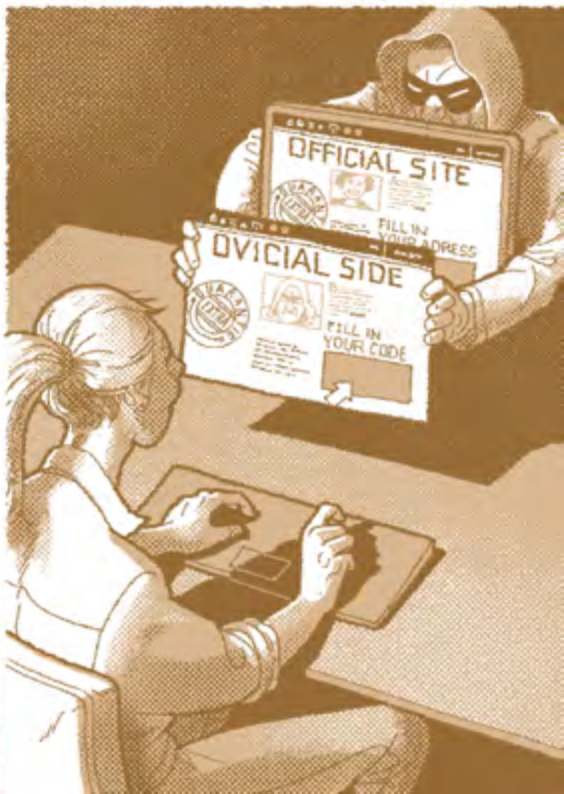


OMBUDSFIN

JAARVERSLAG 2022

Overzicht

VOORWOORD

Dames en heren,

Met de lente breekt een nieuwe periode van jaarverslagen aan. Ook Ombudsfin ontsnapt hier niet aan !

In dit jaarverslag zult u lezen dat we opnieuw een verhoging van dossiers hebben gekend in 2022 : een verhoging van 11,5% voor de ingediende dossiers en van 9% voor de ontvankelijke dossiers.

Zoals in de voorgaande jaren, is online fraude met grote voorsprong het belangrijkste thema : niet minder dan 967 online fraudedossiers zijn door Ombudsfin geanalyseerd (tegenover 658 in 2021).

Het moet opgemerkt worden dat de standpunten van Ombudsfin en de financiële instellingen in deze dossiers in 2022 niet veel dichter bij elkaar zijn gekomen: laatstgenoemden bleven zich in veel gevallen beroepen op de grove nalatigheid van de consument om een tussenkomst te weigeren, waardoor het aantal dossiers waarin een evenwichtige oplossing kon worden gevonden, in het algemeen afnam.

Wij kunnen deze situatie, die een aantal burgers ontredderd en, in sommige gevallen, in dramatische financiële situaties achterlaat, uiteraard alleen maar betreuren.

Men kan de financiële instellingen in elk geval niet verwijten niets te ondernemen in de strijd tegen dit fenomeen: er worden steeds meer bewustmakingscampagnes gevoerd, zeer concrete initiatieven zijn genomen (op punt stellen van een telefonische hulplijn die 24u/24, 7d/7 bereikbaar is, verzending van sms-berichten om de consumenten te waarschuwen voor de installatie van een aan hun rekening gekoppelde applicatie, enz.). De fraudeurs worden echter steeds professioneler. De maatregelen volstaan niet om dit opkomende fenomeen een halt toe te roepen.

Het grootste deel van dit verslag is aan deze problematiek gewijd. U vindt in dit verslag een uitgebreide analyse van de problemen die wij tegenkomen en de redenering die wij volgen in de aan ons toevertrouwde dossiers.

De dossiers met andere thema's, waarin het gelukkig veel gemakkelijker is om een evenwichtige oplossing te vinden (meer dan 93% succespercentage), worden geenszins vergeten. In het verslag kunt u lezen welke types klachten in 2022 populair waren.

Rest mij u nog enkel een goede lezing van dit jaarverslag toe te wensen en te hopen dat 2023 eerder een jaar van daling dan van nieuwe records wordt.

Jean Cattaruzza
Ombudsman

MISSIE OMBUDSFIN

Ombudsfin is een gekwalificeerde entiteit volgens artikel XVI.24 van het Wetboek Economisch Recht. Het doel van Ombudsfin is om geschillen tussen financiële instellingen en consumenten op een buitengerechtelijke manier af te handelen. Dit gebeurt door het verstrekken van advies en aanbevelingen over het betreffende geschil en door op te treden als ombudsman.

Naast geschillen tussen financiële instellingen en consumenten kan Ombudsfin ook in bepaalde geschillen tussen financiële instellingen en ondernemingen tussenkomen. Door het bieden van een onpartijdige en effectieve oplossing voor geschillen draagt Ombudsfin bij aan het vertrouwen van de consument en ondernemingen in de financiële sector.

Wie kan een klacht indienen?

Elke klant van een Belgische bancaire financiële instelling of tussenpersoon, die handelt als natuurlijke persoon in het kader van zijn privé-belangen kan een beroep doen op Ombudsfin wanneer hij geen voldoening heeft bekomen.

Ook ondernemingen kunnen voor bepaalde klachten terecht bij Ombudsfin. Het moet daarbij gaan om klachten in het kader van de uitvoering van een kredietcontract, om klachten die betrekking hebben op een grensoverschrijdende betaling (binnen de Europese Unie) voor een maximumbedrag van € 50.000, MIF's (aangerekende afwikkelingsvergoedingen bij betalingstransacties met kaart) of de basisbankdienst voor ondernemingen.

Hoe een klacht indienen?

De klacht moet schriftelijk worden ingediend via post, mail of via het webformulier op www.ombudsfin.be en moet duidelijk en omstandig geformuleerd en gedocumenteerd zijn. Ombudsfin stelt in dit kader op de website een indicatieve checklist ter beschikking.

De documenten kunnen als volgt worden bezorgd:

Per brief aan het adres
Ombudsfin
North Gate II
Koning Albert II-laan n°8, bus 2
1000 Brussel

Per e-mail
ombudsman@ombudsfin.be

Online op
www.ombudsfin.be

Gratis

De procedure bij Ombudsfin is gratis voor de aanvrager.

Belangrijkste ontvankelijkheidsvoorwaarden

- De financiële instelling waartegen de klacht is geformuleerd, is aangesloten bij Ombudsfin. De lijst van aangesloten instellingen en hun bevoegde diensten is terug te vinden op de website.
- De klacht is reeds schriftelijk voorgelegd aan de bevoegde dienst van de financiële instelling en het antwoord is onvoldoende of er is geen antwoord gekomen binnen een redelijke termijn (1 maand).
- De klacht werd niet langer dan één jaar geleden aan de bevoegde klachtendienst voorgelegd.
- Het geschil is niet hangende voor een rechtbank, noch bestaat hierover reeds een gerechtelijke uitspraak. Ook werd het geschil nog niet ten gronde behandeld door een andere gekwalificeerde entiteit (bv. Ombudsman van Verzekeringen).
- Het geschil betreft geen probleem van overmatige schuldenlast. Ombudsfin doet niet aan schuldbemiddeling.

Een overzicht van alle ontvankelijkheidsvoorwaarden is terug te vinden in het Procedurereglement, gepubliceerd op de website.

Hoe verloopt de behandeling van een ontvankelijk dossier concreet?

Ombudsfin stuurt het dossier vooreerst naar de financiële instelling om te informeren naar haar standpunt in de zaak.

Indien aanvullende informatie vereist is, wordt contact opgenomen met de betrokken partijen.

Na afloop van het onderzoek van de klacht en onderhandelingen, stelt de Ombudsman een advies op.

Wanneer een dossier een principekwestie of een meer complex dossier betreft, kan het dossier voor advies voorgelegd worden aan een college van experten.

Bindende kracht van de adviezen

Uitgezonderd de adviezen betreffende basisbankdienst, zijn de adviezen van de Ombudsman niet bindend. Elke partij blijft vrij om het advies al dan niet te volgen en kan, indien gewenst, het geschil voor een rechtbank brengen.

Medewerkers en raadgevers ombudsman

Voor de behandeling van de aanvragen, wordt de ombudsman bijgestaan door 3 assistenten en 7 adviseurs:

Assistenten

Serge Henris, Christel Speltens en Ingrid Vertenten (deels adviseur).

Adviseurs

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

Voor de complexe dossiers en principekwesties kan de ombudsman beroep doen op volgende colleges van experten:

College van experten

Het college is samengesteld uit permanente onafhankelijke deskundigen.

Samenstelling van het College van experten in 2022 (en tot 15 maart 2023): Françoise Sweerts (Voorzitter), Nadine Spruyt (tot eind juni 2022), Johan Vannerom, Reinhard Steennot, Alain Guigui, Philippe D'Haen, Piet François (vanaf september 2022).

De samenstelling van het college van experten vanaf 15 maart 2023: Reinhard Steennot (Voorzitter), Johan Vannerom, Alain Guigui, Philippe D'Haen, Piet François, Erik Van den Haute.

College van experten voor kredietklachten van ondernemingen

Dit college is samengesteld uit een onafhankelijke voorzitter en 2 vertegenwoordigers van ondernemingen (Unizo, FEB): Lieven Cloots en Arie Van Hoe en 2 vertegenwoordigers van de financiële sector: Luc Declercq en Wim Hendrickx.

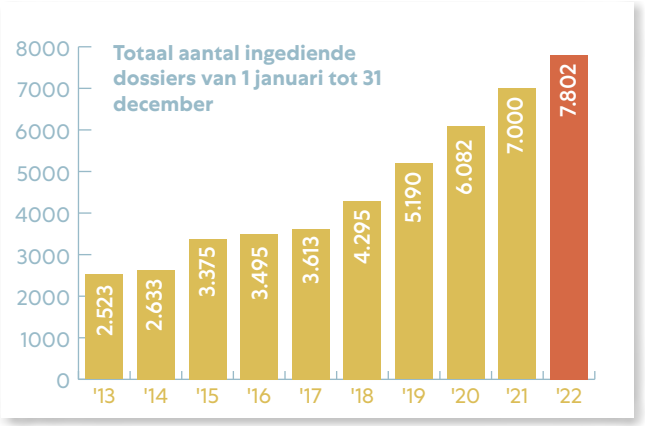
(van links naar rechts): Bérengère de Crombrugghe, Serge Henris, Elke Heymans, Jean Deschuijteneer, Vincent Chambeau, Aline Umwali, Jean Cattaruzza, Ingrid Vertenten, Brent De Waele en Christine Buisseret. Afwezig: Christel Speltens.

1. OMBUDSFIN IN CIJFERS

1.1. Stijging van het aantal ingediende aanvragen

Het totale aantal ingediende aanvragen van consumenten en ondernemingen in 2022 is 7.802. Dit betekent een stijging met 802 dossiers (11,5%) in vergelijking met 2021.

Uit onderstaande tabel blijkt een aanhoudende toename vanaf 2015, met een versnelling van deze trend in de laatste vier jaar.



Deze cijfers omvatten alle nieuwe schriftelijke informatieverzoeken en klachten die in 2022 bij Ombudsfin werden ingediend.

In elk van deze dossiers ontving de klant een antwoord van Ombudsfin of werd hij doorverwezen naar de juiste dienst indien Ombudsfin niet bevoegd was om tussen te komen.

1.2. Kwalificatie van de ingediende aanvragen

1.2.1. Klacht of informatie

Van de 7.802 nieuwe aanvragen van consumenten en ondernemingen waren er 7.616 klachten en 186 informatieverzoeken.

