmentation de 233 dossiers (10,86%) par rapport à 2024.

Plaintes recevables consommateurs
du 1er janvier au 31 décembre



2.3. Résultats des plaintes recevables de consommateurs clôturées en 2025

Ces résultats concernent toutes les plaintes des consommateurs traitées en 2025. Certaines plaintes introduites avant 2025 auprès d'Ombudsfin sont donc aussi incorporées dans ces résultats.

2.129 dossiers ont été clôturés.

Dans 35,84% des dossiers (soit 763 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 63,18% des dossiers (soit 1.345 dossiers), Ombudsfin n'a, en revanche, pas relevé de manquement juridique ou de responsabilité dans le chef de l'institution financière. Ombudsfin a donc jugé ces dossiers non fondés. Dans ces dossiers, les informations et explications utiles ont été données au client afin qu'il puisse comprendre pourquoi Ombudsfin était parvenu à cette conclusion et pourquoi une réparation ou une indemnité de la part de l'institution financière ne pouvait être réclamée.

Dans 21 dossiers, la procédure de médiation a été interrompue par le consommateur (0,98%).

Explication de la diminution du nombre de dossiers fondés

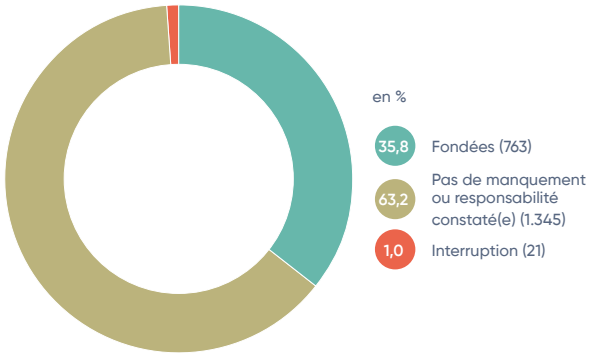
Alors qu'en 2020, Ombudsfin qualifiait encore un peu plus de la moitié des dossiers comme fondés, nous constatons que la proportion de dossiers fondés diminue d'année en année. Cela s'explique principalement par l'évolution des dossiers de fraude[11] (qui représentent une très grande partie des dossiers de plainte auprès d'Ombudsfin) dans lesquels nous sommes amenés à qualifier de plus en plus souvent les opérations contestées d'opérations autorisées (par exemple, en cas de confirmations via itsme) ou dans lesquels nous estimons plus souvent qu'il y a eu une négligence grave sur la base des circonstances spécifiques dans lesquelles le fraudeur a pris connaissance de données bancaires confidentielles cruciales (par exemple en cas d'interaction entre le fraudeur et sa victime). En chiffres, nous parlons pour 2025 de 748 dossiers clôturés, dont seulement 175 ont été jugés fondés (23,4%), tandis que 570 dossiers ont été jugés non fondés (76,2%). Il y a également eu 3 interruptions (0,4%).

À cela s'ajoute l'impact de 42 dossiers clôturés pour fraude à l'investissement (*investment scam*), dont une faible partie ont été considérés fondés puisque les paiements/investissements sont généralement vus comme des opérations autorisées. Dans ce domaine, il y a eu 2 dossiers fondés, 39 dossiers non fondés (92,86%) et 1 interruption en 2025.

Enfin, il y a également l'impact lié au nombre important de plaintes concernant la résiliation de la relation clientèle par l'institution financière, domaine dans lequel Ombudsfin dispose d'une marge de médiation extrêmement limitée. En 2025, 189 dossiers ont été clôturés sur ce thème. Parmi ceux-ci, 135 dossiers ont été jugés non fondés.

Ces 3 thèmes représentent ensemble 55,32% des dossiers non fondés.

Plaintes consommateurs clôturées 2025



Plaintes fondées avec un résultat favorable dans le cadre de la médiation

Sur les 763 plaintes jugées fondées par Ombudsfin en 2025, 82,31% (628 plaintes) ont été résolues. Ce résultat est similaire à celui de l'année dernière.

Explication des dossiers fondés sans résultat favorable dans le cadre de la médiation

En 2025, Ombudsfin a dû clôturer 135 dossiers fondés sans solution, ce qui correspond à 17,69% des dossiers fondés.

Il convient de noter que ce résultat reste influencé par les moins bons résultats obtenus dans les dossiers de fraude classiques (pour plus d'informations sur ces dossiers de fraude, voir *infra* 4.1.). Ombudsfin constate toutefois une amélioration significative des résultats. Alors qu'en 2024, le taux de réussite n'était que de 37,5%, il est monté à 58,3% en 2025.

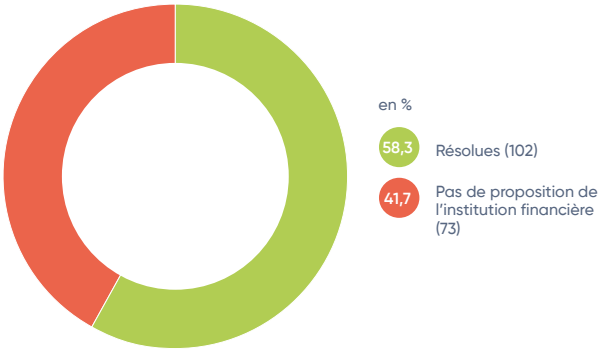
En 2025, les résultats négatifs dans les dossiers de fraude au crédit contracté auprès d'une société de crédit spécifique ont également eu une forte incidence sur le résultat global (pour plus d'informations à ce sujet, voir *infra* 4.2.).

Concrètement, nous parlons de 73 dossiers de fraude « classique » fondés et de 42 dossiers de fraude au crédit fondés, qui représentent donc ensemble 115 (soit 85,19%) des 135 dossiers fondés clôturés sans résultat favorable.

Sans ces dossiers, le taux de réussite chez Ombudsfin serait supérieur à 95%.

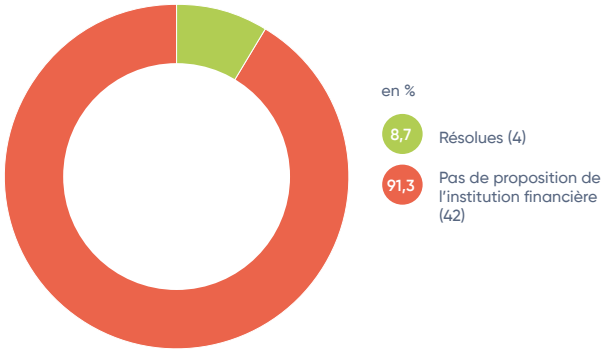
Les graphiques ci-dessous montrent clairement les différences de résultats suivant les thèmes.

Fraude: plaintes fondées consommateurs 2025

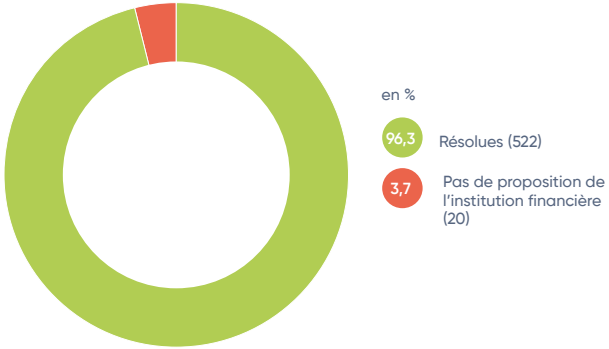


[11] Tous les dossiers de fraude impliquant des opérations de paiement frauduleuses, à l'exception des escroqueries à l'investissement (*investment scam*).

Fraude crédit: plaintes fondées consommateurs 2025



Autres thèmes: plaintes fondées consommateurs 2025

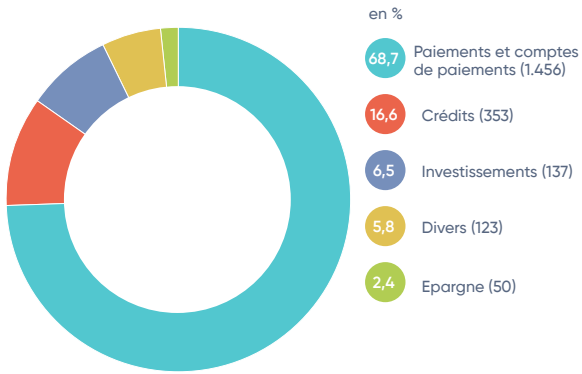


2.4. Thèmes des plaintes des consommateurs

Les thèmes des plaintes analysées des consommateurs en 2025 étaient les suivants (évolution en nombre et en pourcentage par rapport à 2024 et 2023) :

THÈMES	2025		2024		2023	
	Nombre	%	Nombre	%	Nombre	%
Paiements et comptes de paiement	1.456	68,7	1.532	69,9	1.602	74,5
Crédits, dont	353	16,6	246	11,2	223	10,4
Crédits à la consommation	*223*	*10,5*	*132*	*6,0*	*102*	*4,8*
Crédits hypothécaires	*130*	*6,1*	*114*	*5,2*	*121*	*5,6*
Investissements	137	6,5	200	9,1	173	8,1
Divers	123	5,8	151	6,9	120	5,6
Epargne	50	2,4	64	2,9	31	1,4
TOTAL	**2.119**	**100%**	**2.193**	**100%**	**2.149**	**100%**

Part de chaque thème en 2025 :



Le thème principal en 2025 reste « Paiements et comptes de paiements » avec 1.456 dossiers (68,7%). 51,4% (748 dossiers) des dossiers de cette catégorie sont des dossiers de fraude[12].

Le thème principal en 2025 reste « Paiements et comptes de paiements » avec **1.456** *dossiers (68,7%).*

[12] Tous les dossiers de fraude impliquant des opérations de paiement frauduleuses, à l'exclusion des dossiers d'*investment scam*.

2.5. Un aperçu des sous-thèmes les plus importants

2.5.1. Paiements et comptes de paiement

Paiements et comptes de paiement	2025
Opérations via PC ou mobiles (contestées après phishing ou autre fraude)	748
Comptes à vue (résiliation, blocage, clôture, compte dormant)	245
Paiements internationaux	162
Comptes à vue (généralités et tarification)	111
Cartes (opérations contestées après vol, perte)	53
Cartes (généralités et montants réservés/débités)	50
Opérations via PC ou mobiles (mal exécutées ou autres)	38
Guichets automatiques (Self)	18
Domiciliations et ordres permanents	9
Opérations de change	6
Transactions guichet	6
Mobilité bancaire	5
Service bancaire de base	5
TOTAL	**1.456**

La contestation de opérations à la suite d'un phishing ou d'une autre fraude (à l'exclusion des *investment scam/boiler room fraud*) continue donc à constituer, et de loin, le thème le plus important traité par Ombudsfin.

Bien qu'il y ait une diminution légère du nombre de dossiers de fraude par rapport à 2024 (789 dossiers), avec 748 dossiers en 2025, ce thème représente toujours 35,3% du nombre total de plaintes de consommateurs analysées.

A cet égard, nous tenons d'ailleurs à souligner que depuis septembre 2025, Ombudsfin a reçu un nombre nettement plus important de dossiers de fraude qu'au cours des premiers mois de l'année. Tous ces dossiers n'ont pas pu être traités en 2025, ce qui explique que cette tendance ne transparaît pas encore clairement dans les chiffres afférents à l'année 2025.

Le nombre de dossiers liés au blocage et à la résiliation/clôture du compte courant a légèrement diminué en 2025 (245 dossiers en 2025 contre 264 dossiers en 2024), après avoir connu une augmentation remarquable de 66% en 2024.

Les dossiers relevant de ce thème semblent donc se stabiliser plutôt que continuer à augmenter.

Le service bancaire de base pour les consommateurs

La législation qui régit le service bancaire de base se trouve au Chapitre 8, « Accès aux comptes de paiement et service bancaire de base », Section 1, Livre VII, Titre 3 du Code de droit économique.

Ombudsfin est l'organisme compétent pour traiter une procédure de plainte et d'appel extrajudiciaire en ce domaine. À noter qu'Ombudsfin a une compétence contraignante en cette matière. En 2025, Ombudsfin est intervenu dans 5 plaintes concernant le service bancaire de base. 2 plaintes n'étaient pas fondées. Dans les 3 autres dossiers (fondés), les avis d'Ombudsfin ont été suivis positivement.

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 2025:

Statistiques Service bancaire de base (SBB)	2025
Nombre de banques ayant enregistré une demande de SBB	12
Nombre de comptes SBB ouverts	20.706
Nombre total de comptes SBB existants	112.244
Nombre de refus d'ouverture d'un compte SBB	17
Nombre de comptes SBB résiliés (*)	17.612

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

En 2025, 12 banques ont enregistré des services bancaires de base, soit autant qu'en 2024.

Le nombre de services bancaires de base existants à la fin de 2025 était de 112.244, une augmentation de 2,8% par rapport à la fin de 2024.

En 2025, 17 ouvertures de services bancaires de base demandées ont été refusées.

La principale raison d'une clôture est la demande du titulaire (83,8%), suivie par :

- Autres comptes supérieurs à 6.000 euros (15,1 %)
- Un crédit à la consommation supérieur à 6.000 euros auprès d'un établissement de crédit (0,6 %)
- Antécédents négatifs auprès de la banque (0,3 %)
- Compte à vue auprès d'un autre établissement (0,1 %)
- Autres produits incompatibles avec les services bancaires de base (0,1 %)

2.5.2. Crédits

2.5.2.1. Crédits hypothécaires

Crédits hypothécaires	Nombre de plaintes
Exécution du contrat	75
Conclusion du contrat	31
Garanties	10
Mandat hypothécaire	5
Désolidarisation	4
Conditions générales (autres)	3
Crédit-pont	2
TOTAL	**130**

Ombudsfin constate une légère augmentation du nombre de dossiers relatifs aux crédits hypothécaires (de 114 en 2024 à 130 en 2025).