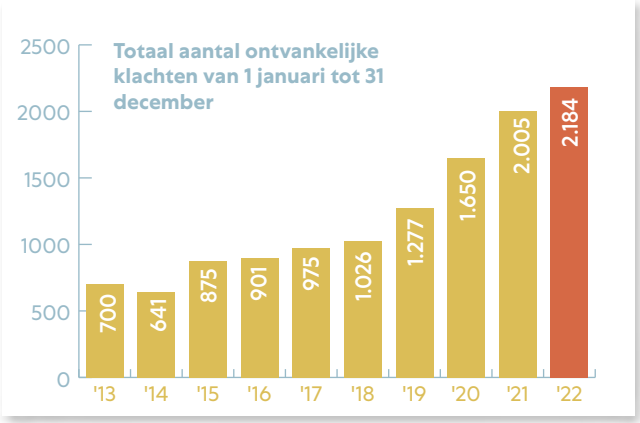
1.2.2. Ontvankelijke klachten

Ontvankelijke klachten zijn klachten waarvoor Ombudsfin de bevoegde gekwalificeerde entiteit is en waarbij voldaan is aan alle ontvankelijkheidsvoorwaarden[1].

Voor elke ontvankelijke klacht, brengt de ombudsman, na grondige analyse van de klacht en de standpunten van de partijen, en na bemiddeling, een advies uit waarin het resultaat van de bemiddeling wordt meegedeeld aan de betrokken partijen. In sommige dossiers formuleert Ombudsfin ook een aanbeveling (zie infra 2.4.).

In 2022 werden er 7.616 klachten ingediend. Van die klachten werden er 2.033 (26,7%) ontvankelijk verklaard. Naast deze klachten werden nog 1 klacht uit 2018, 3 klachten uit 2020 en 147 klachten uit 2021 aanvaard in 2022. Dat betekent dat er in totaal 2.184 klachten werden ontvankelijk verklaard in 2022.

Dit is een toename van 8,9% (of 179 klachten) in vergelijking met 2021, toen er 2.005 klachten werden aanvaard.



1 https://www.ombudsfin.be/nl/particulieren/klacht-indienen/procedure/

1.2.3. Niet-ontvankelijke klachten

Van de 7.616 klachten die in 2022 werden ontvangen, voldeden er 5.583 (of 73,3%) niet aan de ontvankelijkheidsvoorwaarden. Verzoekers werden altijd uitgebreid geïnformeerd over de redenen waarom hun aanvraag niet in behandeling kon worden genomen. Hieronder volgt een overzicht van de verschillende redenen die zijn aangevoerd met de respectievelijke aantallen voor 2022, 2021 en 2020.

Reden	Aantal 2022	Aantal 2021	Aantal 2020
Klacht nog niet voorgelegd aan bevoegde klachtendienst van de financiële instelling in eerste lijn	3.922	3.560	3.092
Klant/instelling niet identificeerbaar of voorwerp aanvraag onduidelijk	519	489	515
Ombudsfin qua materie niet bevoegd	798	671	604
Financiële instelling is niet aangesloten bij Ombudsfin (bv. invorderingsbureaus, buitenlandse financiële instellingen)	219	187	181
Combinatie van redenen vermeld in deze tabel	108	48	46
Gerechtelijke procedure of aanvraag reeds behandeld door een gekwalificeerde entiteit	3	7	8
Aanvraag meer dan 1 jaar geleden voorgelegd aan klachtendienst financiële instelling	14	6	9
Aanvraag verzonnen, kwetsend, eerrovend	0	0	0
Behandeling aanvraag zou werking Ombudsfin ernstig in het gedrang brengen	0	0	2
TOTAAL	**5.583**	**4.968**	**4.457**

Wanneer een andere dienst bevoegd was of wanneer de eerste lijn nog niet werd aangesproken en de betrokken financiële instelling gekend was, werd aan de verzoeker de contactgegevens van de bevoegde dienst bezorgd.

1.3. Behandelingstermijn ontvankelijke klachten

De gemiddelde doorlooptijd van alle in 2022 ontvankelijk verklaarde en afgesloten klachten, bedroeg 50,6 kalenderdagen. In 2021 bedroeg de gemiddelde doorlooptijd 48 kalenderdagen.

Sinds juni 2015 moet Ombudsfin als gekwalificeerde entiteit elke klacht binnen een termijn van 90 kalenderdagen behandelen. Deze termijn kan eenmalig, omwille van de complexiteit van het dossier, worden verlengd met eenzelfde periode. In 2022 werd de behandelingstermijn in 189 dossiers verlengd. Partijen werden tijdig op de hoogte gebracht van deze verlenging.

1.4. Stopzetting bemiddelingsprocedure

Tijdens de bemiddelingsprocedure zijn er 6 dossiers gestopt op verzoek van de klager. In één geval wilde de klant de relatie met de bank volledig beëindigen en alle communicatie stopzetten. In een ander geval was het probleem al opgelost en in nog een ander geval wilde de klant rechtstreeks communiceren met de bank. In de overige drie gevallen werd er geen reden gegeven voor het stopzetten van het dossier.

1.5. Betrokken financiële instellingen bij ontvankelijke klachten

Hieronder volgen de categorieën van financiële instellingen die betrokken waren bij de ontvankelijke klachten in 2022, met de concrete aantallen en percentages erbij vermeld.

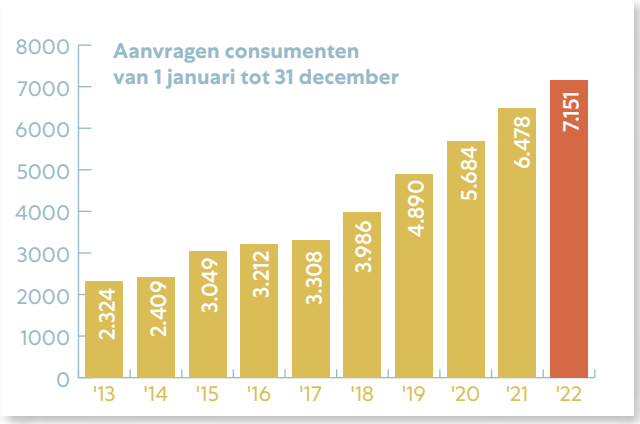
Bank	1919	87,87%
Betalingsinstelling	141	6,46%
Kredietmaatschappij	70	3,21%
Instelling voor elektronisch geld	32	1,47%
Kredietmakelaar	5	0,23%
Sociale kredietgever	5	0,23%
Beleggingsonderneming	4	0,18%
Leasingmaatschappij	3	0,14%
Asset Management	2	0,09%
Verzekeringsmaatschappij	2	0,09%
Beursvennootschap	1	0,05%
TOTAAL	**2184**	**100,00%**

2. AANVRAGEN INGEDIEND DOOR CONSUMENTEN

2.1. Stijging aantal aanvragen

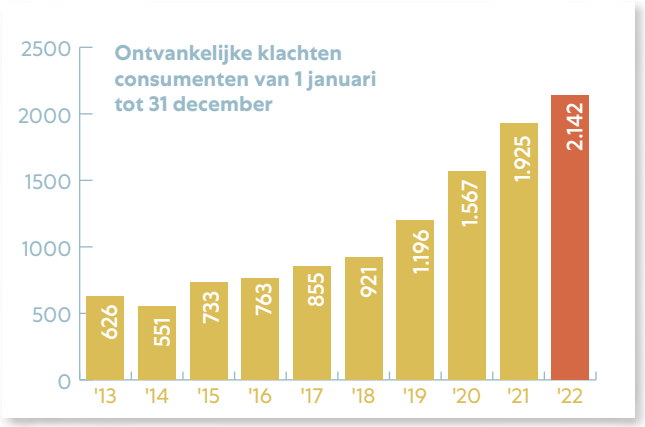
In 2022 ontving Ombudsfin 7.151 aanvragen van consumenten, tegenover 6.478 in 2021, wat overeenkomt met een stijging van 673 dossiers (10,4%) ten opzichte van 2021.

7.042 aanvragen betroffen een klacht, terwijl 109 aanvragen een vraag om informatie betroffen.



2.2. Stijging aantal ontvankelijke klachten

In 2022 registreerde Ombudsfin 2.142 aanvragen van consumenten als ontvankelijk, tegenover 1.925 in 2021, wat een toename betekent van 217 dossiers (11,3%) tegenover 2021.



2.3. Resultaten van de in 2022 afgesloten ontvankelijke klachten van consumenten

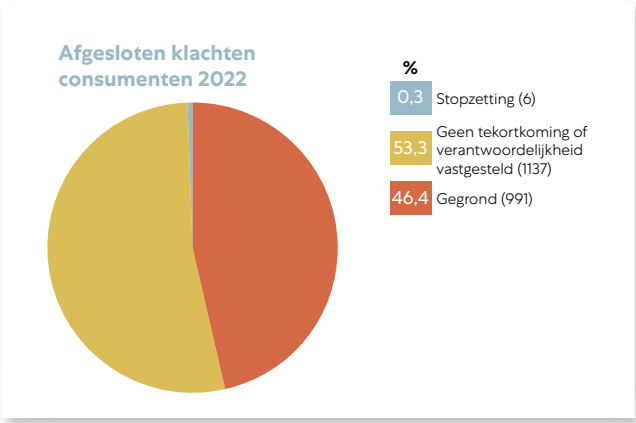
Deze resultaten hebben betrekking op alle in 2022 afgehandelde klachten van consumenten. In deze resultaten zijn dus ook klachten verwerkt die reeds vóór 2022 werden voorgelegd aan Ombudsfin.

2.134 dossiers werden afgesloten.

In 46,4% van de dossiers (of 991 dossiers) achtte Ombudsfin de klacht gegrond op basis van wetgeving, contractuele bepalingen, gedragscodes, marktpraktijken, deontologische codes of elk ander element dat dienstig was voor de beslechting van het geschil.

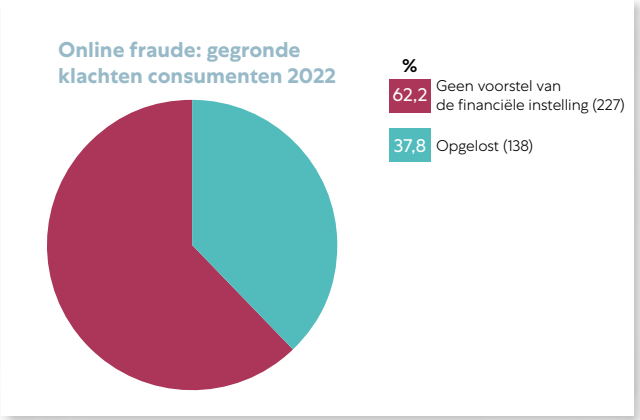
In 53,3% van de dossiers (of 1.137 dossiers) kon Ombudsfin geen tekortkoming of verantwoordelijkheid van de financiële instelling vaststellen. In deze dossiers werd de nodige bijkomende uitleg en toelichting gegeven aan de cliënt zodat die kon begrijpen waarom Ombudsfin tot dit besluit kwam en waarom dan ook geen rechtzetting of tegemoetkoming van de financiële instelling kon worden gevraagd.

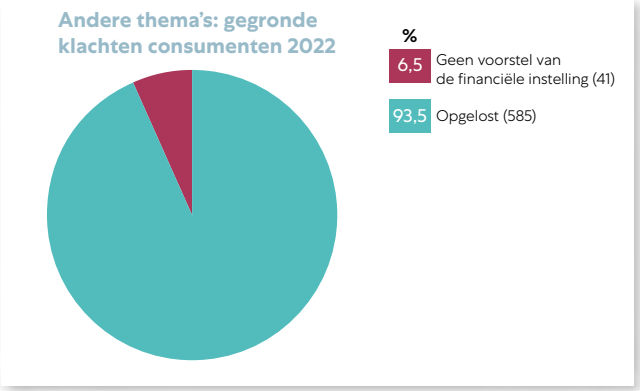
In 6 dossiers werd de bemiddelingsprocedure vroegtijdig stopgezet door de consument (0,3%).



Van de 991 klachten die Ombudsfin gegrond achtte, werd 73% (723 klachten) opgelost. Ombudsfin betreurt dit historisch lage percentage opgeloste dossiers.

Volgende grafieken tonen aan dat dit resultaat het rechtstreekse gevolg is van de bedroevende resultaten in de gegronde online fraudedossiers (phishing) en bevestigen anderzijds ook de mooie resultaten in de dossiers met andere thema's:





In online fraudedossiers valt de analyse van de ombudsman niet altijd samen met die van de financiële instellingen. Het al dan niet toegestane karakter van de frauduleuze verrichtingen wordt door de bank en door Ombudsfin af en toe verschillend beoordeeld maar het is vooral omtrent het bewijs van grove nalatigheid in hoofde van de consument dat de meningen uiteenlopend zijn.

Onze eindbeoordeling, die al dan niet leidt tot een verzoek tot tussenkomst van de bank, is gebaseerd op de analyse van alle feitelijke omstandigheden en de mate van betrokkenheid van de consument in het fraudeproces (in het bijzonder in het geval van "phishing").

2.4. Individuele aanbevelingen

Sinds juni 2015 voorziet het procedurereglement van Ombudsfin dat de ombudsman individuele aanbevelingen kan formuleren aan de financiële instellingen. Ombudsfin vraagt dan binnen de 30 dagen te reageren op de aanbeveling.

Deze aanbevelingen hebben betrekking op een concrete oplossing in een specifieke klacht of worden geformuleerd in een ruimer kader, zoals een aanpassing van procedures, algemene voorwaarden of tarieflijsten.

In 2022 werden 36 individuele aanbevelingen geformuleerd.

Aan 26 aanbevelingen (of 72,2%) werd positief gevolg gegeven door de financiële instellingen. 9 aanbevelingen (of 25%) werden niet gevolgd, waarbij de instelling Ombudsfin heeft toegelicht waarom. 1 aanbeveling (of 2,8%) was op het moment van het opstellen van dit verslag nog in verder onderzoek bij de financiële instelling.

2.5. College van experten[2]

Het college van experten behandelt principekwesties en complexe dossiers.

In 2022 werden 4 dossiers voorgelegd aan het college. Deze dossiers hadden betrekking op volgende thema's: hypothecair krediet, zichtrekening, verkoop van effecten en nalatenschap.

3 van de 4 dossiers (75%) voorgelegd aan het college werden gegrond geacht.

In 2 van de 3 dossiers (of 66,7%), deed de financiële instelling een minnelijk voorstel tot oplossing. In het andere dossier (of 33,3%), volgde de financiële instelling het advies van het College niet.[3]

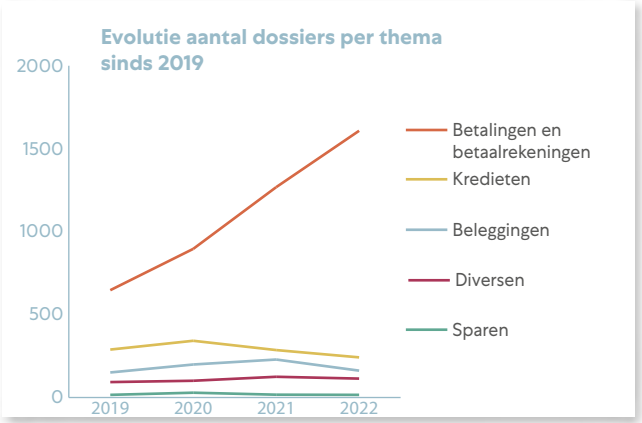
2.6. Thema's ontvankelijke klachten consumenten

De thema's van de ontvankelijke klachten van consumenten in 2022 waren de volgende (evolutie in aantal en percentage sinds 2019):

THEMA'S	2022	2021	2020	2019	2022	2021	2020	2019
	Aantal				%			
Betalingen en betaalrekeningen	1.608	1.268	896	647	75,07	65,87	57,18	54,10
Kredieten, waaronder	242	286	342	289	11,30	14,86	21,83	24,16
Consumentenkredieten	88	133	142	159	4,11	6,91	9,06	13,29
Hypothecaire kredieten	154	153	200	130	7,19	7,95	12,76	10,87
Beleggingen	162	229	199	151	7,56	11,90	12,70	12,63
Diversen	114	125	101	93	5,32	6,49	6,45	7,78
Sparen	16	17	29	16	0,75	0,88	1,85	1,34
TOTAAL	**2.142**	**1.925**	**1.567**	**1.196**	**100%**	**100%**	**100%**	**100%**

Het belangrijkste thema in 2022 was, net als in de voorgaande jaren, met grote voorsprong "Betalingen en betaalrekeningen" met 1.608 dossiers. Dit thema, dat de laatste jaren gestaag is toegenomen, vertegenwoordigt thans 75% van de ontvankelijke klachten. Het omvat onder andere de fraudedossiers en de klachten rond stopzetting van de bankrelatie. Op de analyse van Ombudsfin in fraudedossiers komen wij hierna in detail terug.

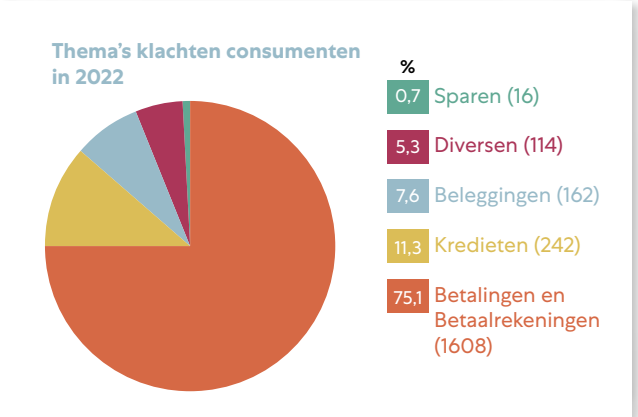
Evolutie van de thema's sinds 2019:



2 Samenstelling van het college, zie supra Missie Ombudsfin – Medewerkers en raadgevers ombudsman

3 De betrokken instelling is Bank Nagelmackers.

Aandeel van elk thema in 2022:



2.7 Een overzicht van de belangrijkste subthema's

2.7.1 Betalingen en betaalrekeningen

Betalingen en betaalrekeningen	Aantal klachten
Verrichtingen via PC of mobiel (betwist na phishing of andere fraude)	967
Zichtrekeningen (beëindiging, blokkering, afsluiting)	226
Zichtrekeningen (algemeen en tarifering)	115
Internationale betalingen	102
Kaarten (betwiste verrichtingen na diefstal, verlies)	51
Verrichtingen via PC of mobiel (foutief uitgevoerd of andere)	40
Kaarten (algemeen)	37
Automatische loketten (Self)	23
Ongeoorloofde debetstand	13
Bankverhuisdienst	8
Basisbankdienst	8
Loketverrichtingen	6
Domiciliëringen en bestendige opdrachten	5
Wisselverrichtingen	4
Cheques	3
TOTAAL	**1.608**

Het overzicht van de subthema's spreekt voor zich. De betwisting van verrichtingen naar aanleiding van phishing of andere fraude (uitgezonderd investment scam) vormt het allerbelangrijkste behandelde thema bij Ombudsfin. Met 967 dossiers vertegenwoordigt dit thema 45,1% van het totaal aantal ontvankelijke consumentenklachten.

Ook de blokkering en beëindiging/afsluiting van de zichtrekening blijft een belangrijk onderwerp met 226 dossiers of 10,6% van het totaal aantal ontvankelijke consumentenklachten.

De basisbankdienst voor de consumenten

De wetgeving die de basisbankdienst in detail regelt, is terug te vinden in Hoofdstuk 8 "Toegang tot betaalrekeningen en basisbankdienst", Afdeling 1 "Betaalrekeningen en basisbankdienst voor consumenten" van boek VII, Titel 3 van het Wetboek van economisch recht.

Ombudsfin is het orgaan dat bevoegd is om een klachten- en buitengerechtelijke beroepsprocedure te behandelen. Bijzonder is dat Ombudsfin een bindende bevoegdheid heeft voor wat de basisbankdienst betreft. In 2022 heeft Ombudsfin 8 klachten ontvangen die handelden over de basisbankdienst.

Kredietinstellingen verstrekken Ombudsfin jaarlijks statistieken over het aantal geopende, geweigerde en opgezegde rekeningen, en de redenen daarvoor.

Zie hieronder de cijfers voor 2022:

Statistieken basisbankdienst	2022
Aantal banken die basisbankdiensten hebben geregistreerd	13
Aantal geopende basisbankdiensten	42.672
Totaal aantal bestaande basisbankdiensten	68.753
Aantal weigeringen van openingen van basisbankdiensten	10
Aantal opgezegde basisbankdiensten (*)	5.886

(*) De basisbankdiensten die worden omgevormd tot een gewone zichtrekening zijn hierin ook opgenomen

In 2022 waren er 13 banken die basisbankdiensten hebben geregistreerd, dat zijn er 2 meer dan in 2021.

Het aantal geopende basisbankdiensten is in 2022 gestegen met 234% tot 42.672. In 2021 waren er 12.771 openingen.

De stijging is hoofdzakelijk toe te schrijven aan openingen van basisbankdiensten door Oekraïense vluchtelingen.

In 2022 werden 10 aanvragen om basisbankdiensten te openen geweigerd wegens negatieve antecedenten bij de bank (80%) en het feit dat de aanvrager al een lopende rekening had (20%).

De belangrijkste reden voor een afsluiting is deze op vraag van de titularis (96,81%), gevolgd door:
- Zichtrekening bij een andere instelling (1,4%);
- Andere niet met de basisbankdienst verenigbare producten (1,13%);
- Negatieve antecedenten bij de bank (0,53%);
- Andere rekeningen met meer dan 6.000 euro (0,13%).

2.7.2. Kredieten

2.7.2.1. Hypothecaire kredieten

Hypothecaire kredieten	Aantal klachten
Uitvoering van het contract	82
Totstandkoming van het contract	58
Desolidarisatie	5
Algemene voorwaarden (andere)	5
Overbruggingskrediet	2
Hypothecaire volmacht	1
Waarborgen	1
Publiciteit	0
Totaal	**154**

De meeste klachten betreffende hypothecaire kredieten kaderden binnen de uitvoering van het krediet (82 dossiers). Daarbij was de aanleiding van de klacht vaak het jaarlijks kostenpercentage of "JKP" (20 dossiers) en terugbetalingsmoeilijkheden (16 dossiers).

Bij de dossiers over de totstandkoming van het contract (58 dossiers) ging het vaak over het verloop van de toekennings-procedure (18 dossiers) en een kredietweigering (13 dossiers).

2.7.2.2. Consumentenkredieten

Consumentenkredieten	Aantal klachten
Uitvoering van het contract	61
Totstandkoming van het contract	22
Algemene Voorwaarden (andere)	4
Publiciteit	1
Totaal	**88**

De meeste klachten over consumentenkredieten gingen over de uitvoering van het krediet (61 dossiers). Daarbij was de aanleiding van de klacht vaak een negatieve melding bij de Nationale Bank van België (21 dossiers) of werden terugbetalingsmoeilijkheden aangekaart (11 dossiers).

Bij de dossiers over de totstandkoming van het contract (22 dossiers) ging het vaak over een kredietweigering (8 dossiers).

2.7.3. Beleggingen

Beleggingen	Aantal klachten
Effectenrekeningen	44
Investment scam	40
Aan-/verkoop effecten (execution only)	29
Fiscale aspecten	13
Pensioenfondssen/pensioensparen	10
Beleggingsadvies	9
Diversen	7
Corporate action	6
Publiciteit en informatie bij de intekening	3
Vermogensbeheer	1
Financial planning	0
Informatie over tarieven/kosten	0
Totaal	**162**

De meeste klachten betreffende beleggingen, handelden over de effectenrekening (44 dossiers) en *investment scam* (40 dossiers).

2.7.4. Diversen

Diversen	Aantal klachten
Nalatenschappen	49
Huurwaarborg (ook spaarrekening)	24
Spaarproducten	16
Know Your Customer	9
Kluizen	8
Diversen	8
Onbekwaamheid (minderjarige)	7
Privacy	5
Discriminatie	4
Fraude bediende	0
Totaal	**130**

De belangrijke thema's blijven, net zoals de voorgaande jaren, nalatenschappen (49 dossiers) en huurwaarborg (24 dossiers). Deze thema's worden later in dit verslag kort aangehaald.