En 2025, la plupart des plaintes concernant les crédits hypothécaires ont trait à l'exécution du contrat de crédit (75 dossiers). Ces dossiers concernaient principalement un fichage négatif auprès de la Banque nationale de Belgique (15 dossiers), des difficultés de remboursement (14 dossiers) et le taux d'intérêt applicable (13 dossiers).

Parmi les dossiers relatifs à la conclusion du contrat (31 dossiers), les motifs les plus importants de plaintes sont le déroulement de la procédure d'octroi (10 dossiers) et un refus de crédit (10 dossiers).

2.5.2.2. Crédits à la consommation

Crédits à la consommation	Nombre de plaintes
Conclusion du contrat	111
Exécution du contrat	110
Autres	2
TOTAL	**223**

En 2025, le nombre de dossiers relatifs aux crédits à la consommation a connu une augmentation remarquable (passant de 132 en 2024 à 223 en 2025). Cette augmentation est principalement liée à l'augmentation du nombre de dossiers relatifs à la conclusion de crédits à la consommation (de 53 dossiers en 2024 à 111 en 2025). 46 dossiers concernent le même problème, qui s'est produit chez une seule société de crédit. Concrètement, il s'agissait de dossiers dans lesquels le contrat avait été conclu de manière frauduleuse (pour plus d'informations à ce sujet, voir *infra* 4.2.). Outre cela, il y a aussi eu 44 dossiers concernant un refus de crédit.

En matière d'exécution du crédit, le nombre de dossiers a également fortement augmenté (de 79 dossiers en 2024 à 110 en 2025). Les plaintes portaient souvent sur un fichage négatif à la Banque nationale de Belgique (45 dossiers), des questions relatives au décompte (21 dossiers) ou des difficultés de remboursement (20 dossiers).

2.5.3. Investissements

Investissements	Nombre de plaintes
Investment scam	42
Achat et vente de titres (execution only)	25
Comptes titres	24
Aspects fiscaux	14
Divers	12
Conseil en placement	8
Fonds de pension/épargne-pension	6
Gestion de fortune	3
Corporate action	2
Information sur les tarifs/coûts	1
TOTAL	**137**

De manière générale, le nombre de dossiers relevant du thème « Investissements » a fortement diminué. En 2025, Ombudsfin n'a traité que 137 dossiers d'investissement, contre 200 en 2024. Cela représente donc une baisse de 31,5%.

La plupart des plaintes portent sur les fraudes à l'investissement (*investment scam/boiler room fraud).* Mais le nombre de dossiers traités a presque diminué de moitié : de 77 dossiers en 2024 à 42 dossiers en 2025.

Le nombre de dossiers a également diminué pour les autres thèmes, mais dans une moindre mesure. Parmi les plaintes liées à « l'achat et la vente de titres (*execution only*) », 11 dossiers concernaient l'achat ou la vente d'actions.

Les dossiers relatifs aux « comptes-titres » portaient souvent sur le transfert des titres (11 dossiers).

2.5.4. Divers (y compris « Epargne »)

Divers	Nombre de plaintes
Produits d'épargne	50
Successions	43
Vie privée	22
Garantie locative	18
Know Your Customer	16
Divers	10
Coffres	6
Incapacité (mineur, administration provisoire)	4
Discrimination	3
Saisie	1
TOTAL	**173**

En 2025, Ombudsfin a reçu 50 plaintes concernant les produits d'épargne, dont 19 dossiers portaient plus spécifiquement sur la manière de comptabiliser la prime de fidélité dues pour les comptes d'épargne.

Les successions (43 dossiers) restent également un thème important. Elles sont suivies par la « vie privée » (22 dossiers) et la « garantie locative » (18 dossiers).

3. DEMANDES INTRODUITES PAR **LES ENTREPRISES**

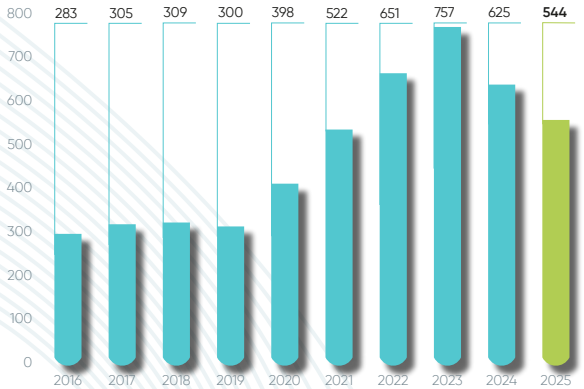
3.1. Diminution du nombre de demandes

En 2025, Ombudsfin a reçu un total de 544 demandes écrites d'entreprises, contre 625 en 2024. Cela représente une diminution de 81 dossiers (12,96%).

Le nombre de demandes reste toutefois élevé. Cela s'explique par le fait que les entreprises s'adressent plus facilement à Ombudsfin, mais ne sont pas toujours conscientes que nos compétences - du moins jusqu'à fin 2025 - étaient limitées pour leurs litiges.

538 demandes concernaient une plainte, tandis que 6 demandes concernaient une demande d'information.

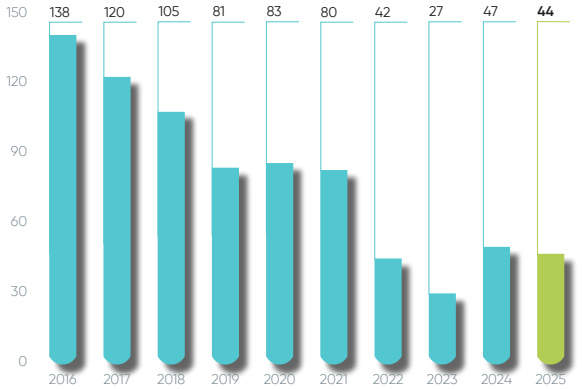
Demandes entreprises
du 1er janvier au 31 décembre



3.2. Légère diminution du nombre de plaintes recevables

En 2025, Ombudsfin a enregistré 44 demandes d'entreprises comme plaintes recevables, contre 47 demandes en 2024, ce qui représente une diminution de 3 dossiers (-6,38%). En raison de l'extension de nos compétences (voir *supra* : Preface et Nouvelle mission Ombudsfin), nous nous attendons à une augmentation significative de ce chiffre en 2026.

Plaintes recevables entreprises
du 1er janvier au 31 décembre



3.3. Résultats des plaintes des entreprises clôturées en 2025

Les résultats dont question ci-dessous concernent toutes les plaintes des entreprises qui ont été traitées et clôturées en 2025.

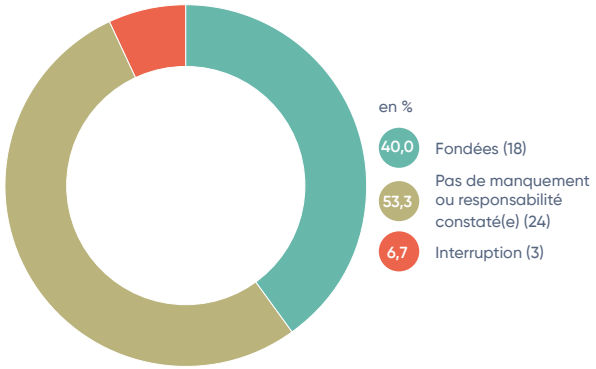
Il s'agit de 45 dossiers.

Dans 18 dossiers (soit 40%), 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 24 dossiers (soit 53,3%), Ombudsfin n'a décelé aucune faute juridique 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 3 dossiers (6,7%), la procédure de médiation a été interrompue anticipativement par l'entreprise.

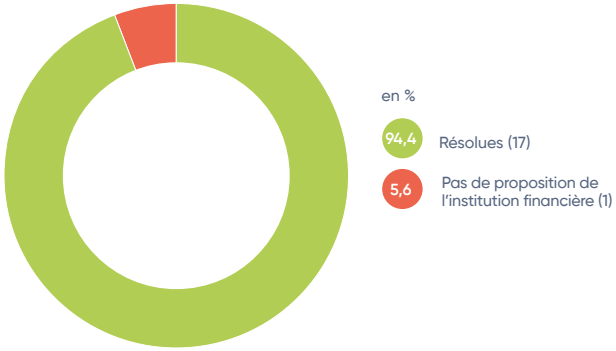
Plaintes clôturées entreprises 2025



Dans l'un des 18 dossiers fondés, l'institution financière n'a pas suivi l'avis d'Ombudsfin. Les 17 autres dossiers (94,44%) ont en revanche pu être clôturés avec une solution satisfaisante.

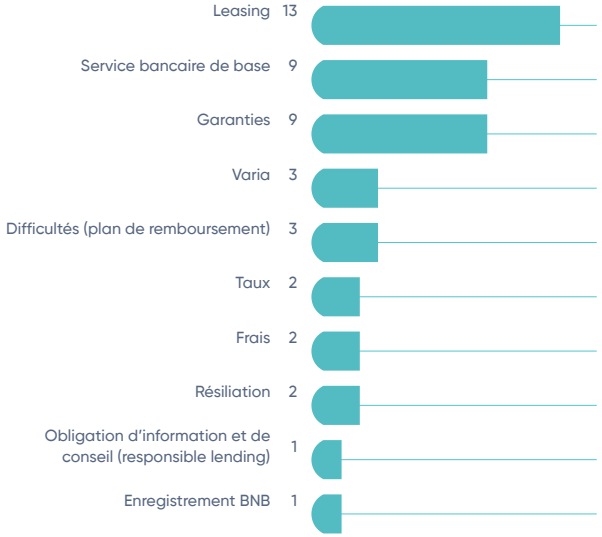
Le dossier dans lequel la banque n'a pas suivi l'avis d'Ombudsfin concernait pourtant un avis contraignant dans le cadre d'un service bancaire de base pour les entreprises (pour une brève discussion, voir *infra* 7.2).

Plaintes fondées entreprises 2025



3.4. Thèmes des plaintes des entreprises

En 2025, les plaintes concernaient les thèmes suivants:



En 2025, Ombudsfin a dû intervenir dans 9 dossiers relatifs au service bancaire de base pour les entreprises (contre 6 dossiers en 2024).

Ombudsfin a jugé 5 de ces dossiers non fondés. Nous avons donc estimé ne pas pouvoir contester la décision de refus.

3 autres dossiers ont en revanche été jugés fondés. Ombudsfin a alors émis un avis contraignant demandant l'octroi du service bancaire de base. Dans 2 dossiers, la banque a accepté de le faire après l'intervention d'Ombudsfin. Dans 1 dossier, la banque a persisté dans son refus, malgré notre avis contraignant.

Enfin, dans 1 autre dossier, l'entreprise a mis fin prématurément à la procédure auprès d'Ombudsfin.

Au point 7.2, nous discutons brièvement de notre expérience dans les dossiers relatifs au service bancaire de base.

En 2025, Ombudsfin a reçu un total de
544
demandes écrites d'entreprises

4. FRAUDE

4.1. Opérations de paiement contestées

Comme les années précédentes, Ombudsfin a traité en 2025 un très grand nombre de plaintes relatives à la contestation d'opérations frauduleuses. Sur les 2.119 dossiers de consommateurs traités par Ombudsfin en 2025, pas moins de 801 dossiers (soit 37,8% du nombre total de plaintes de consommateurs traitées) concernaient la contestation d'opérations frauduleuses. La majorité d'entre elles (748 plaintes) avaient trait à la contestation d'opérations confirmées à distance, c'est-à-dire des dossiers de fraude sur Internet. 53 dossiers portaient sur la contestation d'opérations effectuées avec une carte de paiement physique, après sa perte ou son vol.

En outre, Ombudsfin a également traité 42 plaintes concernant des escroqueries à l'investissement (*investment scam*), qui sont traditionnellement incluses dans nos statistiques sous la rubrique « investissements ».

Dans la catégorie des dossiers de fraude sur Internet, les scénarios de fraude utilisés sont restés globalement les mêmes. Ombudsfin remarque toutefois que le nombre de dossiers traités impliquant un scénario classique de phishing via une communication écrite (par exemple, e-mail, SMS ou messages sur les réseaux sociaux) a diminué. Le nombre de dossiers traités impliquant un scénario de vishing a quant à lui augmenté.

Le vishing (contraction des mots « voice » et « phishing ») désigne une forme d'escroquerie par téléphone. Les escrocs se font passer pour des employés d'une banque, de Card Stop ou d'autres institutions et ont recours à la manipulation psychologique (également appelée « *social engineering* ») pour inciter les victimes à agir de manière urgente et à leur communiquer leurs coordonnées bancaires. Souvent, l'escroc accède également à l'ordinateur ou au téléphone portable de la victime et donc à l'environnement bancaire présent sur cet appareil. Pour plus d'informations, le site web Safeonweb présente différents scénarios de vishing[13].

Dans les dossiers de vishing, Ombudsfin ne peut souvent pas établir de manquement juridique ou de responsabilité de l'institution financière sur la base de la réglementation légale actuelle en matière de répartition de la responsabilité en cas d'opérations de paiement non autorisées. La raison en est que, dans ces dossiers, Ombudsfin doit généralement conclure soit que les opérations de paiement contestées doivent être considérées comme des opérations de paiement autorisées (en particulier lors de l'utilisation d'itsme), soit qu'il y a une négligence grave de la part de la victime (par exemple lorsque la victime donne accès à son appareil et son environnement bancaire ou communique des codes secrets[14] au téléphone). Dans ces circonstances, Ombudsfin ne peut donc pas, sur la base de la réglementation légale actuelle, exiger de l'institution financière qu'elle intervienne pour compenser le préjudice financier subi par la victime. Cette constatation générale n'empêche bien sûr pas Ombudsfin d'examiner les circonstances concrètes et factuelles de la fraude dans chaque dossier individuel et de parvenir, le cas échéant, à une autre conclusion. Dans ces dossiers, Ombudsfin vérifiera également si la banque a agi avec suffisamment de diligence en matière de détection de la fraude et de récupération des fonds.