3. AANVRAGEN INGEDIEND DOOR ONDERNEMINGEN

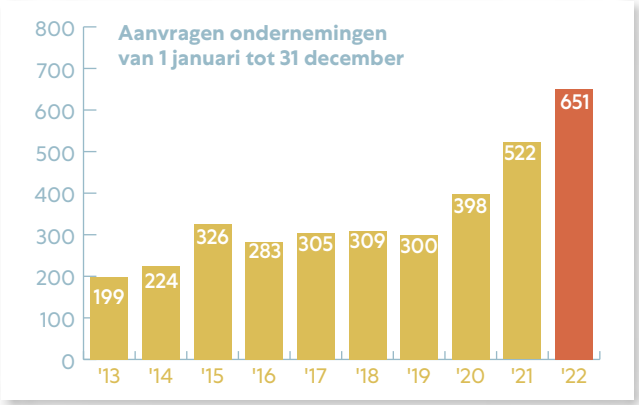
3.1. Aanzienlijke stijging aantal aanvragen

In 2022 ontving Ombudsfin in totaal 651 schriftelijke aanvragen van ondernemingen, tegenover 522 aanvragen in 2021. Dit is een stijging van 129 dossiers (24,7%).

Deze ontwikkeling is deels het gevolg van talrijke informatieverzoeken die zijn ingediend met betrekking tot de basisbankdienst voor ondernemingen. Ondanks het feit dat deze wet sinds mei 2021 van kracht is, had zij in de praktijk nog geen effect in 2022[4].

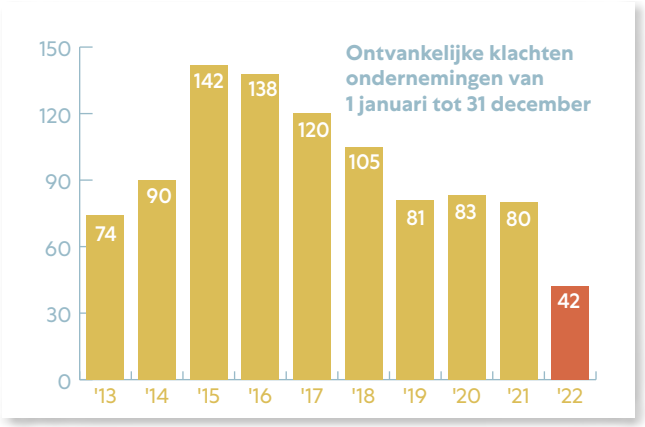
Ook merken we op dat ondernemingen er zich niet altijd van bewust zijn dat onze bevoegdheden voor hun geschillen beperkt zijn.

574 aanvragen betroffen een klacht, terwijl 77 aanvragen een vraag om informatie betroffen.



3.2. Quasi halvering van de ontvankelijke klachten

In 2022 registreerde Ombudsfin 42 aanvragen van ondernemingen als ontvankelijke klacht, tegenover 80 aanvragen in 2021, wat quasi een halvering betreft (38 dossiers minder, en dus daling van 47,5%). Dit is een opmerkelijke evolutie. Nooit eerder in de laatste jaren hebben wij zo weinig ontvankelijke klachten geregistreerd.

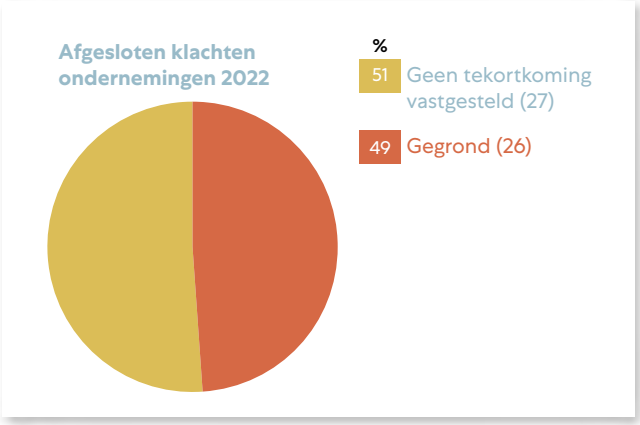


3.3. Resultaten van de in 2022 afgesloten klachten van ondernemingen

De resultaten die hierna besproken worden, hebben betrekking op alle klachten van ondernemingen die in 2022 behandeld en afgesloten werden. In deze resultaten zitten dus ook een aantal klachten die reeds in 2021 aan Ombudsfin werden voorgelegd, maar die pas in 2022 werden afgesloten.

Het gaat in totaal om 53 dossiers.

In 26 dossiers (of 49,1%) achtte Ombudsfin de klacht gegrond op basis van wetgeving, contractuele bepalingen, gedragscodes of marktpraktijken.

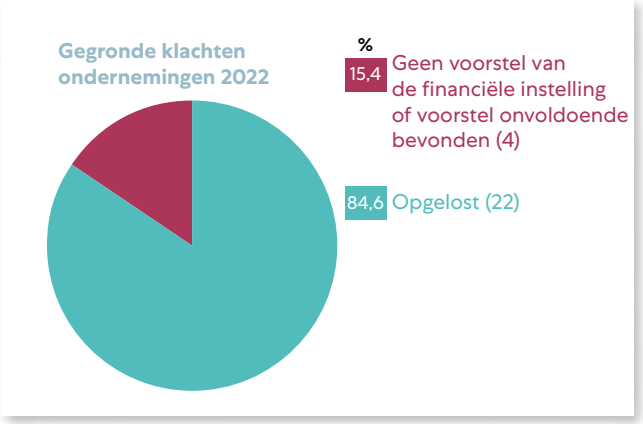


In 27 dossiers (of 50,9%) kon Ombudsfin geen tekortkoming in hoofde van de financiële instelling vaststellen. In deze

[4] Met de publicatie van het Koninklijk Besluit en het Ministerieel Besluit kan de procedure bij de basisbankdienstkamer sinds kort echt gevoerd worden. Voor meer informatie: https://economie.fgov.be/nl/themas/financiele-diensten/betalingsdiensten/basisbankdienst/basisbankdienst-voor-0

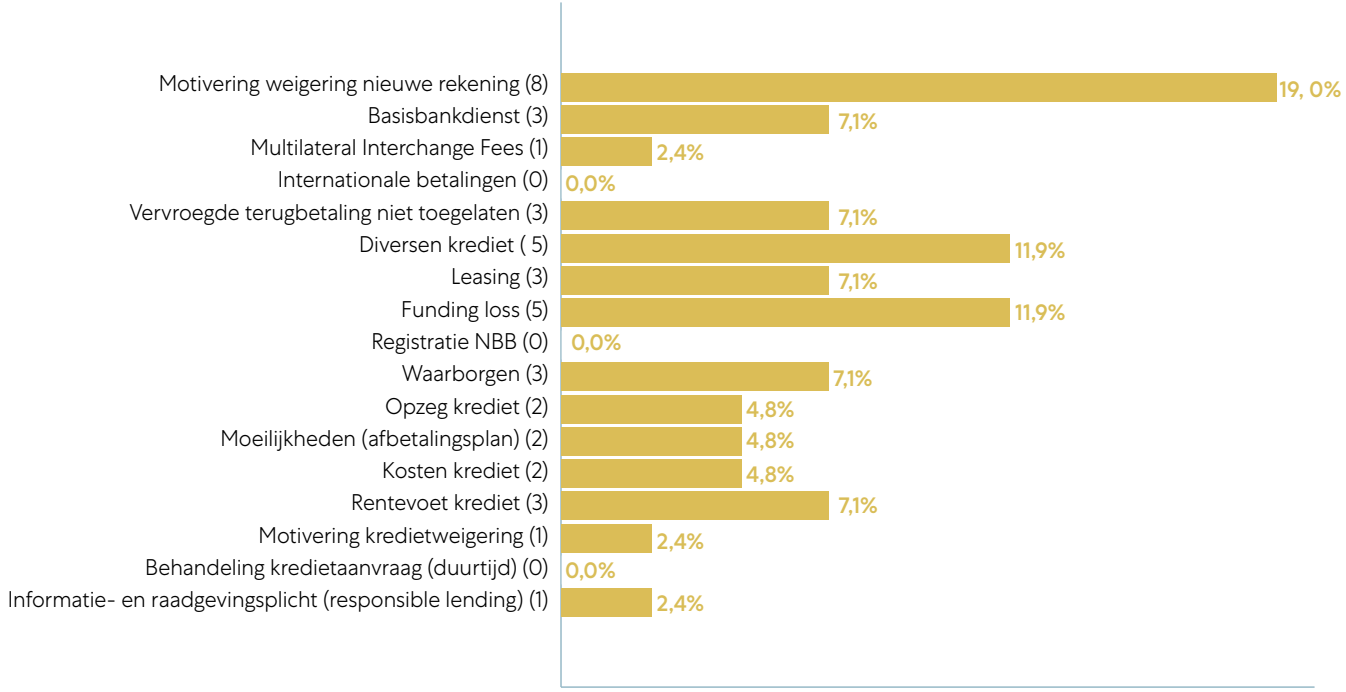
dossiers werd de nodige toelichting aan de onderneming gegeven zodat die kon begrijpen waarom Ombudsfin tot dit besluit kwam en waarom er dan ook geen rechtzetting of tegemoetkoming van de financiële instelling kon worden gevraagd.

In de 26 dossiers die als gegrond werden beschouwd, heeft Ombudsfin verder onderhandeld. Dit leidde in 22 dossiers (84,6 % van de gegronde dossiers) tot een minnelijk akkoord. Hiertegenover staat dat in 4 dossiers (15,4%) geen oplossing werd bereikt.



3.4. Thema's ontvankelijke klachten ondernemingen

In 2022 hadden de klachten betrekking op de volgende thema's:



4. INTERNETFRAUDEDOSSIERS: in welke gevallen moeten de financiële instellingen tussenkomen in de schade geleden door hun klanten?

INLEIDING

Nooit eerder werd er in de media zoveel aandacht besteed aan internetfraude als in de laatste jaren. Safeonweb, Febelfin, financiële instellingen en andere instanties drijven het aantal sensibiliseringscampagnes op om internetfraude te verminderen. Bovendien worden door financiële instellingen alsmaar meer maatregelen genomen en aanpassingen doorgevoerd in onder meer de betalingsprocessen om deze vorm van fraude zoveel mogelijk te voorkomen. Dit mag echter niet verwonderen aangezien phishing en internetfraude in het algemeen vandaag de dag alomtegenwoordig zijn. Belgen die tot op heden nog nooit een phishingbericht ontvangen hebben of een telefonische oproep van een fraudeur gekregen hebben, worden helaas meer en meer de uitzondering. Verder worden fraudeurs steeds professioneler en vindingrijker en passen zij de bestaande fraudescenario's aan de actualiteit en betaalsystemen van de verschillende financiële instellingen aan.

Deze evolutie van een toenemend aantal gevallen van internetfraude houdt uiteraard verband met de steeds meer toenemende digitalisering van bankdiensten. Deze trend is uiteraard ook waar te nemen in de jaarlijkse statistieken van Ombudsfin.

Het aantal internetfraudedossiers dat door Ombudsfin wordt behandeld, is de afgelopen jaren aanzienlijk gestegen. In 2019 werden 221 dossiers (18,5% van het totaal) behandeld, terwijl dit aantal in 2020 steeg tot 393 dossiers (25,1% van het totaal) en in 2021 tot 658 dossiers (34,2% van het totaal). In 2022 was het grootste deel van de door Ombudsfin behandelde dossiers (1.018 van de 2.142 ontvankelijke dossiers) gerelateerd aan de betwisting van frauduleuze verrichtingen. Hiervan betroffen 51 dossiers het gebruik van fysieke kaarten en 967 dossiers (45,1% van het totaal) internetfraude.