Dans ce rapport annuel, nous aborderons plus en détail le déroulement des fraudes par vishing, ainsi que le caractère autorisé ou non des opérations de paiement effectuées lors d'une fraude par vishing. L'analyse par Ombudsfin de la détectabilité préalable et de la négligence grave dans un scénario de vishing fréquemment observé en 2025, dans lequel un escroc se fait passer pour un employé de Card Stop, sera également examinée.

Nous aborderons aussi un « nouveau » scénario de phishing, dans lequel les victimes ont tenté de recharger une carte téléphonique Proximus via des sites web frauduleux qui ressemblaient à celui de Proximus.

Nous rappellerons ensuite les positions d'Ombudsfin concernant la procédure d'installation et de mise en service des applications bancaires mobiles, la nécessité pour les victimes de fraude de pouvoir signaler la fraude

[13] Voir par exemple: https://safeonweb.be/fr/actualite/vishing-les-arnaques-par-telephone-se-multiplient.
[14] Doivent ainsi être gardés secrets et ne pas être communiqués à qui que ce soit : le code PIN de la carte de débit ou de crédit, ou l'application bancaire ou de l'application itsme, mais aussi les codes de réponse générés au moyen du digipass.

à la banque via un seul point de contact central et l'importance des tentatives de récupération rapides par la banque en cas de virements instantanés.

Nous aborderons également brièvement l'entrée en vigueur du contrôle obligatoire du nom associé à l'IBAN, le fonctionnement des limites de dépenses et l'importance pour Ombudsfin de disposer d'un procès-verbal d'une plainte pénale déposée par la victime de la fraude auprès de la police.

Enfin, nous examinerons l'évolution des avis rendus par Ombudsfin en matière de carte bancaire avalée par un distributeur automatique.

Pour une analyse complète de la réglementation relative à la répartition de la responsabilité en cas d'opérations de paiement non autorisées, telle que prévue dans le Code de droit économique (ci-après le « CDE »), nous vous renvoyons à nos rapports annuels précédents[15].

4.1.1. Vishing

4.1.1.1. Déroulement d'une fraude par vishing

Dans les dossiers de vishing, la victime reçoit un appel téléphonique d'un escroc qui se fait généralement passer pour un employé de sa banque, de Card Stop ou d'une autre instance officielle. La victime est appelée sur sa ligne fixe, sur son numéro de GSM ou via une application d'appel vidéo telle que WhatsApp. Certaines victimes entendent d'abord un message automatisé concernant une opération sur leur compte bancaire. Pour confirmer ou contester l'opération, elles doivent composer un chiffre, puis elles sont mises en relation avec l'escroc. Ce dernier indique qu'il y a une opération suspecte sur le compte bancaire de la victime ou que le compte bancaire de la victime est menacé par un phishing, un virus ou un piratage sur l'appareil de la victime. Le fraudeur inspire confiance et convainc la victime qu'il est urgent d'agir pour empêcher toute fraude (supplémentaire). Sous pression, la victime est alors poussée à agir rapidement.

Outre les techniques de manipulation psychologique, les escrocs utilisent également des données (bancaires) précédemment interceptées via un phishing classique afin de convaincre la victime de manière crédible de la légitimité de l'appel. Si l'escroc a déjà obtenu l'accès à l'environnement bancaire en ligne de la victime grâce à un phishing préalable, il peut consulter les comptes de la victime et même effectuer des opérations entre les différents comptes de celle-ci. Grâce à ces informations, l'escroc parvient à construire une histoire très crédible.

Pour soi-disant empêcher la fraude, la victime doit suivre les instructions données par téléphone par l'escroc. Il s'agit par exemple :

- du virement de fonds vers un compte soi-disant sécurisé, également appelé « compte à sécurité renforcée ». Dans ce scénario, la victime effectue et approuve elle-même consciemment un virement dans son environnement bancaire en ligne afin de mettre ses fonds en sécurité[16];
- de donner au fraudeur l'accès à l'appareil (mobile) de la victime via des logiciels tels qu' Anydesk ou Teamviewer ou via l'installation d'une application frauduleuse. Grâce à ce logiciel ou à cette application, le fraudeur peut non seulement voir ce qui se passe sur l'appareil de la victime, mais aussi en prendre le contrôle. Si la victime se connecte ou est connectée à son environnement bancaire en ligne dans ces circonstances, le fraudeur a également accès à l'environnement bancaire en ligne sur l'appareil de la victime elle-même;
- de la transmission au fraudeur par téléphone (ou via un appareil ou un site web sous le contrôle du fraudeur) des codes générés par la carte bancaire, le code PIN et le digipas[17];
- de confirmer les actions qui apparaissent dans l'application itsme de la victime;
- de scanner les codes QR envoyés par le fraudeur à l'aide de l'application bancaire mobile de la victime.

Si la victime pense que ses actions permettent d'empêcher ou d'annuler des opérations frauduleuses, elles permettent en réalité à l'escroc d'accéder à l'environnement bancaire en ligne de la victime et d'effectuer des virements et/ou des paiements à partir des comptes de la victime.

Ce type de fraude est en augmentation et oblige les banques à prendre des mesures de précaution tant en matière d'information aux clients qu'en matière d'ajustement des systèmes de détection des fraudes de la banque.

Au cours de l'année écoulée, certaines banques ont lancé des outils sous le nom « vérifiez votre appel », qui permettent aux clients de vérifier via leur application bancaire si un appel téléphonique provient réellement de la banque. Récemment, une banque a également annoncé un outil permettant aux clients de faire appel à une personne de confiance qui aide à détecter les virements suspects. itsme a également pris une mesure

[15] Voir en particulier le rapport annuel 2022, pages 16 à 39. Les rapports annuels 2023 et 2024 expliquent des phénomènes et des évolutions spécifiques.
[16] Pour une analyse de la fraude liée aux comptes à sécurité renforcée, voir le rapport annuel 2020, titre 2.8.2.2, p. 24 et 25.
[17] Dans ce rapport, le terme « digipass » désigne à la fois le Digipass et le lecteur de carte bancaire.

supplémentaire dans la lutte contre le vishing : lorsque l'application itsme détecte qu'un utilisateur reçoit une action itsme pendant un appel téléphonique, un écran de vérification apparaît via un pop-up qui avertit d'une possible escroquerie. Cet écran ne bloque toutefois pas l'action. C'est à l'utilisateur de décider de refuser l'action ou de l'exécuter malgré tout[18].

Ombudsfin se réjouit de ces différentes initiatives et espère qu'elles seront suivies d'autres. L'avenir nous dira toutefois si ces mesures suffiront à réduire la fraude par vishing.

4.1.1.2. Opérations de paiement (non) autorisées en cas de vishing et impact de l'utilisation d'itsme

Lorsqu'il analyse des opérations de paiement contestées dans un contexte de vishing, Ombudsfin vérifie en premier lieu s'il s'agit d'opérations de paiement autorisées ou non au sens de l'article VII.32 du CDE.

Comme expliqué dans le rapport annuel 2022[19], Ombudsfin ne peut considérer une opération de paiement comme autorisée que si le payeur a librement et consciemment accepté l'opération de paiement. Selon Ombudsfin, cela signifie qu'une opération ne peut être qualifiée d'autorisée que si, au moment du paiement, le payeur connaissait le montant et le bénéficiaire (en cas de virement) ou l'objet (en cas de paiement) de l'opération.

Lorsqu'un escroc demande par téléphone à la victime d'effectuer elle-même un virement vers un compte prétendument sécurisé et que la victime encode (et confirme) elle-même le virement dans son environnement bancaire en ligne, il s'agit, selon Ombudsfin, d'une opération de paiement autorisée. Bien que la victime soit trompée, elle connaît le montant et le numéro de compte du bénéficiaire et les saisit elle-même dans son environnement bancaire en ligne. Dans ces circonstances, le consentement de la victime à l'exécution du virement est donc établi.

Au cours de l'année passée, Ombudsfin a constaté une augmentation du nombre de dossiers de vishing dans lesquels la victime était invitée à confirmer une action à l'aide de son application itsme, soi-disant pour sécuriser des fonds ou pour empêcher ou annuler des opérations frauduleuses. Dans ces dossiers, ce n'est généralement pas la victime qui effectue une opération de paiement dans son environnement bancaire en ligne, mais le fraudeur qui a accédé d'une manière ou d'une autre à cet environnement. La victime reçoit ensuite une action sur son application itsme qu'elle peut confirmer ou refuser.

D'après notre expérience, l'application itsme indique généralement clairement quelle action la victime doit confirmer. Dans le cas d'un virement, le montant, le numéro de compte du bénéficiaire et le fait qu'une opération doit être confirmée sont en principe mentionnés. Pour les paiements, l'application itsme indique le montant, le bénéficiaire (commerçant) et le fait qu'une opération doit être confirmée.

Bien que nous comprenions parfaitement que les victimes agissent dans un état de panique sur les instructions d'un escroc crédible, Ombudsfin estime qu'il est difficile de défendre l'idée que la victime n'ait pas pu comprendre, sur la base des informations disponibles dans l'application itsme, que sa confirmation entraînerait l'approbation d'une opération de paiement. Dans ce type de dossiers, Ombudsfin conclut dès lors généralement qu'il s'agit de opérations de paiement autorisées. Cela n'empêche pas Ombudsfin d'insister auprès des banques pour qu'elles formulent leurs messages dans itsme de la manière la plus claire possible. Ombudsfin n'hésitera pas, dans les dossiers où le message affiché serait ambigu (par exemple en raison d'un défaut technique), à adopter une position différente quant au caractère autorisé ou non d'une opération de paiement confirmée avec itsme.

Ombudsfin recommande aux consommateurs de ne jamais approuver avec itsme une action qu'ils n'ont pas eux-mêmes initiée et souligne qu'avec itsme (tout comme avec un code généré par digipass), les opérations de paiement ne peuvent pas être annulées.

Dans un faible nombre de dossiers de vishing, Ombudsfin a constaté que la victime était invitée à scanner, à l'aide de son application bancaire mobile, un code QR envoyé par l'escroc, à la suite de quoi elle devait approuver une opération de paiement via l'application bancaire. Dans la mesure où l'écran de l'application bancaire indique clairement le montant, le bénéficiaire et le fait qu'il s'agit d'une opération de paiement avant que la victime ne procède à l'approbation, il s'agit également dans ces dossiers de opérations de paiement autorisées.

Pour les opérations de paiement autorisées, le CDE ne prévoit actuellement aucune disposition sur la base duquel la banque peut être tenue d'intervenir

[18] Voir le communiqué de presse d'itsme du 5 février 2026 : https://press.itsme-id.com/itsme-lance-de-nouvelles-fonctionnalites-pour-faciliter-son-utilisation-et-ameliorer-la-protection-des-utilisateurs.
[19] Voir le rapport annuel 2022, p. 19.

dans le préjudice financier subi par la victime. Cela pourrait changer à l'avenir. La proposition de nouveau Règlement européen sur les services de paiement[20] prévoit en effet un régime de responsabilité dans lequel les consommateurs victimes d'usurpation d'identité (lorsqu'un fraudeur se fait passer pour un employé de la banque) auraient droit à un remboursement (sous certaines conditions).

Bien que le nombre de dossiers de vishing dans lesquels Ombudsfin estime qu'il s'agit de opérations de paiement autorisées augmente (grâce à l'utilisation d'itsme), cela ne signifie pas pour autant qu'il ne peut y avoir de opérations de paiement non autorisées dans le cadre du vishing.

Lorsque la victime transmet par téléphone, sur instruction du fraudeur, un code généré à l'aide de sa carte bancaire, de son code PIN et de son digipass, elle n'est pas nécessairement informée que ce code permet de confirmer une opération de paiement, et elle ne connaît généralement pas le montant ni le bénéficiaire de la opération. Même si la victime doit saisir ce code sur un site web frauduleux ou sur un appareil contrôlé par l'escroc, l'objectif de l'action est caché par l'escroc. Nous notons à cet égard que lors de la prise de contrôle d'un appareil via un logiciel tel qu'Anydesk ou Teamviewer ou via une application frauduleuse, la victime ne voit généralement pas ce que le fraudeur fait réellement sur son appareil. Elle voit souvent un écran noir, un message d'erreur ou un message similaire. En outre, le digipass de la victime n'affiche pas toujours des informations détaillées sur le montant et le bénéficiaire (cela dépend du type de digipass). Dans ces circonstances, Ombudsfin estime qu'on a affaire à des opérations de paiement non autorisées.

Il arrive aussi régulièrement que le fraudeur réussisse à lier les données bancaires de la victime à l'une de ses applications de paiement (comme l'application *Payconiq by Bancontact*[21]) ou à activer une application bancaire et/ou l'application itsme au nom de la victime sur son propre appareil mobile. Le fraudeur approuve alors les opérations de paiement via ces applications à l'aide d'un code d'accès qu'il a lui-même choisi. Dans ces dossiers, il est également clair que la victime n'a pas donné son accord pour les opérations contestées et Ombudsfin considère qu'il s'agit de opérations de paiement non autorisées.

En cas de opérations de paiement non autorisées, le régime de responsabilité légale, en vertu duquel la banque peut, sous certaines conditions, être tenue d'intervenir pour compenser le préjudice financier subi par la victime, est applicable. L'analyse de ce régime repose essentiellement sur les concepts de détectabilité préalable de la fraude et de négligence grave.