Rekening houdende met voorgaande cijfers lijkt het ons nuttig om in dit jaarverslag de door Ombudsfin in internetfraudedossiers gevolgde redenering uiteen te zetten inzake de regelgeving betreffende de aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties, zoals voorzien in Boek VII van het Wetboek Economisch Recht (hierna WER). Op basis van recente rechtsleer en rechtspraak is onze visie, zoals uiteengezet in ons jaarverslag van 2019, immers geëvolueerd. In deze uiteenzetting wordt eveneens stilgestaan bij de verschillende tegenargumenten van de financiële instellingen, waarmee Ombudsfin in haar bemiddelingsopdracht geconfronteerd wordt. Hierbij worden voorbeelden gegeven aan de hand van relevante fraudetechnieken. Tot slot wordt stilgestaan bij een aantal

(genomen) maatregelen om het aantal fraudegevallen en de ermee gepaard gaande schade te beperken en worden een aantal algemene aanbevelingen gedaan aan de consumenten en de sector.

Voordat we onze juridische uiteenzetting beginnen, willen we kort stilstaan bij de bemiddelingsresultaten die we in 2022 hebben behaald in fraudezaken, en bij de verschillende fraudescenario's die door fraudeurs worden gebruikt:

Ook dit jaar merkt Ombudsfin op dat de bemiddelingsresultaten in fraudezaken niet zo positief zijn. Slechts in 38% van de gegronde internetfraudedossiers (138 dossiers) kon Ombudsfin positief bemiddelen. Dit komt doordat de vraag of banken al dan niet verplicht zijn om de schade ten gevolge van niet-toegestane betalingstransacties te vergoeden, afhankelijk is van verschillende factoren, met name of de fraude op voorhand kon worden gedetecteerd door het slachtoffer en of er sprake is van grove nalatigheid van het slachtoffer. Dit moet worden beoordeeld op basis van alle feitelijke omstandigheden. Ombudsfin stelt vast dat banken vaak op een andere manier naar de feiten kijken. Er wordt vaak gediscussieerd over de vraag of de klant grof nalatig is geweest, waarbij banken een zeer brede definitie van grove nalatigheid hanteren.

Volledigheidshalve dienen wij wel op te merken dat niet alle dossiers omtrent internetfraude gegrond worden geacht. In bepaalde dossiers weerhouden wij eveneens de grove nalatigheid, in andere dossiers kunnen wij ons niet concreet uitspreken omdat er onvoldoende zicht is op de feitelijke omstandigheden van de fraude. Concreet voor 2022 sloten wij 549 internetfraudedossiers (of 60% van de internetfraudedossiers) af als ongegrond en 365 dossiers (of 40%) als gegrond.

Ombudsfin stelt ook vast dat de door fraudeurs gehanteerde fraudescenario's over het algemeen dezelfde gebleven zijn in 2022. Ombudsfin behandelde nog altijd veel gevallen waarbij slachtoffers werden opgelicht via phishingmails of -sms'jes, of via frauduleuze aan- of verkopen op zoekertjessites. Ook waren er gevallen waarbij slachtoffers werden misleid door een nepwebsite van hun bank en probeerden in te loggen, of werden ze telefonisch benaderd in zogenaamde "kluisrekeningfraude"-gevallen.

Als de gehanteerde technieken en scenario's dezelfde bleven, werden ze verder gefinetuned en afgestemd op de actualiteit (bijv. bekomen van een energiepremie) en eventuele door de financiële instelling doorgevoerde aanpassingen in de betalingsprocessen en bijvoorbeeld de installatieprocedures van mobiele bankapps. Voor tips en waarschuwingen over de meest voorkomende fraudescenario's verwijzen wij naar www.safeonweb.be.

4.1. (Niet-)Toegestane betalingstransacties

4.1.1. Definitie toegestane betalingstransactie

Boek VII van het WER voorziet een aansprakelijkheidsregeling bij niet-toegestane betalingstransacties. Alvorens deze regels kunnen worden toegepast, moet logischerwijs worden nagegaan of een door de betaler betwiste betalingstransactie al dan niet als toegestaan kan worden gekwalificeerd. Het is immers niet omdat sprake is van betalingsfraude, dat automatisch ook sprake is van een niet-toegestane betalingstransactie.

Het WER voorziet dat een betalingstransactie pas als toegestaan wordt aangemerkt indien de betaler heeft ingestemd met de uitvoering van de betalingsopdracht. Zonder instemming door de betaler wordt een betalings-

transactie als niet-toegestaan aangemerkt. In de memorie van toelichting bij de wet staat dat pas sprake kan zijn van een toegestane betalingstransactie indien de betaler hiermee **uitdrukkelijk** heeft ingestemd.

Hoewel het onderscheid tussen toegestane en niet-toegestane betalingstransacties relatief eenvoudig lijkt, bestaat hierover in de praktijk discussie. Deze discussie bestaat voornamelijk over de invulling van het begrip "instemming". Alvorens hierop in te gaan, lijkt het nuttig de bewijsregeling in artikel VII.42 WER te bespreken.

4.1.2. Bewijslast: is de transactie al dan niet toegestaan?

Artikel VII.42 WER regelt de bewijslast inzake het al dan niet toegestaan karakter van een betwiste verrichting. Zo voorziet deze bepaling dat wanneer een betalingsdienstgebruiker ontkent dat hij een uitgevoerde betalingstransactie heeft toegestaan of aanvoert dat de betalingstransactie niet correct is uitgevoerd, de betalingsdienstaanbieder gehouden is het bewijs te leveren dat de betalingstransactie is geauthenticeerd, juist is geregistreerd, is geboekt en niet door een technische storing of enig ander falen van de door de betalingsdienstaanbieder aangeboden diensten is beïnvloed. Indien de betalingsdienstaanbieder deze technische bewijzen niet kan leveren, zal de betalingsdienstgebruiker niet aansprakelijk kunnen worden gesteld.

Verder voorziet artikel VII.42 WER dat het gebruik van een betaalinstrument, dat door de betalingsdienstaanbieder is geregistreerd, op zichzelf niet noodzakelijkerwijze afdoende bewijs vormt dat de betalingstransactie door de betaler is toegestaan of dat de betaler frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer van de verplichtingen niet is nagekomen. Wanneer de betalingsdienstaanbieder de in artikel VII.42, §1, lid 1 WER vermelde bewijzen levert, brengt dit dus niet automatisch mee dat de betwiste verrichting als toegestaan mag worden aangemerkt.

Het gebruik van de woorden "niet noodzakelijkerwijze" brengt mee dat het bewijs van de registratie van het gebruik van het betaalinstrument, in sommige gevallen voldoende bewijs kan vormen van het toegestaan karakter van de betwiste verrichting, maar dat dit niet altijd en automatisch het geval is. Eenmaal de betalingsdienstaanbieder bovenvermelde bewijzen geleverd heeft, dient de betaler aannemelijk te maken dat hij niet bewust met de transactie ingestemd heeft. De betaler dient hiervan dus geen absoluut bewijs te leveren. Indien de betaler aannemelijk kan maken dat hij niet met de betwiste verrichting heeft ingestemd, kan de betalingsdienstaanbieder niet meer volstaan met het enkele bewijs van de registratie van het gebruik van het instrument (en de bijbehorende geheime code) om aan te tonen dat de transactie werd toegestaan. Indien de betaler dit niet aannemelijk kan maken, vormen de technische bewijzen wel voldoende bewijs dat de transactie werd toegestaan.

De betaler kan het best aannemelijk maken dat hij niet met de betwiste verrichting(en) heeft ingestemd door een gedetailleerde uiteenzetting van het fraudeverloop (de modus operandi van de fraudeur) te geven. In sommige gevallen kan het niet-toegestaan karakter van de betwiste verrichtingen aannemelijk worden gemaakt doordat men klacht neergelegd heeft bij de politie, doordat de betaler door bepaalde omstandigheden onmogelijk de betwiste verrichtingen kon hebben geïnitieerd, of op basis van de aard, de omvang of de opeenvolging van de betwiste verrichtingen, etc.

In de praktijk behandelt Ombudsfin vaak dossiers waarin een betaler één of meerdere transacties betwist, waarvan de financiële instelling kan aantonen dat deze correct geauthenticeerd werd(en) (bijvoorbeeld door middel van een met bankkaart, pincode en digipass[5] gegenereerde code, of via een nieuw geïnstalleerde mobiele app, gekoppeld aan de rekeningen van het slachtoffer), maar waarbij de klager niet de minste informatie kan geven over het fraudeverloop. In deze dossiers kan Ombudsfin, afhankelijk van de concrete omstandigheden in het dossier, besluiten dat de klager onvoldoende aannemelijk maakt dat hij niet heeft ingestemd met de betwiste verrichting(en), waardoor de door de financiële instelling geleverde technische bewijzen toch volstaan om te besluiten dat sprake is van (een) toegestane betalingstransactie(s).

[5] Hiermee worden zowel de Digipass als bankkaartlezer bedoeld. In deze bijdrage wordt geen onderscheid gemaakt tussen een Digipass en kaartlezer. Beide termen worden dan ook zonder onderscheid gebruikt.

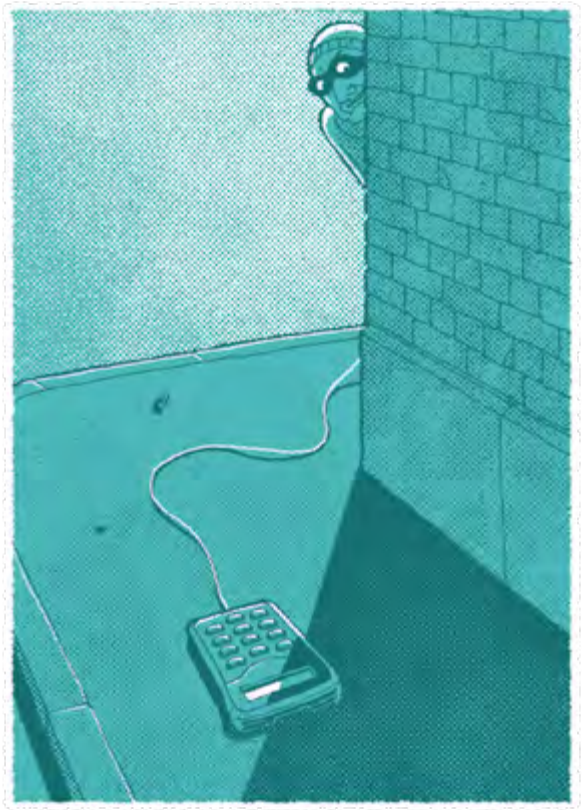
4.1.3. Subjectieve of objectieve instemming? Autorisatie ≠ authenticatie

4.1.3.1. Standpunt van Ombudsfin

Ombudsfin hanteert het principe van een subjectieve uitdrukkelijke instemming. Volgens Ombudsfin kan pas sprake zijn van een toegestane betalingstransactie wanneer de betaler hiermee vrij en bewust heeft ingestemd. Dit betekent dat Ombudsfin een transactie pas als toegestaan zal kwalificeren wanneer de betaler op het moment van de betaling het bedrag en de begunstigde of het doel van de transactie kent.

Het uitgangspunt van de subjectieve uitdrukkelijke instemming kan het best worden uitgelegd aan de hand van een aantal voorbeelden. Zo is in vele gevallen van Whaling vaak duidelijk sprake van toegestane betalingstransacties. Bij deze vorm van fraude sturen fraudeurs (veelal) via WhatsApp een bericht naar hun slachtoffer en doen zij zich hierbij voor als een familielid van het slachtoffer. Ze stellen dat hun gsm stukgegaan is waardoor zij een nieuw telefoonnummer hebben. Na een kort gesprek met het slachtoffer vraagt de fraudeur vervolgens aan zijn slachtoffer om verschillende overschrijvingen voor hem uit te voeren. Het slachtoffer voert hier dus zelf de overschrijvingen uit via zijn eigen internetbankieren of mobiele app. Bijgevolg is duidelijk sprake van toegestane betalingstransacties. Het motief voor de verrichting (het feit dat men dacht betrokken verrichting uit te voeren op vraag van een familielid) is hier dus niet relevant.

Een tweede voorbeeld betreft gevallen van phishing of smishing (sms + phishing) waarbij het slachtoffer een mail of bericht ontvangt betreffende bijvoorbeeld een nieuwe digipass die zogezegd kan worden aangevraagd via een bijgevoegde link, of bijvoorbeeld met de melding dat het itsme-account van het slachtoffer geblokkeerd is en de vraag om dit te deblokkeren via een bijgevoegde link. In deze gevallen zal het slachtoffer op betrokken link in het



frauduleuze bericht klikken en zo terechtkomen op een valse website die onder controle van de fraudeur staat. Daar zal aan het slachtoffer gevraagd worden om bepaalde bancaire gegevens in te voeren, alsook handelingen met de bankkaart en digipass te stellen en de berekende responscodes in te voeren, zogezegd om de aanvraag van de nieuwe digipass of de deblokkering van het itsme-account te bevestigen. Doordat de fraudeur controle heeft over de valse website slaagt hij erin de ingevoerde gegevens te onderscheppen. De onderschepte codes misbruikt hij vervolgens om bijvoorbeeld betalingen te bevestigen op de website van een handelaar of om eerst een mobiele app, gekoppeld aan de rekeningen van zijn slachtoffer te installeren en vervolgens met deze app overschrijvingen of betalingen te bevestigen. Volgens het standpunt van Ombudsfin is in deze gevallen steeds sprake van niet-toegestane betalingstransacties. Het slachtoffer dacht immers dat hij door zijn handelingen de aanvraag van een nieuwe digipass of de deblokkering van zijn itsme-account zou bevestigen. Hij wist echter niet dat zijn handelingen de bevestiging van bepaalde betalingen zouden toelaten of een derde in staat zouden stellen om een mobiele app te installeren waarmee vervolgens verrichtingen kunnen worden bevestigd.

4.1.3.2. Standpunt van bepaalde financiële instellingen en van een deel van de rechtsleer

a) Authenticatie = autorisatie

Ondanks de duidelijke bewoording van de wet, stelt Ombudsfin vast dat verschillende financiële instellingen autorisatie (toestaan) en authenticatie nog steeds aan elkaar gelijkstellen. Na bewijs van een correcte authenticatie geleverd te hebben, conform de hierboven reeds besproken bewijsregeling, besluiten betrokken instellingen dat sprake is van een toegestane betalingstransactie en dat de regels inzake niet-toegestane betalingstransacties bijgevolg niet van toepassing zijn, waardoor zij niet meer gehouden zijn om de betaalrekening van het slachtoffer voorlopig te crediteren en zij van oordeel zijn geen verdere analyse van het dossier te moeten doen, bijvoorbeeld betreffende de beoordeling van een eventuele grove nalatigheid.

Betrokken financiële instellingen beroepen zich hierbij veelal op artikel VII.32, §2, lid 1 WER, op basis waarvan de instemming om een betalingstransactie of een reeks betalingstransacties te doen uitvoeren wordt verleend in de tussen de betaler en de betalingsdienstaanbieder overeengekomen vorm en volgens de overeengekomen procedure. Na bewijs te hebben geleverd dat de in de reglementen van de instelling overeengekomen procedure en vorm (bijvoorbeeld: aankopen op het internet gebeuren via gebruik van de digipass, bankkaart, invoeren pincode en genereren responscodes) werden nageleefd, menen betrokken financiële instellingen bewijs te hebben geleverd van het toegestaan karakter van de betwiste verrichtingen.

Ombudsfin is echter van mening dat betrokken financiële instellingen zich foutief op artikel VII.32WER beroepen wanneer zij stellen dat als de fraudeur de overeengekomen procedure gerespecteerd heeft, de titularis van het betaalinstrument ingestemd heeft met de transactie. Volgens Ombudsfin heeft deze bepaling immers uitsluitend tot doel ervoor te zorgen dat als instemming voor een transactie wordt gegeven, dit uitsluitend mogelijk mag zijn volgens de overeengekomen procedure. Deze bepaling voorziet daarentegen niet dat als de overeengekomen procedure werd doorlopen, de betaler automatisch ingestemd heeft met de betrokken verrichting. Dit is ook logisch: het is niet omdat de toegangsmiddelen van de betalingsdienstgebruiker werden gebruikt dat hijzelf ook daadwerkelijk zijn toestemming tot de transactie heeft gegeven.

Bovendien valt deze stelling, op basis waarvan een transactie automatisch als toegestaan wordt gekwalificeerd van zodra de overeengekomen procedure werd nageleefd, niet te rijmen met artikel VII.42, §2, lid 1 WER, waar staat dat het gebruik van het betaalinstrument niet noodzakelijkerwijze voldoende bewijs vormt dat de betaler de transactie heeft toegestaan. Een dergelijke invulling van de wet waarbij autorisatie compleet gelijkstaat aan authenticatie zou de bescherming die de Europese en Belgische wetgever aan de betaler wou bieden nagenoeg volledig uithollen. Bij toepassing hiervan zou in ieder van de onder vorige titel besproken voorbeelden immers sprake zijn van toegestane betalingstransacties.

b) Technische instemming

Bepaalde auteurs matigen bovenvermeld standpunt en hanteren het uitgangspunt van de objectieve uitdrukkelijke, ofwel de technische, instemming. Deze auteurs stellen dat als kan worden aangetoond dat de authenticatie door de rechtmatige kaarthouder is uitgevoerd, er sprake is van een toegestane betalingstransactie. Het doorlopen van de bedongen betalingsprocedure zou volgens deze auteurs dus moeten volstaan om te spreken van een toegestane betaling, mits dit gebeurt door de rechtmatige kaarthouder. Hierbij wordt dan geen rekening gehouden met de intentie van de betaler, de vraag of hij werkelijk ingestemd heeft met het bereikte resultaat van de betaling.

Volgens de stelling van deze auteurs zal dus steeds rekening moeten worden gehouden met de wijze waarop de authenticatie plaatsgevonden heeft. Indien een fraudeur met behulp van responscodes, die door het slachtoffer met de digipass gegenereerd werden en vervolgens onderschept werden via bijvoorbeeld een phishingmail, rechtstreeks betalingen uitvoert op de website van een handelaar, zal volgens deze stelling sprake zijn van toegestane betalingstransacties. De authenticatieprocedure, nl. het berekenen van responscodes met de digipass, werd immers door de rechtmatige kaarthouder doorlopen. Misbruikt de fraudeur de onderschepte codes echter om bijvoorbeeld een mobiele app, gekoppeld aan de rekeningen van het slachtoffer te installeren en voert hij vervolgens met deze app de betwiste verrichtingen uit (zonder dat dus bijkomende handelingen moeten worden gesteld door het slachtoffer), dan is volgens deze auteurs wel sprake van niet-toegestane

betalingstransacties. De authenticatieprocedure, nl. het bevestigen van de verrichtingen via de app, werd immers doorlopen door de fraudeur.

4.1.3.3. Standpunt in de rechtspraak

In een arrest van 21 mei 2021 oordeelde de Nederlandse Hoge Raad, een instantie te vergelijken met het Belgische Hof van Cassatie, uitdrukkelijk dat de omstandigheid dat de betwiste betaalopdrachten werden verleend overeenkomstig de tussen de betaler en de betaaldienstverlener overeengekomen vorm en procedure er niet aan in de weg staat dat deze betalingstransacties worden aangemerkt als niet-toegestaan. De Hoge Raad oordeelde met andere woorden expliciet dat authenticatie en autorisatie niet aan elkaar gelijkgesteld mogen worden. Zo weerlegt dit arrest alvast de stelling dat steeds sprake zou zijn van toegestane betalingstransacties wanneer de authenticatie gebeurd is volgens de overeengekomen vorm en procedure, ongeacht wie de authenticatieprocedure heeft doorlopen (het slachtoffer of de fraudeur).

In een arrest van 9 januari 2020 oordeelde het hof van beroep van Luik in een phishing-zaak dat sprake was van een niet-toegestane betalingstransactie, hoewel de instemming met de betwiste verrichtingen gegeven werd volgens de tussen de betalingsdienstaanbieder en de betaler overeengekomen vorm en procedure. Het hof van beroep verwijst hierbij naar de bepaling op basis waarvan het gebruik van een betaalinstrument, zoals geregistreerd door de betalingsdienstaanbieder, op zich niet noodzakelijk volstaat om te bewijzen dat de betalingstransactie door de betaler was toegestaan. Voor zijn conclusie dat sprake is van een niet-toegestane betalingstransactie benadrukt het hof van beroep dat de betaler nooit de bedoeling heeft gehad de betwiste verrichting te bevestigen. Het hof houdt dus rekening met de bedoeling van de betaler, het intentioneel element, en bevestigt op die manier het standpunt van Ombudsfin inzake een subjectieve uitdrukkelijke instemming. Bovendien werd in deze zaak de authenticatieprocedure, namelijk het genereren van een responscode met behulp van de bankkaart en de digipass waarmee vervolgens de betwiste overschrijving via internetbankieren bevestigd werd, doorlopen door de betaler zelf, waardoor betrokken arrest duidelijk de stelling inzake de objectieve uitdrukkelijke, ofwel technische, instemming weerlegt.

Ombudsfin stelt echter vast dat dit arrest niet door alle rechtspraak gevolgd wordt. Volgens een aantal vonnissen die na deze datum in eerste aanleg geveld werden, volstond de overdracht van een code aan de fraudeur als bewijs van de wil van het slachtoffer om de transactie te autoriseren, zelfs wanneer het vaststond dat het slachtoffer het bedrag en de begunstigde van de frauduleuze verrichting niet kende. Hoewel deze overdracht in bepaalde gevallen kan leiden tot het besluit van een grove nalatigheid in hoofde van het slachtoffer, lijkt deze daarentegen op zichzelf niet relevant om een transactie al dan niet als toegestaan te kwalificeren.

Ombudsfin stelt ten slotte vast dat in de meeste, door Ombudsfin gekende, rechtspraak geen of weinig aandacht wordt besteed aan de vraag of de betwiste verrichtingen al dan niet als niet-toegestaan kunnen worden gekwalificeerd. Dit komt doordat de betrokken financiële instellingen in deze zaken het niet-toegestaan karakter van de betwiste verrichtingen niet betwisten. Het niet-toegestaan karakter van de betwiste verrichtingen wordt als het ware als vanzelfsprekend beschouwd.

4.2. Verplichting tot onmiddellijke terugbetaling

4.2.1. Regeling in artikel VII.43 WER

Artikel VII.43 WER voorziet dat de betalingsdienstaanbieder, in geval van een niet-toegestane betalingstransactie, de betaler onmiddellijk het bedrag van de niet-toegestane betalingstransactie dient terug te betalen. Deze onmiddellijke terugbetaling moet gebeuren vanaf het moment dat de betalingsdienstaanbieder zich rekenschap heeft gegeven van de transactie of daarvan in kennis is gesteld. De wet voorziet dat de terugbetaling uiterlijk aan het einde van de eerstvolgende werkdag dient te gebeuren.

Deze verplichting tot onmiddellijke terugbetaling geldt echter niet indien de betalingsdienstaanbieder redelijke gronden heeft om fraude in hoofde van de betaler te vermoeden en deze gronden schriftelijk aan de FOD Economie meedeelt. De betalingsdienstaanbieder heeft bijgevolg de mogelijkheid om binnen een redelijke termijn een prima facie onderzoek hiernaar in te stellen, alvorens de betaler terug te betalen. Indien de betalingsdienstaanbieder dus een sterk vermoeden heeft dat een niet-toegestane transactie het resultaat is van frauduleus gedrag van de betalingsdienstgebruiker en indien dat vermoeden gebaseerd is op aan de betrokken nationale

autoriteit gemelde objectieve gronden, dan dient de betalingsdienstaanbieder de mogelijkheid te hebben binnen een redelijke termijn een onderzoek in te stellen alvorens de betaler terug te betalen.

Eenmaal vaststaat dat sprake is van een niet-toegestane betalingstransactie en er geen vermoeden van fraude in hoofde van de betaler is, dient de gedebiteerde betaalrekening in zijn oorspronkelijke toestand hersteld te worden, alsof de niet-toegestane betalingstransactie nooit heeft plaatsgevonden. De valutadatum van deze creditering mag niet later zijn dat de datum waarop het bedrag werd gedebiteerd. De betalingsdienstaanbieder kan met andere woorden niet wachten om de rekening van de betalingsdienstgebruiker opnieuw te crediteren tot er definitief uitsluitsel is over de aansprakelijkheid van de betaler.