4.1.1.3. Détectabilité et négligence grave dans le cadre d'une tentative de vishing par un soi-disant employé de Card Stop

Dans les dossiers de vishing traités par Ombudsfin en 2025, nous avons constaté plusieurs cas dans lesquels l'escroc s'est fait passer pour un employé de Card Stop. L'appel, qui n'est pas effectué à partir du numéro officiel de Card Stop (078 170 170), évoque une opération suspecte sur le compte bancaire de la victime. Pour empêcher ou annuler la opération suspecte, la victime doit communiquer ses coordonnées bancaires et effectuer certaines opérations (comme décrit ci-dessus).

Dans certains dossiers, nous constatons également que le soi-disant employé de Card Stop demande les coordonnées bancaires de la victime auprès de plusieurs banques ou celles d'autres membres du ménage, sous prétexte que la fraude présumée s'étendrait à plusieurs comptes et serait donc plus importante que ce qui avait été initialement allégué.

Card Stop est un service belge permettant de bloquer les cartes de paiement et certains autres instruments de paiement en cas de perte, de vol ou de suspicion de fraude[22]. Tout titulaire d'une carte de paiement ou d'un instrument de paiement peut appeler Card Stop pour obtenir un blocage, et ce 24 heures sur 24, 7 jours sur 7. Card Stop n'a toutefois pas accès aux comptes bancaires et ne peut ni consulter ni bloquer les opérations[23]. Après un appel, Card Stop procède uniquement au blocage des cartes de paiement et/ou des instruments de paiement communiqués par le demandeur.

[20] Voir le texte de la proposition initiale : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52023PC0367.
[21] À partir de mars 2026, l'application s'appellera Bancontact Pay. Voir le communiqué de presse à ce sujet : https://www.payconiq.be/fr/payconiq-evolue.
[22] Voir: https://www.cardstop.be/
[23] Card Stop ne doit pas être confondu avec d'autres services de Worldline, notamment macarte.be, qui permet aux titulaires de cartes de crédit de contester un achat. Les titulaires d'une carte de crédit peuvent toutefois être contactés par écrit par Worldline (en particulier par SMS) lorsque Worldline ou la banque détecte une opération potentiellement suspecte. Dans ce message, le titulaire de la carte est invité à contacter lui-même le service clientèle de Worldline. Pour plus d'info voir : https://www.cardstop.be/fr-be/home/dans-quels-cas-bloquer.

Card Stop n'appelle jamais de manière proactive les titulaires de cartes pour les informer de opérations suspectes. Card Stop ne demande jamais non plus de partager des codes secrets ou d'utiliser un lecteur de carte, itsme ou une application (bancaire).

Si ces dossiers concernent des opérations de paiement non autorisées (voir l'analyse ci-dessus), Ombudsfin vérifie si la victime aurait pu détecter la fraude à l'avance et, dans l'affirmative, si elle a commis une négligence grave.

L'article VII.44, §1, alinéa 2, 1° du CDE prévoit qu'un payeur ne supporte aucune perte si la perte, le vol ou l'utilisation abusive de son instrument de paiement n'ont pas pu être constatés par le payeur avant que l'opération n'ait été effectuée (sauf si le payeur a lui-même agi de manière frauduleuse).

Dans les dossiers de vishing impliquant un un faux employé de Card Stop, Ombudsfin a généralement estimé que, selon les circonstances, la victime aurait pu détecter la fraude à l'avance, et ce sur la base (i) du numéro utilisé par l'escroc, qui ne correspondait pas au numéro officiel de Card Stop, et (ii) du fait que la victime était invitée par téléphone à communiquer certains codes ou à utiliser itsme, ce qui n'est jamais nécessaire pour bloquer une opération frauduleuse.

Lorsque la fraude est détectable, la règle de base prévue à l'article VII.44 du CDE est que la banque doit supporter la perte liée à une opération de paiement non autorisée, après déduction d'une franchise de 50 euros, à moins que la banque ne puisse prouver que le payeur a manqué à certaines obligations par négligence grave.

Bien que, dans les dossiers en question, la victime ait été manipulée au téléphone, mise sous pression et ait probablement agi dans un état de panique dans le but de lutter contre la fraude, les actes commis par la victime peuvent, selon Ombudsfin, en fonction des circonstances factuelles de l'espèce, donner lieu à une qualification de négligence grave.

Ainsi, la communication de codes par téléphone (y compris les codes de réponse générés par digipass), l'utilisation d'itsme ou d'une application bancaire sur instruction téléphonique pour « annuler » des opérations (alors que les messages visibles dans itsme et l'application bancaire sont clairs) et le fait d'autoriser un tiers à prendre le contrôle de l'environnement bancaire en ligne sur l'appareil de la victime via des applications logicielles telles qu'Anydesk ou Teamviewer sont, selon Ombudsfin, des actes qui vont tellement à l'encontre de l'obligation pour le payeur de garantir la sécurité de ses instruments de paiement et de leurs données de sécurité personnelles, prévue à l'article VII.38§2 du CDE, qu'ils peuvent être constitutifs de négligence grave. En ce cas, la banque n'est pas tenue d'intervenir pour compenser le préjudice financier subi par la victime.

4.1.2. Phishing des détenteurs de cartes téléphoniques Proximus

Au cours du premier semestre de l'année dernière, Ombudsfin a traité plusieurs dossiers de fraude au phishing dans lesquels les victimes souhaitaient recharger en ligne leur carte téléphonique prépayée Proximus. Après une recherche sur internet, elles se sont retrouvées sur un site web frauduleux qui semblait provenir de Proximus. Dans ces dossiers, Ombudsfin a notamment relevé les noms de domaine suivants : 'Proxlmus.com', 'proximus-e.com', 'proximus-re.com', 'proximus-be.com', 'proximus-telecom.com', 'my-proximus.fr' et 'reload-click.com'.

Les victimes tentent d'approuver des paiements d'un montant limité sur ces sites web frauduleux afin de recharger leur carte téléphonique, en utilisant un code de réponse généré par digipass. En réalité, le code de réponse est intercepté par un fraudeur et utilisé de manière abusive pour approuver un autre paiement à l'insu de la victime.

Les paiements contestés dans ces dossiers ont été qualifiés par Ombudsfin de opérations de paiement non autorisées. En effet, la reconstitution du déroulement de la fraude a montré que, dans ces dossiers, les victimes n'ont à aucun moment pu connaître le montant ni le bénéficiaire de la opération de paiement et n'ont donc pas pu donner leur accord. En conséquence, Ombudsfin a appliqué le régime de responsabilité prévu par le CDE pour les opérations de paiement non autorisées.

Dans aucun des dossiers traités, la banque n'a procédé au remboursement provisoire des opérations de paiement non autorisées, bien qu'un tel remboursement soit prévu à l'article VII.43, §1 du CDE. Dans le contexte

de la fraude sur Internet, Ombudsfin constate que les banques procèdent très rarement à un remboursement (provisoire), car elles souhaitent généralement analyser au préalable l'application des règles prévues à l'article VII.44 du CDE en matière de répartition de la responsabilité entre le client et la banque. L'application des règles prévues à l'article VII.44 du CDE détermine de manière définitive dans quelle mesure la banque doit intervenir dans le préjudice.

Lors de l'analyse de l'application de l'article VII.44 du CDE, Ombudsfin vérifie en premier lieu si la victime pouvait détecter la fraude à l'avance. L'article VII.44, §1, alinéa 2, 1° du CDE prévoit en effet qu'un payeur ne supporte aucune perte si la perte, le vol ou l'utilisation frauduleuse de son instrument de paiement n'ont pas pu être constatés par le payeur avant que l'opération n'ait été effectué (sauf si le payeur a lui-même agi de manière frauduleuse).

Dans les dossiers qui lui ont été soumis, Ombudsfin a généralement conclu que la victime aurait pu détecter la fraude, notamment sur la base des noms de domaine utilisés par les sites web frauduleux, qui ne correspondent pas au nom de domaine officiel utilisé par Proximus (proximus.be). Il convient en effet d'être particulièrement vigilant lors de l'utilisation des moteurs de recherche en ligne.

Lorsque la fraude est détectable, la règle de base prévue à l'article VII.44 du CDE est que la banque doit supporter la perte liée à une opération de paiement non autorisée, après déduction d'une franchise de 50 euros, à moins que la banque ne puisse prouver que le payeur a manqué à certaines obligations par négligence grave.

Dans les dossiers "Proximus" examinés, Ombudsfin a conclu dans la plupart des cas qu'il n'y avait pas eu de négligence grave de la part des victimes. Les victimes souhaitaient bel et bien effectuer un paiement et n'ont pas délibérément communiqué des données bancaires confidentielles à un fraudeur. Elles se sont retrouvées sur un site web frauduleux mais bien contrefait, par le biais duquel leurs données bancaires ont été interceptées et utilisées de manière abusive pour effectuer un paiement dont la victime n'avait pas connaissance et qu'elle ne souhaitait pas. Bien que la fraude ait été détectable et qu'il y ait eu une certaine imprudence, les actes des victimes n'étaient, selon Ombudsfin, pas suffisamment atypiques pour considérer qu'une personne normalement prudente ne les aurait jamais accomplis dans les mêmes circonstances.

Ombudsfin doit malheureusement constater que, dans les dossiers concernés, les banques n'ont pas suivi son argumentation relative à l'absence de négligence grave et ont souvent refusé d'intervenir pour compenser le préjudice financier subi par les victimes. Dans les dossiers où Ombudsfin a jugé la plainte de la victime fondée, Ombudsfin n'a pu obtenir une intervention partielle que dans 4 dossiers sur 12 (33%).

4.1.3. Installation d'une application bancaire mobile

Comme les années précédentes, Ombudsfin a constaté en 2025 que les fraudeurs parviennent, grâce à différents scénarios frauduleux, à installer sur leur propre appareil une application bancaire mobile liée aux comptes de la victime[24]. Comme un fraudeur peut, via cette application, effectuer des opérations entre les comptes de la victime à l'aide d'un code PIN qu'il a lui-même choisi, augmenter les limites d'utilisation et confirmer des opérations de paiement, le préjudice pour la victime dans ces dossiers peut rapidement devenir très important.

Nous remarquons à cet égard que, malgré les recommandations antérieures visant à demander à la fois une authentification du payeur et une activation supplémentaire lors de la procédure d'installation de l'application bancaire mobile, il n'existe pas toujours de phase d'activation via, par exemple, un message SMS ou un e-mail contenant un code ou un lien d'activation. Nous constatons également dans certains dossiers que les fraudeurs peuvent utiliser l'application bancaire très rapidement après son installation. Après l'installation de l'application bancaire, la victime reçoit certes un message d'avertissement par e-mail ou par SMS, mais même si elle réagit très rapidement, cela n'empêche pas le fraudeur d'approuver, dès la réception de l'avertissement, des opérations de paiement via la nouvelle application. Dans ce contexte, Ombudsfin recommande à nouveau aux banques de laisser un certain délai entre l'envoi d'un avertissement et la mise en service de l'application afin de permettre à la victime de la fraude de prendre connaissance de l'avertissement et de prendre les mesures nécessaires.

Si Ombudsfin constate qu'aucune activation distincte n'est requise lors de l'installation d'une application bancaire mobile et qu'une application bancaire peut être utilisée immédiatement sans délai raisonnable pour que la victime puisse réagir à un message d'avertissement, il n'hésitera pas à demander à la banque d'intervenir dans le cadre d'une médiation afin de compenser le préjudice financier subi par la victime et adressera une recommandation à cet effet à la banque concernée.

[24] Voir le rapport annuel 2022, p. 33 à 35 et le rapport annuel 2023, p. 20 à 21.

4.1.4. Notification de fraude à la banque

Conformément à l'article VII.38 du CDE, une victime de fraude est tenue d'informer immédiatement la banque ou l'entité désignée par celle-ci (généralement Card Stop) lorsqu'elle constate la perte, le vol ou l'utilisation frauduleuse de son instrument de paiement. Si la victime ne le fait pas, elle risque d'être accusée de négligence grave si elle souhaite ensuite invoquer le régime de responsabilité légale en cas de opérations de paiement non autorisées.

Dès la notification de la fraude par la victime, la banque est notamment tenue d'empêcher toute utilisation ultérieure du moyen de paiement de la victime. Il doit donc être impossible pour le fraudeur de confirmer de nouvelles opérations de paiement avec l'instrument de paiement de la victime. L'article VII.44 §3 du CDE prévoit expressément que la banque est responsable de tous les dommages survenant après la notification de la fraude.

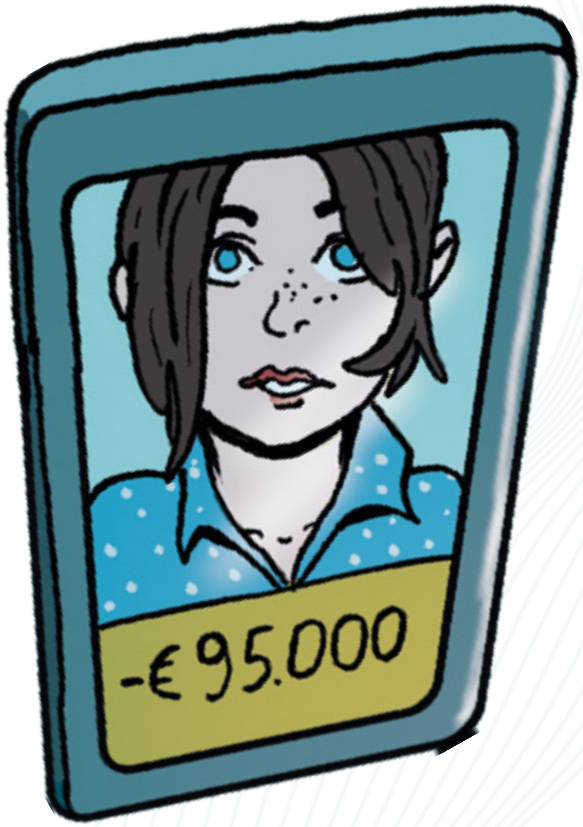
Comme les années précédentes[25], Ombudsfin a traité cette année plusieurs dossiers dans lesquels des banques demandaient aux victimes de fraude de faire plusieurs notifications dans le cadre d'un même dossier de fraude afin de garantir le blocage de tous ses instruments de paiement.