Het doel van deze onmiddellijke terugbetalingsverplichting in hoofde van de financiële instelling bestaat er dus in de aansprakelijkheidsverdeling voorlopig te regelen in afwachting van de definitieve aansprakelijkheidsverdeling op basis van artikel VII.44 WER. Deze verplichting bevestigt dat de betalingsdienstaanbieder in principe, tenzij in geval van bedrog vanwege de betaler zelf, aansprakelijk is voor en het risico draagt van niet-toegestane betalingstransacties. Bepaalde juristen stellen dat de betalingsdienstaanbieder hierbij de betaalrekening van de betaler niet eenzijdig mag debiteren wanneer hij op basis van de definitieve aansprakelijkheidsregeling in artikel VII.44 WER tot het besluit komt toch niet aansprakelijk te zijn (tenzij uit nader onderzoek blijkt dat de betaler zelf frauduleus gehandeld heeft). De betalingsdienstaanbieder zal slechts tot debitering mogen overgaan indien de betaler daarmee instemt of indien hij daartoe een uitvoerbare titel heeft verkregen.

Deze onmiddellijke terugbetalingsverplichting heeft als voordeel voor de betaler dat hijzelf geen actie moet ondernemen tegen de betalingsdienstaanbieder als hij beweert niet of slechts in beperkte mate aansprakelijk te zijn. De betalingsdienstaanbieder die beweert dat de betaler aansprakelijk is, zal daarentegen het bedrag van de niet-toegestane betalingstransacties moeten terugvorderen. Het risico om te procederen wordt zo dus bij de betalingsdienstaanbieder gelegd. Dit kan echter ook negatieve gevolgen hebben voor de betaler, daar financiële instellingen in bepaalde gevallen sneller zouden kunnen beslissen tot het instellen van een rechtsvordering, waardoor bepaalde betalers ongewild tot een gerechtelijke procedure gedwongen zouden kunnen worden. Meer gerechtelijke procedures zullen dan weer leiden tot bijkomende druk op onze rechtbanken.

4.2.2. Vaak niet-naleving in de praktijk

Ombudsfin stelt vast dat de meeste financiële instellingen deze verplichting in de praktijk, althans in de door Ombudsfin behandelde dossiers, niet naleven. Onder andere op basis van het foutieve argument dat een geauthenticeerde verrichting ook een toegestane verrichting is, menen betrokken instellingen niet verplicht te zijn tot onmiddellijke terugbetaling. Zoals vermeld hierboven, bestaat deze verplichting tot onmiddellijke terugbetaling immers enkel bij niet-toegestane transacties.

Bepaalde juristen stellen anderzijds dat de verplichting tot onmiddellijke terugbetaling mogelijk uitsluitend speelt voor niet-toegestane betalingstransacties zonder betaalinstrument. Betrokken auteurs erkennen echter dat de Europese Commissie hierover anders oordeelt. Bovendien wordt deze stelling ook tegengesproken in een vonnis van 11 februari 2022 van de Nederlandstalige rechtbank van eerste aanleg van Brussel.[6]

Aangezien Boek VII WER niet in een specifieke privaatrechtelijke sanctie voorziet, kan de betaler uitsluitend aanspraak maken op een vergoeding van de door de niet-naleving van deze verplichting veroorzaakte schade. Zo oordeelde het College van experten van Ombudsfin reeds dat de betaler geen schade lijdt bij niet-naleving van deze onmiddellijke terugbetalingsverplichting indien op grond van de definitieve aansprakelijkheidsregeling in artikel VII.44 WER komt vast te staan dat de aansprakelijkheid uiteindelijk bij de betaler ligt. Indien de definitieve aansprakelijkheid echter bij de betalingsdienstaanbieder ligt, zal de betaler minstens aanspraak kunnen maken op intresten aan de wettelijke intrestvoet vanaf de datum waarop de creditering conform artikel VII.43 WER diende te gebeuren.

[6] In de overige door Ombudsfin gekende rechtspraak wordt geen of weinig aandacht besteed aan deze problematiek.

4.3. Aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties

4.3.1. Basisgedachte

De betalingsdienstaanbieder is gehouden om structuren op te zetten of te organiseren binnen zijn onderneming waardoor betalingstransacties op een veilige manier kunnen plaatsvinden. In principe is het dan ook de betalingsdienstaanbieder die in de eerste plaats ter verantwoording moet worden geroepen voor het goed functioneren van het betalingsverkeer. Van de gemiddelde betaler kan immers niet verwacht worden dat hij een volledige kennis van dit technische proces heeft.

In de voorbereidende werken bij de wet van 19 juli 2018 houdende wijziging en invoering van bepalingen inzake betalingsdiensten in verschillende boeken van het Wetboek van Economisch Recht wordt uitdrukkelijk gesteld dat deze regeling in geval van twijfel in het voordeel van de betaler geïnterpreteerd moet worden. Deze regeling heeft immers tot doel de betaler een maximale bescherming te verzekeren.

4.3.2. Betwiste betalingstransacties voor én na kennisgeving van de fraude

Het WER maakt een onderscheid tussen transacties die hebben plaatsgevonden voor en na de kennisgeving van het verlies, de diefstal, het onrechtmatige gebruik of het niet-toegestane gebruik van het betaalinstrument.

4.3.2.1. Verplichting tot onverwijlde kennisgeving

De betalingsdienstgebruiker is krachtens artikel VII.38 WER verplicht de betalingsdienstaanbieder of de door hem aangeduide entiteit (veelal Card Stop) onverwijld in kennis te stellen van het verlies, de diefstal, het onrechtmatige gebruik of het niet-toegestane gebruik van het betaalinstrument, van zodra hij zich hiervan rekenschap geeft.

Verder stelt artikel VII.41 WER dat de betalingsdienstgebruiker alleen rechtzetting van een niet-toegestane transactie zal kunnen verkrijgen indien de betalingsdienstgebruiker de betalingsdienstaanbieder onverwijld en uiterlijk dertien maanden na de valutadatum van de debitering of creditering kennisgeeft van zulke transactie. Ondertussen is het in de rechtsleer min of meer aanvaard dat betrokken criteria twee onderscheiden en cumulatieve voorwaarden betreffen. Dit werd ook bevestigd door de Europese Commissie. Dit betekent dat de betalingsdienstgebruiker na vaststelling van de fraude in ieder geval onverwijld kennis hiervan moet geven aan zijn financiële instelling. Stelt hij de fraude echter pas vast dertien maanden na de debitering (of later), dan ontstaat een onweerlegbaar vermoeden dat de betaler de betalingstransactie heeft aanvaard en zal hij de niet-toegestane transacties ten aanzien van de bank niet meer succesvol kunnen betwisten op basis van Boek VII WER. Anderzijds, wanneer de betalingsdienstgebruiker wel overgaat tot kennisgeving binnen een termijn van dertien maanden, maar dit niet onverwijld doet na vaststelling, wordt de betalingsdienstgebruiker weerlegbaar vermoed de transactie te hebben aanvaard. In dit geval zal hij de transactie dus wel nog kunnen betwisten.

Voorwaarde bij bovenvermelde termijnen is wel dat de betalingsdienstaanbieder zijn wettelijke informatieverplichtingen, met name het tijdig en correct informeren over de betalingstransactie, heeft vervuld. Indien de betalingsdienstaanbieder deze informatieverplichtingen niet heeft nageleefd, zal de betaler ook na bovenvermelde termijnen verrichtingen succesvol kunnen betwisten. Hieromtrent raadt Ombudsfin de betaler aan op regelmatige basis zijn rekeninguittreksels en uitgavenstaten na te kijken.

In een arrest van 2 september 2021 sprak het Hof van Justitie zich uit over de vraag of de betaler na het verstrijken van de voormelde termijn van dertien maanden toch nog op basis van een andere aansprakelijkheidsregeling, in casu het gemeen recht, meer bepaald de zorgvuldigheidsplicht in hoofde van de betalingsdienstaanbieder, en met inachtname van de overeenkomstige verjaringstermijnen zijn bank aansprakelijk kan stellen. Het Hof van Justitie heeft deze vraag negatief beantwoord en verwees hiervoor naar de maximaal harmoniserende werking[7] van PSD I en de bedoeling door middel van deze richtlijn een interne markt te creëren. Aangezien ook PSD II een maximale harmonisatie beoogt, lijkt het ons dat betrokken arrest van het Hof van Justitie overeenkomstig kan worden toegepast op het huidige artikel VII.41 WER.

7 Onze Belgische wetgeving inzake niet-toegestane betalingstransactie is immers het resultaat van de omzetting van Europese richtlijnen. Deze richtlijnen zijn maximaal harmoniserend, wat betekent dat de lidstaten bij de omzetting ervan naar nationaal recht geen extra bescherming voor de betaler mogen voorzien.

Van zijn kant is de betalingsdienstaanbieder op basis van artikel VII.39 WER ertoe gehouden om ervoor te zorgen dat de betaler te allen tijde (24/7) deze kennisgeving kan doen. Bovendien stelt artikel VII.39, 4° WER dat de betaler deze kennisgeving kosteloos moet kunnen doen. Het WER regelt echter niet hoe de kennisgeving in artikel VII.41 WER dient te gebeuren. Bijgevolg houdt artikel VII.39, 3° WER geen verplichting in hoofde van de betalingsdienstaanbieder in om bijvoorbeeld een telefonische permanentie te voorzien. Zo kan de betalingsdienstaanbieder er bijvoorbeeld ook voor kiezen om de kennisgeving van de fraude per mail te laten verlopen. Hierbij kan echter de vraag worden gesteld of dit wel volstaat ten aanzien van klanten die niet over een emailadres beschikken. Deze problematiek is echter niet meer relevant sinds januari 2023. Op 23 januari 2023 verklaarde Alexia Bertrand, Staatssecretaris voor Begroting en Consumentenbescherming, immers dat alle banken sinds januari 2023 een klantendienst hebben die 24/7 bereikbaar is. Hoewel hiertoe geen wettelijke verplichting bestaat, voorzien banken vandaag dus wel degelijk een telefonische permanentie. Ombudsfin kan dit alleen maar aanmoedigen.

Artikel VII.189 WER voorziet dat de betalingsdienstaanbieder bij niet-naleving van de verplichting in artikel VII.39,3° WER[8] alle gevolgen van het gebruik van het betalingsinstrument door een niet-gerechtigde derde dient te dragen, ongeacht de omstandigheden (tenzij de betalingsdienstaanbieder bewijst dat de betaler bedrieglijk heeft gehandeld). Aangezien artikel VII.189 WER geen causaal verband tussen de miskenning van deze wettelijke verplichting en de niet-toegestane betalingstransactie vereist, zal de betaler dan ook niet de gevolgen moeten dragen voor de transacties die hebben plaatsgevonden voorafgaand aan het ogenblik waarop de betaler trachtte kennis te geven.

Op basis van de artikelen VII.22 en VII.21 WER moet de betalingsdienstaanbieder op een duurzame drager en voorafgaand aan het sluiten van de raamovereenkomst aan de betalingsdienstgebruiker informatie verstrekken over de wijze waarop de betalingsdienstgebruiker de betalingsdienstaanbieder in kennis moet stellen.