Si un appel à Card Stop permet de bloquer les cartes de paiement (24 heures sur 24 et 7 jours sur 7), cela ne suffit pas auprès de certaines banques pour bloquer également les autres moyens de paiement, tels que les applications bancaires mobiles. Pour cela, il est nécessaire de contacter directement la banque[26].

À l'inverse, nous constatons dans certains dossiers que les victimes de fraude qui contactent directement leur banque pour signaler une fraude sont invitées à contacter également Card Stop, au motif que le blocage des cartes de paiement via la banque serait apparemment moins rapide.

Ombudsfin estime qu'une seule notification devrait suffire lorsqu'une victime signale une fraude et défend dans les dossiers que la première notification à Card Stop ou à la banque vaut notification de fraude conformément à l'article VII.38 du CDE. Les banques ne suivent toutefois pas toujours cette position. Dans la mesure où, pour des raisons techniques ou d'efficacité, il est encore nécessaire qu'une victime contacte à la fois la banque et Card Stop, il nous semble approprié que l'appel de la victime soit directement transféré à l'autre service concerné.

En ce qui concerne le moment exact de la notification, c'est le moment où la victime appelle la banque ou Card Stop qui constitue, pour Ombudsfin, le moment de la notification. Bien qu'il soit normal que la banque ou Card Stop pose un certain nombre de questions afin d'identifier l'appelant avant de pouvoir procéder au blocage des instruments de paiement, ces étapes et leur durée ne peuvent porter préjudice au fait que la notification de la fraude par la victime a lieu au moment de l'appel et à la répartition des risques prévue à cet égard dans le CDE. D'après notre expérience, la plupart des banques suivent ce raisonnement.



[25] Voir par exemple le rapport annuel 2023, p. 21 à 22.

[26] Les banques belges proposent aujourd'hui un service permanent téléphonique qui permet aux clients de signaler une fraude à leur banque 24 heures sur 24, 7 jours sur 7. En février 2025, Febelfin a diffusé un dépliant numérique reprenant les numéros de téléphone des différentes banques auxquelles il est possible de signaler une fraude: https://febelfin.be/media/pages/publicaties/2025/flyer-telefoonnummer-online-fraude/554025dfd8-1747396049/flyer_fraude_fr_fin.pdf

4.1.5. Tentative de récupérer les fonds par la banque en cas de virement instantané

Après avoir été informée d'une fraude concernant des opérations de paiement, la banque doit faire des efforts raisonnables pour récupérer les fonds des opérations contestées. Cela signifie qu'après avoir été informée, la banque doit prendre le plus vite possible les mesures nécessaires pour (i) bloquer les opérations contestées (si cela est encore possible), (ii) bloquer les éventuels comptes bénéficiaires auprès de la banque elle-même et (iii) envoyer un message à chaque établissement financier bénéficiaire pour lui demander de bloquer les comptes bénéficiaires et de rembourser les fonds éventuellement disponibles. Cette obligation qui incombe à la banque s'inscrit dans le cadre de la norme générale de diligence qui s'applique à chacun, et plus particulièrement du devoir général de diligence de la banque envers ses clients.

Même dans le cas d'un virement instantané[27], l'obligation de récupération s'applique dès notification de la fraude et la banque doit prendre les mesures de récupération nécessaires. Les virements instantanés ont pour particularité d'être traités immédiatement, 24 heures sur 24 et 7 jours sur 7, donc y compris la nuit, les jours fériés et le week-end. L'argent se retrouve en quelques secondes sur le compte du bénéficiaire. Compte tenu de la mise à disposition immédiate des fonds au bénéficiaire, il est essentiel, dans ce type de dossier, de lancer rapidement une tentative de récupération afin de conserver une chance réelle de récupérer l'argent.

Dans l'analyse des dossiers, Ombudsfin vérifie donc si la banque a effectivement pris les mesures nécessaires pour lancer très rapidement (presqu'immédiatement) une tentative de récupération.

Ombudsfin note également que depuis le 9 octobre 2025, les banques de la zone euro sont tenues de proposer à leurs clients des virements instantanés via les canaux par lesquels un client peut également effectuer un virement standard[28]. Cette obligation ne porte toutefois pas atteinte à l'obligation de récupération décrite ci-dessus.

4.1.6. Vérification du nom IBAN

Depuis le 9 octobre 2025, les banques sont tenues de vérifier, pour les virements en euros et au sein de la zone euro, que le numéro de compte saisi corresponde au nom du bénéficiaire[29]. Si le numéro de compte et le nom ne correspondent pas, la banque doit en avertir expressément le payeur avant que celui-ci n'approuve le virement. L'avertissement doit mentionner que le fait d'autoriser le virement pourrait entraîner le transfert des fonds vers un compte de paiement qui n'est pas détenu par le bénéficiaire désigné par le payeur. Si le numéro de compte et le nom correspondent presque (mais pas entièrement), la banque doit indiquer le nom correct du bénéficiaire.

La banque est donc tenue de mettre à la disposition des payeurs un service de vérification sur la base duquel le payeur peut décider lui-même de poursuivre ou non l'exécution du virement. Si la banque n'offre pas ce service ou si celui-ci ne fonctionne pas correctement et qu'il y a eu un virement mal exécuté, la banque est tenue de rembourser le montant transféré et de rétablir le compte de paiement du payeur dans l'état où il se serait trouvé si le virement n'avait pas eu lieu.

Il reste à espérer que l'utilisation du service de vérification entraînera une diminution réelle de certaines formes de fraude dans lesquelles la victime est amenée à effectuer elle-même un virement bancaire, comme par exemple la fraude relative aux factures, le whaling et la fraude au compte à sécurité renforcée.

4.1.7. Respect des limites de dépenses

Dans les dossiers relatifs à des opérations contestées, Ombudsfin constate régulièrement que la question se pose de savoir si ces opérations ont bien été effectuées dans les limites de dépenses fixées.

Les limites de dépenses sont fixées par défaut par la banque, mais peuvent dans la plupart des cas être modifiées (augmentées ou diminuées) par le payeur.

Les limites de dépenses sont fixées par instrument de paiement. Chaque instrument de paiement (tel qu'une carte bancaire, une application bancaire, une application de paiement, etc.) a ses propres limites, qui dépendent également du type d'opérations effectuées. Ainsi, des limites différentes s'appliquent aux virements, aux paiements ou aux retraits d'argent.

Les limites pour les différents types d'opérations s'appliquent de manière cumulative. Cela peut prêter à confusion pour les clients, car ceux-ci ne connaissent pas toujours suffisamment la différence entre un virement et un paiement, par exemple. Dans les cas de fraude où un escroc parvient à effectuer à la fois des virements et des paiements, le préjudice pour la victime peut ainsi sensiblement augmenter.

[27] Selon le communiqué de presse de Febelfin du 30 janvier 2026, les virements instantanés représentaient à cette date un peu plus de 31% de l'ensemble des virements effectués en Belgique.
[28] Cette obligation est imposée par le Règlement européen 2024/886 du 13 mars 2024, également connu sous le nom de Règlement sur les paiements instantanés ou Instant Payments Regulation.
[29] Cette obligation est imposée par le Règlement sur les paiements instantanés ou Instant Payments Regulation.

Ombudsfin recommande aux banques d'informer explicitement leurs clients de l'application cumulative des limites d'utilisation lorsque ceux-ci fixent des limites.

La fixation de limites (basses) peut certainement aider les clients à limiter les dommages en cas de fraude au phishing 'simple'. Ombudsfin constate toutefois régulièrement, dans les cas de fraude plus complexes, où un fraudeur parvient à accéder à l'environnement bancaire en ligne de la victime, que le fraudeur augmente lui-même les limites de virement ou de paiement (à l'aide d'un code de réponse généré par digipass, d'une confirmation via itsme ou d'une confirmation via le code PIN de l'application bancaire). Une notification séparée à la victime concernant l'augmentation des limites et l'instauration d'un certain délai entre l'approbation de l'augmentation de la limite et son entrée en vigueur (*'slow banking'*) pourraient permettre aux victimes de fraude de détecter la fraude à temps et de prendre les mesures nécessaires pour limiter autant que possible leur dommage.

4.1.8. Importance du procès-verbal d'une plainte pénale en cas de fraude

Ombudsfin a remarqué ces derniers temps que les victimes de fraude qui souhaitent porter plainte auprès de la police ne sont pas toujours interrogées de manière approfondie sur le déroulement de la fraude dont elles ont été victimes. Ainsi, dans les dossiers de fraude sur Internet où le préjudice financier est limité, certains commissariats de police se contentent d'établir un procès-verbal simplifié. Ce procès-verbal ne mentionne que les éléments les plus importants des infractions signalées (notamment l'identité de la victime, le type d'infraction, le mode opératoire, le préjudice, la date et l'heure de l'infraction et un résumé des faits rapportés par la victime). Le recours à un tel procès-verbal simplifié dépend souvent de la politique menée à cet égard par les autorités judiciaires compétentes.

Or, lors de l'analyse des dossiers de fraude et, en particulier, de l'application du régime de responsabilité légale en cas de opérations de paiement non autorisées, il est essentiel pour Ombudsfin de bien comprendre les circonstances factuelles concrètes de la fraude. En effet, le régime de responsabilité repose sur des concepts tels que la détectabilité de la fraude et la négligence grave. Pour évaluer ces concepts, les circonstances factuelles dans lesquelles la victime a agi sont déterminantes. Les déclarations de la victime telles qu'elles figurent dans le procès-verbal de plainte déposé auprès de la police constituent dès lors une source d'information importante pour Ombudsfin, d'autant plus que cette plainte est généralement déposée très peu de temps après la fraude, à un moment où les faits sont encore bien connus de la victime.

En l'absence de procès-verbal contenant l'audition de la victime, la reconstitution des faits et l'analyse du dossier peuvent s'avérer difficiles pour Ombudsfin.

Ombudsfin recommande aux victimes de documenter le déroulement de la fraude dont elles ont été victimes dès que possible après les faits, à l'aide de tous les éléments pouvant prouver la fraude (par exemple, des captures d'écran des communications avec les fraudeurs, des données détaillées sur les appels, les communications reçues de la banque pendant la fraude, etc. Les victimes peuvent également rédiger elles-mêmes une déclaration écrite sur le déroulement de la fraude et la faire ajouter au procès-verbal (simplifié) de leur plainte auprès de la police afin que leur déclaration sur le déroulement de la fraude puisse être intégrée au dossier pénal.

Enfin, nous tenons à souligner que les banques demandent presque toujours aux victimes de fraude de déposer plainte auprès de la police et de fournir à la banque l'attestation de dépôt de plainte. Les banques demandent cette attestation notamment afin de pouvoir démontrer, dans le cadre de tentatives de récupération des fonds auprès d'autres institutions financières, que la récupération est demandée pour cause de fraude. Selon Ombudsfin, le lancement d'une tentative de récupération ne peut toutefois être reporté jusqu'à la réception du procès-verbal de plainte. Un tel report compromettrait en effet fortement les chances de succès d'une telle tentative.

4.1.9. Avalement de la carte – Obligations du titulaire et évolution du raisonnement suivi par Ombudsfin

Ombudsfin est régulièrement confronté à des dossiers de fraude dans lesquels le fraudeur a fait croire à sa victime que sa carte avait été avalée par un distributeur dans une agence bancaire ou dans un point Bancontact.

Afin d'éviter que sa victime ne fasse immédiatement bloquer sa carte via sa banque ou Card Stop (078 170 170), le fraudeur (qui se fait passer pour un autre client) déclare en général à la victime que sa propre carte vient également d'être avalée et que, soit il suffit de revenir le lendemain à l'agence pour la récupérer, soit que le distributeur est équipé d'un microphone et qu'il faut lui parler, soit encore prétend être en ligne avec Card Stop (ou la banque) et prête son GSM à la victime (qui pense être en communication avec un préposé de Card Stop ou de sa banque alors qu'il parle en réalité à un complice du fraudeur).

En réalité, la carte de la victime n'a pas été avalée et, dès que la victime quitte les lieux, le fraudeur la récupère et réalise des opérations par son biais le plus rapidement possible en en profitant pour vider les comptes du payeur malheureux.

Selon un arrêt de la Cour d'appel de Bruxelles du 14 novembre 2019 (R.G. 2013/AR/2696), l'avalement d'une carte ne s'identifie pas strictement à sa perte ou son vol. Partant, en ne faisant pas immédiatement bloquer sa carte, le titulaire de la carte ne commettrait pas une négligence grave au sens de l'article VII.44, §4 du CDE.

Cet arrêt a été rendu il y a plus de six ans. Or, depuis lors, les habitudes des payeurs ont changé et ils sont mieux conscientisés par rapport au devoir de bloquer leurs instruments de paiement en cas de vol, perte, détournement ou avalement. Ombudsfin considère donc devoir procéder à une analyse cas par cas avant de déterminer si le titulaire de la carte soi-disant avalée a commis une négligence grave. Ombudsfin prendra notamment en considération dans son analyse :

(i) sur le plan purement contractuel, le libellé des dispositions contractuelles applicables et le fait qu'il y soit stipulé clairement et de manière suffisamment évidente la nécessité de faire bloquer la carte en cas d'avalement, sous forme d'obligation et non pas de simple conseil (comme c'était le cas dans l'affaire dont la Cour d'appel de Bruxelles a eu à connaître) ;

(ii) sur le plan communicationnel, la publicité faite aux alentours du distributeur, dans l'agence et sur le site internet de la banque relativement aux démarches à entreprendre en cas d'avalement de la carte ; et

(iii) les circonstances de l'espèce.

4.1.10. Envoi de la carte et du code PIN par deux canaux de communication différents

Face au risque d'interception et détournement des courriers postaux ordinaires, de nombreuses banques envoient désormais à leur client la carte (de débit ou de crédit) et son code PIN initial[30] par deux canaux de communication différents.

Ainsi, si la carte physique doit nécessairement être envoyée au client par courrier postal, le code PIN pourrait lui être remis par un autre biais.

A titre d'illustration, certaines banques requièrent de leurs clients qu'ils envoient un SMS à un numéro donné via leur numéro de GSM connu de la banque. Les clients reçoivent en retour un SMS contenant le code PIN initial (qui s'efface automatiquement 24 ou 48 heures plus tard).

Une telle procédure nous apparaît renforcer la sécurité de l'envoi de cartes puisqu'elle implique que seul le client soit en principe en mesure d'obtenir ses codes PIN initiaux.

Les banques ont d'ailleurs tout intérêt à mettre en place une procédure robuste et sécurisée car l'article VII.39, 6° du CDE leur fait supporter le risque lié à l'envoi de l'instrument de paiement (i.e. la carte) et de toute donnée de sécurité personnalisée (i.e. son code PIN).

Malheureusement, Ombudsfin constate que des institutions financières continuent à envoyer la carte et son code PIN par deux courriers postaux. S'ils sont certes envoyés à quelques jours d'intervalle, il n'en demeure pas moins que cette manière de faire est loin d'être optimale.

Sans préjudice des recommandations précédemment formulées en ce sens, nous profitons du présent rapport pour enjoindre les institutions financières concernées à revoir leurs procédures afin de tenir compte des considérations évoquées ci-dessus.

[30] Que ce client pourra librement modifier par la suite.

4.2. Vague de crédits frauduleux conclus auprès de Buy Way

Depuis la fin de l'année 2024 et tout au long de l'année 2025, Ombudsfin a été saisi d'un nombre extrêmement important (68) de plaintes introduites à l'égard de Buy Way relativement à des ouvertures de crédit conclues frauduleusement[31]. La presse francophone et néerlandophone[32], ainsi que Test-Achats[33], s'en sont d'ailleurs fait l'écho.

Les faits sous-jacents étant substantiellement identiques, nous pouvons parler d'une vague de fraudes, qui a débuté courant novembre 2024 et a apparemment – fort heureusement – pris fin le 4 août 2025, suite aux renforcements apportés par Buy Way à sa procédure d'octroi de crédit.

Nous évoquerons ci-dessous la manière dont la fraude prend naissance, selon notre expérience, et l'analyse juridique que nous avons suivie dans ces différents dossiers.

4.2.1. Les faits

Un commerçant (une société d'électroménager connue) propose, en sa qualité d'intermédiaire de crédit, à ses clients de financer leurs achats en magasin et en ligne auprès d'elle par le biais de différents types de crédit octroyés par Buy Way, dont notamment des ouvertures de crédit. Cela permet à un client qui ne souhaite pas payer en une fois des produits (par exemple : un smartphone, un téléviseur ou encore une machine à laver) de les acheter à crédit et les rembourser en plusieurs fois.

Le fraudeur utilise cette procédure en ligne à son profit afin d'obtenir du commerçant la livraison à l'adresse qu'il a spécifiée des articles commandés sur le site web (en général : des smartphones) après que le prix de ceux-ci ait été payé au moyen d'une (ou deux) ouvertures de crédit(s) conclue(s) auprès de Buy Way au nom de sa victime.

Si la manière dont le fraudeur a obtenu les coordonnées du consommateur n'est, dans la plupart des cas, pas claire[34], ce qu'il s'est passé le jour de la fraude l'est en revanche beaucoup plus.

Pour la victime, tout commence généralement par un contact téléphonique (appel et/ou SMS) présenté comme émanant de « Buy Way » (si elle était déjà cliente de celle-ci) ou de « Card Stop » ou « itsme » (si elle n'était pas encore cliente de Buy Way)[35]. Après l'avoir mise en confiance, le fraudeur amène la victime à réaliser certaines actions sur son propre GSM, qui ignore qu'elle est en train de permettre l'ouverture d'un crédit à son nom.

En général, ce n'est que lorsque le consommateur recevait le contrat de crédit par e-mail[36] ou la carte de crédit par la poste qu'il s'apercevait qu'il avait été victime d'une fraude. A ce stade, il était déjà trop tard.

[31] Parmi ces dossiers, 46 d'entre eux ont été clôturés en 2025, comme expliqué sous 2.5.2.
[32] Le Soir, « Arnaque via itsme : un réseau criminel démantelé, 300 victimes recensées », 13 juin 2025, ; Sud Info, « « 2.500 euros pour un crédit qu'ils n'ont jamais signé » : des dizaines de Belges victimes de cette arnaque, Test-Achats met en garde », 13 septembre 2025 ; Het Laatste Nieuws, « Tientallen Belgen krijgen plots factuur tot 3.000 euro na hack bij kredietmaatschappij achter IKEA en MediaMarkt : « We krijgen schrijnende verhalen binnen » », 13 septembre 2025 ; VRT NWS, « Minstens 80 Belgen slachtoffer van fraude via kredietmaatschappij Buy Way », 13 septembre 2025.
[33] Test-Achats, « Attention à la fraude au crédit BuyWay: des dizaines de consommateurs ont déjà été arnaqués », 15 septembre 2025.
[34] Certaines victimes (qui étaient déjà clientes auprès de Buy Way au jour de la fraude) se rappellent avoir reçu un e-mail de Buy Way les invitant à mettre à jour leurs coordonnées en remplissant un faux formulaire web.
[35] Initialement, entre novembre 2024 et mai 2025, le fraudeur contacte systématiquement le consommateur par téléphone. Par la suite, aux alentours de juin 2025, le fraudeur envoie un SMS au consommateur via le numéro court 8629.
[36] Sachant que jusqu'en janvier 2025 le fraudeur pouvait remplacer l'adresse e-mail du consommateur par la sienne, une fois la validation via itsme effectuée.

En effet, même lorsque la victime prenait rapidement contact avec Buy Way et/ou le commerçant pour les avertir de la fraude, force est de constater que le commerçant considérait la vente parfaite et livrait les articles commandés[37].

4.2.1.1. Validation d'une action itsme

Le fraudeur demande d'abord au consommateur de valider une action itsme sur sa propre application itsme au moyen de son code secret ou d'une reconnaissance digitale ou faciale.

Le libellé de cette action itsme est « *Connexion* » « *Buy Way* » « *Info : S'identifier pour une demande de crédit* »[38].

4.2.1.2. Réception par SMS d'un code de vérification

Ensuite, un SMS, libellé comme suit, est envoyé par Buy Way[39]: « *Votre code de vérification Buy Way est: [code de vérification]* ».

Jusque fin décembre 2024, le fraudeur pouvait modifier le numéro de GSM auquel le SMS était envoyé pour y indiquer le sien. Il n'avait donc plus besoin du concours du consommateur après la validation de l' (des) action(s) itsme.

A partir de fin décembre 2024, Buy Way a supprimé la possibilité de modifier le numéro de GSM de sorte que le SMS soit envoyé au même numéro que celui de l'appareil ayant servi à valider l'action itsme. En résumé, à compter de cette date, le consommateur devait communiquer au fraudeur le code de vérification qu'il avait reçu par SMS, en plus de valider au moins une action itsme.

Si l'on avait pu penser que cette amélioration endiguerait la vague de fraudes, cela n'a pas été le cas, le libellé du SMS étant trop vague, de notre point de vue, pour comprendre à quoi servait le code de vérification qu'il contenait.

A noter que ce libellé a été modifié courant juin 2025 en : « *Votre code de vérification confidential signature code est : [code de vérification]* » en lieu et place de « *Votre code de vérification Buy Way est: [code de vérification]* ». Ombudsfin a constaté que cette modification n'a malheureusement pas résolu le problème. Au contraire, selon nous, elle a accru l'opacité puisque le nom de Buy Way n'était plus mentionné.

4.2.1.3. Signature du contrat de crédit et mise à disposition de son montant

Une fois que le fraudeur est mis en possession du code de vérification contenu dans le SMS envoyé par Buy Way, il n'a plus besoin du consommateur et peut librement – sans que la victime n'en ait conscience – compléter et signer d'une seule traite les différents documents relatifs à l'ouverture de crédit (formulaire de demande, contrat, mandat SEPA et cession de rémunération).

Le montant du crédit est alors mis à disposition sous forme d'une ouverture de crédit[40]. Une partie des fonds sert à financer le panier d'achat en ligne qui est validé par le webshop du commerçant.

4.2.2. Problèmes juridiques[41]

Pour refuser d'intervenir dans les différents dossiers soumis à notre examen, Buy Way a mis en avant la négligence grave de la victime, qui a effectivement, d'une manière ou d'une autre, réalisé des manipulations et communiqué au fraudeur des informations indispensables à l'octroi du (des) crédit(s).

Ombudsfin a toutefois estimé qu'il n'avait pas à se prononcer sur cette question dans la mesure où, en l'occurrence, les dispositions de l'article VII.44 du Code de droit économique ne trouvaient pas à s'appliquer. Au contraire des dispositions du même Code relatives à l'octroi d'un crédit à la consommation, que nous allons passer en revue ci-dessous.

4.2.2.1. Signature du contrat de crédit

Pour rappel, l'article VII.76 du CDE prévoit que le prêteur ne peut conclure un contrat de crédit qu'après avoir vérifié l'identité du consommateur. Il s'agit d'une obligation de résultat.

L'article VII.78 du CDE définit quant à lui le type de signature électronique requis pour qu'un contrat de crédit à la consommation (telle une ouverture de crédit) puisse être valablement conclu.

Le Code annoté des crédits aux consommateurs ajoute, relativement à l'article VII.76 du CDE[42], que, si l'identité du consommateur a été usurpée, celui-ci ne sera en tout état de cause pas tenu par les termes du contrat

[37] Ombudsfin constate qu'une telle livraison a même été effectuée plusieurs jours après que le commerçant ait confirmé à la victime que les articles ne seraient pas livrés.
[38] A noter que Buy Way conteste ce libellé et soutient que l'action itsme est libellée « *Buy Way Ouverture Mastercard* ». Ce n'était pas le cas selon nos constatations dans les dossiers dont nous avons eus à connaître.
[39] Plus précisément, par OneSpan, un prestataire de service auquel Buy Way a recours.
[40] Face au nombre croissant de dossiers soumis à Ombudsfin, nous avons soumis l'un d'eux à notre Collège d'experts. L'avis de notre Collège d'experts est reproduit sur notre site web.
[41] Face au nombre croissant de dossiers soumis à Ombudsfin, nous avons soumis l'un d'eux à notre Collège d'experts. L'avis de notre Collège d'experts est reproduit sur notre site web.
[42] Consultable ici.

et pourra, le cas échéant, s'il démontre un défaut de vérification dans le chef du prêteur, mettre en cause sa responsabilité afin d'obtenir l'indemnisation de son préjudice.

En l'occurrence, selon la procédure mise en place par Buy Way, tant la demande de crédit que le contrat de crédit sont signés d'une seule traite dans une session de signature préalablement ouverte par le biais d'un code de vérification unique contenu dans un SMS envoyé à la victime (voire même au fraudeur avant fin décembre 2024) (*cf.* point 4.2.1.2).

De notre point de vue, une telle signature, qui ne constitue pas une signature électronique qualifiée, ne permet pas de garantir ni l'identité du demandeur de crédit, ni son consentement sur le contenu du contrat de crédit, ni l'intégrité de celui-ci.

Dès lors que cette signature électronique ne satisfait pas[43] au prescrit de l'article VII.78, §1er, al. 4 du CDE[44], le contrat de crédit conclu frauduleusement doit être annulé. Bien que l'annulation implique en principe une obligation de restitution réciproque, étant donné que la victime de la fraude n'a pas reçu la moindre somme, elle ne peut être tenue à restitution.

Par conséquent, la signature électronique utilisée satisfait aux exigences de l'article VII.78, § 1, quatrième alinéa, puisqu'elle garantit l'identification des parties contractantes.

4.2.2.2. Collecte des informations et évaluation de la solvabilité du demandeur de crédit

Les articles VII.69 et VII.77 du CDE prévoient les obligations incombant à la fois au prêteur et à l'intermédiaire de crédit en ce qui concerne (i) la collecte des informations nécessaires à l'appréciation de la situation financière et des facultés de remboursement du demandeur de crédit et (ii) l'évaluation de sa solvabilité.

Selon les guidelines du SPF Economie[45] et la jurisprudence de la C.J.U.E.[46], de simples déclarations non-corroborées du demandeur de crédit ne peuvent pas être considérées suffisantes si elles ne s'accompagnent pas de pièces justificatives (par exemple en ce qui concerne les revenus).

Par ailleurs, le prêteur a une obligation de vérification raisonnable en matière de crédit à la consommation. Cette obligation existe quel que soit le montant du crédit même s'il est exact qu'un contrôle plus souple est possible pour les crédits inférieurs à 3.000 EUR). Pour une analyse complète de ce point, voy. l'avis du Collège.

Or, Buy Way s'est contentée des seules déclarations unilatérales non-documentées du demandeur de crédit (soit le fraudeur), sans exiger le moindre justificatif, y compris lorsque celles-ci étaient en contradiction avec les informations dont elle disposait déjà (i.e. lorsque la victime était déjà cliente auprès d'elle) et/ou avec la Centrale des Crédits aux Particuliers (ci-après la « CCP »).

Buy Way s'est défendue en soutenant qu'elle retenait les informations les moins favorables au consommateur en cas de divergence entre les déclarations et les informations glanées dans ses registres et la CCP. Ombudsfin a toutefois observé que, dans différents cas, les victimes étaient vulnérables et dans une situation financière précaire. Dans ces cas, Ombudsfin se serait attendu à ce que des justificatifs et/ou éléments complémentaires soient demandés avant d'accorder le crédit (le cas échéant).

En outre, dans bon nombre de dossiers examinés par Ombudsfin, deux crédits étaient conclus successivement et très rapidement (à quelques minutes voire secondes d'intervalle), ce qui était en soi assez suspect mais il n'a pas été tenu compte de ce comportement par Buy Way. Pourtant, selon les Guidelines du SPF Economie précitées (p. 16), la souscription de plusieurs crédits endéans un laps de temps inférieur à un an peut à tout le moins être révélatrice d'un début de surendettement[47]. A défaut pour elle de tout simplement bloquer toute nouvelle demande de crédit après qu'une précédente demande ait été acceptée le même jour, l'on aurait été en droit d'attendre de Buy Way qu'elle prenne contact avec la victime dont elle connaissait le numéro de GSM (à partir de la fin décembre 2024), mais elle ne l'a pas fait.

[43] Selon Buy Way, l'article VII.78, §1er, al. 4du CDE distingue deux types de signatures électroniques : (i) la signature électronique qualifiée, et (ii) la signature électronique permettant de garantir l'identité des parties. Buy Way estime dès lors que le processus de signature mis en place repose sur une authentification forte via itsme, ce qui permet de garantir de manière fiable l'identité du signataire..

[44] Par contraste, d'autres prêteurs en crédits à la consommation et hypothécaires exigent à chaque étape et pour chaque document à signer, une signature électronique distincte (par exemple via une action itsme ou via un code de réponse généré au moyen du digipass, de la carte et du code PIN).

[45] Guidelines du SPF Economie relatives à l'évaluation de la solvabilité du consommateur dans le cadre de l'octroi d'un crédit à la consommation du 4 juillet 2022, p. 5, https://economie.fgov.be/fr/themes/entreprises/guidance/entreprises-de-service/evaluer-la-solvabilite-du.

[46] C.J.U.E., C-449/13 Consumer Finance, 18 décembre 2014. .

[47] Quand bien même les crédits auraient des objets et buts différents les uns des autres.

4.2.2.3. Mise à disposition du montant du crédit

Selon l'article VII.90, §1er du CDE, le montant du crédit ne peut être mis à disposition du consommateur tant que le contrat de crédit n'a pas été signé par toutes les parties.

Si le prêteur devait mettre les fonds à disposition du consommateur en violation de cet article, ce dernier ne pourrait être tenu de rembourser le crédit ou de restituer le bien livré (article VII.198 du CDE).

Ombudsfin constate dans les dossiers qui lui ont été soumis qu'un document écrit mentionnant les modalités de financement et le prix d'achat des articles commandés auprès du commerçant et payé par le biais de l'ouverture de crédit a été signé par le consommateur avant que le contrat de crédit n'ait été signé par Buy Way.

En revanche, le moment exact de la libération des fonds par Buy Way n'est pas clairement précisé et les modalités de paiement de l'achat non plus, malgré les demandes d'Ombudsfin. Buy Way soutient que les fonds sont libérés au moment de la signature par elle du contrat de crédit, mais ne nous en fournit pas la preuve technique.

4.2.2.4. Conclusion

Dans tous les dossiers soumis à notre examen, nous avons considéré que Buy Way devait intervenir dans le préjudice subi par les plaignants en annulant le crédit et supprimant le fichage des emprunteurs au volet négatif de la CCP.

Buy Way n'a malheureusement pas accepté de suivre notre raisonnement, ce que nous regrettons vivement.

Ajoutons encore que, dans quelques dossiers, nous avons dû rappeler à Buy Way qu'aucune mesure de recouvrement ne pouvait être prise ou poursuivie pendant toute la durée de la procédure de médiation.

Buy Way a reconnu cette problématique et sa responsabilité dans ces dossiers et a accordé une compensation financière substantielle aux consommateurs concernés afin de les indemniser pour le désagrément subi.

4.2.3. Modifications par Buy Way suite à notre intervention

Des modifications ont été apportées par Buy Way à sa procédure de demande et d'octroi d'ouvertures de crédit depuis le début de la vague de crédits frauduleux dont elle a eu à connaître.

4.2.3.1. Modification du libellé du SMS envoyé

Buy Way a modifié le libellé du SMS contenant le code de vérification courant juin 2025. Toutefois, celui-ci nous apparaît encore plus opaque qu'auparavant. Comme évoqué au point 4.2.1.2., cette modification n'a malheureusement pas eu l'effet escompté.

Ombudsfin a dès lors enjoint Buy Way à revoir ce libellé.

Cependant, Buy Way déclare que, en raison de contraintes techniques par rapport au nombre de caractères pouvant être contenus dans ce SMS, elle ne peut y stipuler à quoi le code de vérification sert (l'ouverture de ce qu'elle appelle une « session de signature ») et dans quel contexte il est envoyé (une demande d'ouverture de crédit de 2.500 EUR).

Pourtant, de l'avis d'Ombudsfin, ce n'est que via un libellé totalement clair que le consommateur pourrait être adéquatement informé et conscient de la procédure de demande de crédit dans laquelle il s'engage.

Selon l'expérience d'Ombudsfin, tout SMS envoyé contenant un code doit préciser de manière claire le but auquel celui-ci est assigné. Or, en l'espèce, n'étaient pas mentionnés : le type de contrat de crédit, le montant du crédit et les modalités et but du crédit.

4.2.3.2. Blocage des demandes de crédit successives

Dans la première partie des dossiers dont nous avons eu à connaître, le fraudeur avait quasi systématiquement demandé et conclu deux ouvertures de crédit de 2.500 EUR chacune.

Courant 2025, nous avons constaté que les plaintes reçues par Ombudsfin ne portaient plus que sur une seule ouverture de crédit.

Buy Way nous a confirmé avoir bloqué la possibilité de soumettre et obtenir plusieurs crédits successivement via le même canal à partir du 15 janvier 2025, ce qui a permis de limiter le préjudice total subi par chaque victime.

4.2.3.3. Utilisation d'un module d'open banking

Le 4 août 2025, Buy Way a mis en place un module *d'open banking*[48] lui permettant, dans le cadre de l'examen d'une demande de crédit, d'accéder aux informations bancaires du consommateur soit via son application bancaire, soit via son homebanking (auxquels il devra se connecter).

Buy Way a ainsi l'occasion de vérifier la solvabilité du consommateur sur base de ses données bancaires réelles (revenus et charges récurrentes) en les confrontant aux données enregistrées par la BNB.

Cette modification oblige le consommateur à se connecter à son profil bancaire. Cette étape supplémentaire constitue un obstacle pour le fraudeur, qui n'a en principe pas accès audit profil.

Selon Buy Way, plus aucune fraude de ce type n'a été commise depuis cette date, ce qui semble compréhensible vu la nécessité pour le demandeur de crédit de se connecter à son application bancaire ou son homebanking personnel. Ombudsfin s'en réjouit et peut confirmer n'avoir, à la date du présent rapport, pas reçu de dossiers pour des faits postérieurs au 4 août 2025.

4.2.4. Restez vigilants !

Ces conseils de bon sens peuvent vous être utiles :

- Toujours vérifier attentivement le libellé de toute action itsme que vous êtes invité à valider. Il est très généralement indiqué l'objet ou la conséquence de l'action itsme dans son libellé.
  Une action itsme sert soit à s'identifier, soit à signer une opération. Il est rare de devoir valider une action sans être soi-même à l'origine de la demande de validation ; si c'est tout de même le cas, cela implique qu'un tiers est derrière cette demande de validation.
  Si le libellé de l'action itsme ne correspond pas à l'objectif recherché ou fait référence à une entreprise différente de celle concernée, mieux vous tout simplement s'abstenir de la valider !

- Toujours lire attentivement le libellé de tout SMS reçu. Si ce SMS contient un code de sécurité, d'activation ou de vérification, il ne faut jamais le communiquer à un tiers mais au contraire le garder confidentiel.

[48] *L'open banking* désigne le partage sécurisé de données financières entre les institutions financières (et possiblement des tiers) auquel le consommateur a donné son consentement.

5. CREDITS **HYPOTHECAIRES**

5.1. Réduction conditionnelle du taux d'intérêt débiteur et perte de cette réduction

Dans ce type de dossiers, un contrat de crédit est conclu moyennant un taux d'intérêt plus avantageux mais conditionné au respect de diverses conditions précisées dans le contrat par le prêteur, par exemple l'obligation pour l'emprunteur de conclure une assurance solde restant dû, une assurance incendie auprès d'un tiers désigné par le prêteur, une assurance-caution ou ouvrir un compte courant. Souvent, les emprunteurs se plaignent lorsqu'après analyse du marché, ils concluent par exemple le contrat d'assurance solde restant dû ou une assurance incendie auprès d'un autre fournisseur pratiquant des prix moins élevés que celui désigné et perdent ainsi la réduction de leur taux.

Il appartient à Ombudsfin d'expliquer aux plaignants que l'article VII.147 du Code de droit économique permet cette pratique, à titre d'exception, dans le cadre d'une vente groupée (telle que définie à l'article I.9, 89° du Code de droit économique) et qu'il convient de vérifier si tel est bien le cas. Si le prêteur impose une telle condition, celle-ci et les conséquences de la cessation de son respect devront être précisées dans le formulaire « Informations européennes standardisées » (ESIS) et dans le contrat de crédit, conformément à l'article VII.129, al. 2, 4° du CDE. Ombudsfin contrôle si les dispositions du contrat de crédit sont suffisamment claires (i) quant aux obligations qui incombent à l'emprunteur (de souscrire une assurance solde restant dû, assurance incendie auprès du tiers désigné, assurance caution, ouverture d'un compte courant) pour pouvoir bénéficier d'une réduction conditionnelle du taux d'intérêt débiteur applicable au crédit et (ii) quant au fait que le non-respect des conditions entraînerait la perte du droit à la réduction conditionnelle du taux d'intérêt.

La réduction conditionnelle du taux d'intérêt débiteur n'est maintenue qu'aussi longtemps que la condition prévue est respectée. Lorsque cela n'est plus le cas, le taux d'intérêt débiteur peut être porté à son taux de base.

Dans d'autres dossiers, la banque a toutefois appliqué le taux réduit alors que la condition prévue pour en bénéficier n'était pas remplie. La banque s'en rend compte après un certain temps (parfois un ou deux ans) et décide alors de mettre fin au taux réduit pour le futur. Les plaignants s'en émeuvent, estimant que le comportement de la banque pendant tout ce temps équivaut à renonciation à la condition posée dans le contrat.

Ombudsfin observe qu'après la déchéance du bénéfice de la réduction, quand bien même la condition prévue viendrait à être (à nouveau) remplie dans le futur, les banques ont de moins en moins tendance à accepter de réappliquer la réduction conditionnelle, ce qui est effectivement leur droit.

Rappelons toutefois que, depuis le 1er juin 2024, une nouvelle loi en Belgique limite la "vente groupée" pour les crédits hypothécaires. Les emprunteurs peuvent changer d'assurance solde restant dû (ASRD) ou d'assurance incendie après un tiers de la durée du prêt sans perdre leur taux réduit.

5.2. Révision du taux d'intérêt débiteur

Dans ces dossiers, le contrat de crédit a été conclu moyennant un taux d'intérêt débiteur variable. Si la formule de variabilité est, comme il se doit, précisée dans ledit contrat (par exemple les formules dites « 5-5-10 »), il convient également de tenir compte de l'article VII.143 du Code de droit économique qui détaille les modalités qui doivent être indiquées dans le contrat de crédit. En cas de contestation sur le taux révisé, Ombudsfin s'attache à vérifier si toutes ces modalités ont été prévues et respectées et vérifie la formule de calcul ainsi que les taux de base et plafonds appliqués au taux. Ombudsfin constate que, dans la grande majorité des cas, le nouveau taux appliqué est correct mais que le plaignant n'a pas compris les explications qui lui avaient été fournies lors de la conclusion du contrat ou lors de la communication du nouveau taux applicable par le prêteur.

5.3. Conversion d'un mandat hypothécaire

A l'instar d'une prise d'hypothèque (impliquant une inscription hypothécaire), un mandat hypothécaire a pour objet de garantir la créance du prêteur sur l'emprunteur. Le mandat hypothécaire présente, pour l'emprunteur, l'avantage d'être moins coûteux lors de sa conclusion puisque les frais sont nettement moins importants que lors d'une inscription hypothécaire. Il est courant qu'un prêteur prenne une inscription hypothécaire en premier rang sur l'immeuble donné en garantie et accorde parallèlement un mandat pour le surplus emprunté afin que le coût soit moins important pour son client. C'est une forme de geste commercial qui peut toutefois entraîner des surprises désagréables par la suite car ce mandat peut être converti à tout moment en inscription hypothécaire par le prêteur. Lorsque le mandat est converti, les frais encourus lors de cette conversion (acte notarié et inscription hypothécaire) sont à charge de l'emprunteur. Le plaignant s'adresse alors à Ombudsfin pour obtenir la restitution des frais de conversion débités de son compte courant en estimant que cette conversion n'est pas justifiée.

La situation classique dans laquelle la banque décide de faire convertir le mandat hypothécaire que l'emprunteur a consenti à son profit en inscription hypothécaire pour augmenter ses garanties est la détérioration de la situation financière de l'emprunteur, le plus souvent matérialisée par des retards de paiement.

Dans ce cas, le prêteur commence par adresser des rappels de paiement mais lorsque la situation n'est pas totalement régularisée et qu'aucun élément permettant de rassurer le prêteur à propos d'un remboursement rapproché ou d'une restauration de la situation financière de l'emprunteur ne lui a été adressé, le prêteur est en droit de décider de faire exécuter sans délai un mandat d'hypothéquer et ce sans en aviser préalablement l'emprunteur. Ce droit discrétionnaire tient à la nature de « pré-garantie » du mandat d'hypothéquer et à la politique de gestion des risques, politique qu'Ombudsfin n'a pas le pouvoir d'apprécier sous réserve de l'existence d'un abus de droit. Ombudsfin examine ainsi quel risque accru a précisément conduit le prêteur à prendre la décision de convertir le mandat hypothécaire (dans son intégralité). Si Ombudsfin estime que la détérioration présumée de la situation financière de l'emprunteur (mandant) est contestable, il exigera le remboursement de tous les frais de conversion. Si la détérioration de la situation du mandant est avérée, Ombudsfin vérifiera si le montant converti du mandat ne dépasse pas le capital restant dû. Si le montant du mandat excède manifestement le montant du capital restant dû, Ombudsfin demandera, généralement avec succès, à la banque de prendre à sa charge la partie des coûts qui aurait pu être évitée si la conversion s'était limitée au montant restant à rembourser au moment de la conversion. Ajoutons toutefois que l'existence d'autres garanties comme la cession de rémunération, ne fait pas obstacle à la conversion du mandat.

5.4. Crédit-pont

Dans ces dossiers, un crédit-pont est généralement conclu pour permettre au plaignant de bénéficier d'une période « tampon » entre le financement d'un nouveau bien acquis et la vente d'un ancien immeuble. Ce type de crédit permet au plaignant, pendant une durée courte et déterminée, de payer uniquement les intérêts du crédit pendant cette période et de rembourser le crédit en totalité (capital et intérêts) lorsqu'il perçoit le produit de la vente de son ancien immeuble et ce au plus tard à l'échéance contractuelle de ce crédit-pont. Ce type de crédit peut parfois être prolongé mais cette prolongation n'est pas automatiquement accordée par le prêteur. Elle doit être demandée par écrit, avant l'échéance du crédit-pont et motivée par exemple en produisant un compromis de vente signé. Elle n'est accordée que dans certains cas, après analyse par le prêteur.

Dans de nombreux dossiers, le plaignant demande cette prolongation oralement ou trop tard, ne produit aucun compromis ou rembourse le crédit avec quelques jours ou semaines de retard, pensant échapper aux sanctions. Ombudsfin tente dans certains cas exceptionnels d'obtenir un accord mais doit constater que les prêteurs ne pratiquent pas la tolérance en cette matière et dénoncent les crédits à leur échéance lorsqu'ils sont impayés, conformément aux dispositions contractuelles du crédit-pont. Ceci entraine l'imputation de frais supplémentaires et d'intérêts de retard et le fichage négatif à la Centrale des Crédits aux Particuliers (en abrégé la "CCP") à la Banque Nationale Belge. Dans la plupart des cas, Ombudsfin n'est pas en mesure de trouver une solution favorable et ne dispose pas d'arguments pour obtenir la suppression du fichage négatif.

6. INVESTISSEMENT

6.1. Gestion des attestations fiscales et prévention de la double imposition

Dans le cadre des conventions préventives de la double imposition conclues entre États, les établissements financiers sont tenus de s'assurer, au moment du paiement des revenus, que les conditions permettant l'application d'une exonération ou d'un taux réduit de retenue à la source sont effectivement remplies. À défaut de disposer de documents fiscaux valides et à jour, ils doivent appliquer la retenue prévue par la législation nationale.

En pratique, cette exigence se traduit par la demande, auprès des clients non-résidents, d'une attestation fiscale périodique, généralement sous la forme d'une auto-certification établie et signée par le bénéficiaire effectif des revenus. Si d'autres documents, tels que des attestations émanant d'un employeur ou d'une autorité tierce, peuvent constituer des éléments justificatifs utiles, ils ne dispensent pas nécessairement de la remise d'une attestation conforme aux exigences propres de l'établissement financier et aux directives des autorités fiscales compétentes.

Un dossier soumis à Ombudsfin a montré que l'absence de renouvellement, dans les délais requis, de l'attestation fiscale exigée par l'institution financière a conduit à l'application du précompte mobilier belge pour une période déterminée. D'un point de vue juridique, cette pratique ne peut être considérée comme irrégulière dès lors qu'elle découle des obligations légales de la banque et de l'absence, à la date pertinente, de documents fiscaux valides dans le dossier du client. La restitution d'un précompte indûment perçu relève, dans une telle situation, de la compétence exclusive de l'administration fiscale.

Ce cas met toutefois en évidence l'importance d'une communication claire, transparente et suffisamment étalée dans le temps à destination des clients. Une information précise sur la durée de validité des attestations requises, sur leur caractère indispensable et sur la nécessité de leur renouvellement périodique est essentielle afin de prévenir les incompréhensions et les conséquences financières qui peuvent en découler.

Dans ce contexte, Ombudsfin a recommandé à l'institution financière de renforcer ses pratiques d'information, notamment en mentionnant explicitement la durée de validité des attestations fiscales concernées et en multipliant les rappels à l'approche de leur expiration. L'acceptation de ces recommandations par la banque témoigne d'une volonté d'amélioration continue de ses procédures et contribue à une meilleure protection des clients dans un environnement fiscal de plus en plus complexe et internationalisé.

7. SERVICE BANCAIRE **DE BASE**

7.1. Consommateurs

En 2025, Ombudsfin a dû examiner 5 dossiers concernant le refus de la banque d'accorder un service bancaire de base à un consommateur. Nous rappelons que les avis d'Ombudsfin en la matière ont un caractère contraignant.

Ombudsfin a jugé 3 dossiers fondés. Dans ces dossiers, Ombudsfin a donc demandé à la banque d'accorder tout de même le service bancaire de base. La banque a finalement accepté de le faire dans chacun de ces dossiers.

2 des 3 dossiers concernaient le même problème au sein d'une même banque, à savoir la langue du consommateur, qui n'était pas une langue dans laquelle cette banque, conformément à ses conditions générales, communique avec ses clients. La banque doutait dès lors de la validité du consentement au contrat.

Bien que le demandeur ait été assisté par un interprète, ce qui garantissait suffisamment qu'il comprenait les implications de son engagement, la banque concernée a initialement refusé la demande par principe. Ombudsfin a toutefois estimé que la discrimination fondée sur la langue pratiquée par cette banque viderait complètement de sa substance le droit à un service bancaire de base tel que prévu et souhaité par le législateur.

La personne concernée remplissait toutes les conditions pour bénéficier d'un service bancaire de base. Seule la langue posait donc problème à la banque.

Or, la langue n'est en aucun cas une condition d'accès au service bancaire de base, ni un motif de refus prévu par la loi. Le fait que la banque exige la maîtrise d'une langue spécifique, même pour un service bancaire de base, est contraire aux dispositions impératives du Code de droit économique, qui ont été créées pour offrir aux personnes résidant légalement dans le pays la possibilité, voire le droit, de bénéficier d'une série spécifique de services bancaires de base.

Ombudsfin a insisté auprès de la banque pour qu'elle ne fasse pas de discrimination linguistique dans ce contexte.

La banque a finalement accepté d'ouvrir le service bancaire de base à condition de faire appel à un interprète.

7.2. Entreprises

Contexte général

Tout d'abord, rappelons que le service bancaire de base pour les entreprises a été introduit afin d'éviter que ces dernières ne soient exclues des services bancaires et de leur permettre de poursuivre leurs activités. Il s'agit d'un droit à un service minimal : l'accès à un compte de paiement et aux opérations les plus essentielles qui y sont liées.

Les dossiers spécifiquement soumis à Ombudsfin sont ceux dans lesquels les entreprises peuvent présenter une décision positive de la chambre du service bancaire de base, mais dans lesquels le prestataire de services bancaires de base désigné refuse finalement d'accorder le service bancaire de base. Les décisions d'Ombudsfin en la matière ont un caractère contraignant ; Ombudsfin peut donc obliger la banque à fournir le service bancaire de base, comme le prévoit le Code de droit économique.

Dans ces dossiers, nous constatons souvent que le refus fait suite à l'évaluation des informations et documents complémentaires que la chambre du service bancaire de base demande à l'entreprise dans sa décision et transmet au prestataire de services bancaires de base désigné et/ou que le prestataire de services bancaires de base désigné demande lui-même après la décision de la chambre du service bancaire de base.

Parfois, le prestataire de services bancaires de base ne reçoit pas toutes les données (et l'entreprise ne

comprend pas bien quelles données sont exactement nécessaires et pourquoi), parfois, le prestataire de services bancaires de base estime que l'évaluation des données fournies l'oblige à refuser le service bancaire de base.

Le refus est souvent lié à l'incapacité de satisfaire aux obligations fondamentales prévues par la législation anti-blanchiment ou à des motifs de refus expressément prévus (tels que l'existence d'une certaine condamnation ou le non-respect par l'entreprise des mesures spécifiques de limitation des risques prévues par l'arrêté royal).

Il est établi que le contrôle du contenu des informations et des documents supplémentaires fournis incombe au prestataire de services bancaires de base et que ce contrôle peut, dans certaines circonstances, aboutir à un refus, malgré une décision positive de la chambre des services bancaires de base. La chambre du service bancaire de base ne procède pas à une telle analyse de ces documents et informations qui, en principe, peuvent être considérés comme faisant partie du dossier global des services bancaires de base.

Nous devons constater que cette nuance n'est pas toujours claire pour l'entreprise et que la décision positive de la chambre du service bancaire de base est considérée par l'entreprise comme une décision définitive dont le prestataire de services bancaires de base ne peut en aucun cas s'écarter. Il serait bon que la chambre du service bancaire de base communique plus clairement à ce sujet, d'autant plus que les dossiers soumis à Ombudsfin montrent que certains prestataires de services bancaires de base fondent à juste titre leur refus sur des motifs de refus expressément prévus par la loi ou l'arrêté royal (qui peuvent être invoqués sur la base de l'évaluation des données supplémentaires obtenues).

Dans ce contexte, 5 des 9 dossiers soumis à Ombudsfin ont donc été jugés non fondés par Ombudsfin. Nous avons estimé ne pas pouvoir contester la décision de refus.

3 autres dossiers étaient toutefois fondés. Ombudsfin a alors émis un avis contraignant demandant l'octroi du service bancaire de base. Dans 2 dossiers, la banque a accepté de le faire après l'intervention d'Ombudsfin. Dans 1 dossier, la banque a continué à refuser de le faire.

Un avis contraignant non suivi par l'institution financière

Dans ce dossier où l'avis d'Ombudsfin n'a pas été suivi, l'entreprise contestait la décision de refus de la banque, désignée par la chambre du service bancaire de base comme prestataire de services bancaires de base pour les comptes de 2 sociétés.

Ombudsfin a estimé, pour l'une des sociétés, que la décision de refus de la banque pouvait être comprise, sur la base d'une mention de l'entrepreneur sur la liste des sanctions de l'OFAC en raison d'une activité bien définie qui est également visée et sanctionnée au niveau européen.

En ce qui concerne le service bancaire de base demandé pour l'autre société, Ombudsfin a estimé que la banque devait bien accorder ce service. Malgré le caractère contraignant de notre avis, la banque a refusé de se conformer à cette dernière décision.

Deux procédures en cours devant le Conseil d'État

Dans le dossier évoqué aux alinéas précédents, l'entreprise a introduit, en ce qui concerne la première décision (confirmation du refus), une procédure en annulation contre Ombudsfin devant le Conseil d'État, qui est actuellement toujours pendante. Dans un premier temps, l'entrepreneur a tenté d'obtenir la suspension de la décision dans le cadre d'une procédure d'urgence devant le Conseil d'État, mais celui-ci a estimé que l'urgence n'était pas démontrée. Après cet arrêt négatif, l'entrepreneur a poursuivi la procédure d'annulation.

L'autre procédure a été engagée par une banque (elle a déjà été mentionnée dans le rapport annuel précédent). La banque contestait l'avis contraignant rendu par Ombudsfin selon lequel elle ne pouvait refuser le service bancaire de base. Aucune décision n'a encore été rendue dans cette procédure.

8. COLLABORATION

8.1. Belgique

8.1.1. Service de Médiation pour le Consommateur

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

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

8.1.2. OMBUDSMAN.BE

L'ombudsman fait partie d'Ombudsman.be, le réseau belge des médiateurs. Celui-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 sont disponibles sur le site www.ombudsman.be

8.2. Europe

8.2.1. 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.

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

Ombudsfin participe activement aux deux réunions FIN-NET organisées chaque année par la Commission européenne.

1. Procédure pour les plaintes transfrontalières

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 dans la plupart des cas 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.

2. Exemples concrets

En 2025, Ombudsfin n'a reçu aucun dossier dans lequel la procédure FIN-NET a dû être utilisée.

8.3. 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, voir : www.networkfso.org.

9. MOYENS **FINANCIERS**

Au moment de la publication du rapport annuel 2025, les comptes annuels de l'exercice comptable d'Ombudsfin asbl de 2025 n'avaient pas encore été approuvés par l'assemblée générale. Dès que ceux-ci l'auront été, 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).

Vous trouverez toutefois ci-dessous un aperçu du budget établi pour 2025 :

	Budget 2025
Revenus	
Cotisation fixe membres Ombudsfin asbl	795.832,18
Cotisation variable membres Ombudsfin asbl	898.320,00
Produits financiers	5.000,00
Dépenses	**1.699.152,18**
Frais de personnel + honoraires	1.481.300,00
Frais de fonctionnement	162.650,00
Moins-values factures impayées + notes de crédits	10.000,00
Compensation du résultat négatif de l'exercice 2023	45.202,18
Dépenses totales	**1.699.152,18**

Lors du calcul et de l'approbation du budget, il doit toujours être 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 (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 et des rappels (en cas d'absence de réponse aux demandes d'Ombudsfin dans les délais prévus) au cours de l'année civile précédente.