Ombudsfin stelt vast dat soms in één fraudedossier meerdere kennisgevingen van de fraude noodzakelijk zijn om alle betaalinstrumenten te blokkeren. Wanneer de fraudeur er bijvoorbeeld in geslaagd is een mobiele app, gelinkt aan de rekeningen van zijn slachtoffer, te installeren, zal het bij sommige banken onvoldoende zijn dat de betaalkaart via Card Stop geblokkeerd wordt. Bij deze banken zal de fraudeur dan geen gebruik meer kunnen maken van de kaartgegevens, maar wel nog frauduleuze verrichtingen kunnen uitvoeren via de nieuw geïnstalleerde app. Deze banken vragen in hun algemene bankvoorwaarden om een dubbele kennisgeving van de fraude te doen. Dit is niet altijd handig voor de betaler daar deze niet altijd een volledige kennis van de kennisgevingsprocedure heeft en bovendien vaak niet weet welke betaalinstrumenten de fraudeur al dan niet achterliggend geïnstalleerd heeft. Zo kan de betaler vaak onmogelijk weten dat een kennisgeving aan Card Stop niet volstaat om verdere schade te voorkomen. Vanuit de politiek is er dan ook vraag om dit te veranderen en een systeem te voorzien waarbij de betaler met één muisklik of telefonische oproep zowel zijn bankkaart, bankrekening als bankapp kan blokkeren. Men kan alleen maar hopen dat dit verzoek snel zal gehoord worden.

Naast de verplichting in artikel VII.22 WER om de betaler voorafgaand aan het sluiten van de raamovereenkomst te informeren over de wijze waarop de kennisgeving van de fraude dient te gebeuren, is Ombudsfin bovendien van mening dat de betalingsdienstaanbieder de kennisgevingsprocedure ook steeds duidelijk moet vermelden op zijn website. Bovendien moet deze informatie eenvoudig terug te vinden zijn (bv. op de startpagina van de website). Dit kan immers alleen maar bijdragen tot een vlotte kennisgeving van de fraude.

4.3.2.2. Belang van de kennisgeving

a) Aansprakelijkheid betalingsdienstaanbieder voor frauduleuze verrichtingen na kennisgeving

Op basis van artikel VII.39 WER is de betalingsdienstaanbieder verplicht te beletten dat het betaalinstrument nog kan worden gebruikt, nadat de kennisgeving van de fraude door de betaler gedaan is. Deze verplichting houdt een resultaatsverbintenis in.

8 De wetgever is in art. VII.189 WER vergeten de nummering aan te passen aan de nieuwe nummering na omzetting van PSD II. Zie ook art. 74, §3, lid 2 PSD II.

Artikel VII.44, §3 WER voorziet uitdrukkelijk dat het gebruik van het verloren, gestolen of wederrechtelijk toegeëigende betaalinstrument na kennisgeving geen financiële gevolgen voor de betaler kan hebben, tenzij de betalingsdienstaanbieder bewijst dat de betaler bedrieglijk gehandeld heeft. De betaler kan bijgevolg in geen ander geval aansprakelijk gesteld worden voor transacties die na de kennisgeving hebben plaatsgevonden, zelfs niet wanneer vaststaat dat hij zijn verplichtingen met grove nalatigheid heeft miskend.

De betalingsdienstaanbieder kan derhalve niet aan aansprakelijkheid ontkomen door bijvoorbeeld aan te tonen dat het betrokken (betaal)systeem niet toelaat om verder gebruik van het betaalinstrument na kennisgeving onmiddellijk te vermijden. Zo stelde Ombudsfin in een aantal dossiers vast dat de blokkering van de bankkaart via Card Stop niet alle gebruik van de fysieke kaart kon voorkomen. In betrokken dossiers kon de via Card Stop geblokkeerde kaart na blokkering toch nog gebruikt worden om met behulp van de kaartlezer codes te genereren en zo aan te melden via internetbankieren en overschrijvingen uit te voeren. De blokkering van de kaart voor aanmeldingen in internetbankieren en uitvoering van overschrijvingen werd in betrokken dossiers niet onmiddellijk, maar wel per batch verwerkt. Een via Card Stop geblokkeerde kaart mag in feite niet meer fysiek gebruikt kunnen worden, ook niet om met behulp van de kaartlezer codes te genereren en hiermee vervolgens online overschrijvingen te initiëren. Bij een correcte blokkering van de betaalkaart en een onmiddellijke verwerking hiervan zou in deze dossiers alle schade, ontstaan na het contact met Card Stop, kunnen zijn voorkomen. Ombudsfin stelt met voldoening vast dat banken in deze dossiers steeds tussengekomen zijn in alle schade die was ontstaan na de blokkering van de kaart.

Wat de betwisting van niet-toegestane betalingstransacties, uitgevoerd voorafgaand aan de kennisgeving, betreft, dienen de onder titels 3.3. tot en met 3.6. uiteengezette regels te worden gevolgd.

b) Recuperatiepoging

Het tijdstip van de kennisgeving van de fraude aan de financiële instelling is ook belangrijk omdat, vanaf dat moment, in hoofde van de financiële instelling een verplichting ontstaat om redelijke maatregelen te nemen om de frauduleus ontvreemde gelden te recupereren. Deze verplichting kadert binnen de algemene zorgplicht in hoofde van de bank. Van de financiële instelling wordt verwacht dat deze na de kennisgeving van de fraude zo snel mogelijk het nodige doet om, in de mate van het mogelijke, betwiste verrichtingen tegen te houden, eventuele begunstigde rekeningen, die bij deze zelfde instelling worden aangehouden, te blokkeren en een bericht te sturen naar iedere begunstigde financiële instelling met de vraag om de begunstigde rekening(en) te blokkeren en eventueel beschikbare fondsen terug te storten. Op deze manier worden vaak bepaalde (soms relatief grote) bedragen alsnog gerecupereerd.[9]

De vraag stelt zich in welke mate de betalingsdienstaanbieder aansprakelijk gesteld kan worden bij niet-naleving van deze recuperatieverplichting of bij het laattijdig nemen van recuperatiemaatregelen. Op basis van bovenvermeld arrest van het Hof van Justitie van 2 september 2021 zou kunnen worden geoordeeld dat dit niet mogelijk is en de aansprakelijkheidsregeling definitief geregeld wordt in Boek VII WER. Toch zal Ombudsfin in het kader van haar bemiddelingsopdracht de naleving van de recuperatieverplichting controleren en, indien nodig, de betrokken financiële instelling vragen om een voorstel tot tegemoetkoming in een deel van de schade te formuleren. De eventuele schade ten gevolge van laattijdige recuperatiemaatregelen zal hierbij vaak moeilijk te bepalen en vaak zelfs niet bewezen zijn. Jammer genoeg komen financiële instellingen op basis van dit argument slechts in een zeer beperkt aantal gevallen tussen.

4.3.3. Sterke cliëntenauthenticatie

4.3.3.1. Regelgeving

Krachtens artikel VII.44, § 2 WER dient de betaler geen eventuele financiële verliezen te dragen wanneer de betalingsdienstaanbieder van de betaler geen sterke cliëntauthenticatie verlangt, tenzij de betaler zelf frauduleus gehandeld heeft. In dergelijk geval kan de betaler dus niet aansprakelijk gesteld worden voor de niet-toegestane betalingstransactie.

[9] Het succes van deze recuperatiemaatregelen hangt logischerwijs af van een goede medewerking van de begunstigde bank. Wij stellen vast dat dat hiervan in de meeste gevallen sprake is wanneer de begunstigde bank een Belgische bank betreft. Helaas is de situatie vaak ingewikkelder wanneer deze bank in het buitenland is gevestigd.

Sterke cliëntenauthenticatie wordt in artikel I.9, 33/16° WER als volgt gedefinieerd: “authenticatie met gebruikmaking van twee of meer factoren die worden aangemerkt als «kennis» (iets wat alleen de gebruiker weet), “bezit” (iets wat alleen de gebruiker heeft) en “inherente eigenschap” (iets wat de gebruiker is) en die onderling onafhankelijk zijn, in die zin dat compromittering van één ervan geen afbreuk doet aan de betrouwbaarheid van de andere en die zodanig is opgezet dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd”. Van zodra twee van de voornoemde factoren gecombineerd worden, is sprake van een sterke cliëntenauthenticatie. De European Banking Authority (EBA) heeft in een opinie van 21 juni 2019 meer uitleg gegeven bij de invulling van deze begrippen. Voorbeelden van een bezitselement zijn de kaartgegevens, de bankkaart en de mobile banking-app. Voorbeelden van een kenniselement zijn de pincode van de betaalkaart en de toegangscode van de mobile banking-app. Voorbeelden van een inherente eigenschap zijn de vinger- en gezichtsscan.

Bij een online kredietkaartbetaling die uitsluitend geschiedt op basis van de kredietkaartgegevens, wat een bezits-element vormt, is op basis van bovenvermelde definitie en rekening houdende met de opinie van 21 juni 2019 van de EBA, geen sprake van sterke cliëntenauthenticatie. Er is anderzijds wel sprake van sterke cliëntenauthenticatie indien een online betaling wordt bevestigd door middel van een met de bankkaart, pincode en digipass gegenereerde responscode. Voor het aanmaken van deze responscode zijn immers de bankkaart (elektronische chip), een bezitselement, en de pincode, een kenniselement, vereist.

PSD II voorziet dat betalingsdienstaanbieders een sterke cliëntenauthenticatie dienen te voorzien wanneer een betaler zich online toegang tot zijn rekening verschaft, een elektronische betaling initieert of via een communicatiemiddel op afstand een handeling van eender welke aard uitvoert die een risico op betalingsfraude of andere vormen van misbruik met zich mee kan brengen. De regelgeving inzake de vereisten van sterke cliëntenauthenticatie kan verder worden teruggevonden in de Gedelegeerde Verordening van de Commissie van 27 november 2017 wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden (GV SCA).

In principe dienen betalingsdienstaanbieders dus in de in artikel 97, §1 van PSD II voorziene gevallen een sterke cliëntenauthenticatie te voorzien. De GV SCA voorziet echter een aantal vrijstellingen, waarbij onder bepaalde voorwaarden dus geen sterke cliëntenauthenticatie vereist is. Bekende voorbeelden waar geen sterke cliëntenauthenticatie moet worden toegepast, betreffen enerzijds elektronische betalingstransacties op afstand voor een bedrag kleiner dan 30 euro, waarvoor bijvoorbeeld uitsluitend kaartnummer, vervaldatum en CVC-code gevraagd worden, en anderzijds contactloze betalingen onder de 50 euro waarvoor geen pincode vereist is.

Hoewel de meeste voorziene vrijstellingen in de GV SCA duidelijk zijn, zal het toch niet altijd eenvoudig zijn om eenduidig te stellen wanneer een transactie al dan niet met sterke cliëntenauthenticatie moet worden bevestigd. Artikel 18 van de GV SCA voorziet immers dat betalingsdienstverleners geen sterke cliëntenauthenticatie dienen toe te passen bij elektronische betalingstransacties op afstand, wanneer betrokken betalingstransacties op basis van de analyse van de transactierisico’s (mechanisme voor transactiemonitoring) geïdentificeerd zijn als transacties die weinig risico opleveren. Deze bepaling voorziet verder een aantal cumulatieve voorwaarden waaraan een transactie moet voldoen opdat deze beschouwd kan worden als een transactie die weinig risico oplevert. Deze vrijstelling laat dus een zekere ruimte om te oordelen of sterke cliëntenauthenticatie al dan niet vereist is.

Wanneer een betaler het slachtoffer wordt van niet-toegestane betalingstransacties zonder sterke cliëntenauthenticatie, zal hij steeds (tenzij hij zelf frauduleus gehandeld heeft) vrijgesteld zijn van aansprakelijkheid. Hij zal niet aansprakelijk kunnen worden gesteld wanneer hij bepaalde verplichtingen met grove nalatigheid heeft miskend. Dit geldt ook wanneer de betalingsdienstaanbieder op grond van de GV SCA wordt vrijgesteld van de verplichting tot sterke cliëntenauthenticatie. Met andere woorden, indien de betalingsdienstaanbieder ervoor kiest in bepaalde gevallen geen sterke cliëntenauthenticatie te vereisen, dan draagt hij daar zelf het risico van.

Wanneer de afwezigheid van sterke cliëntenauthenticatie te wijten is aan het feit dat de begunstigde of zijn betalingsdienstaanbieder geen sterke cliëntenauthenticatie aanvaardt, zal de betaler nog steeds op basis van artikel VII.44, §2 WER zijn eigen betalingsdienstaanbieder kunnen aanspreken tot vergoeding van de schade. Op basis van dit artikel zal de betalingsdienstaanbieder van het slachtoffer

zich kunnen wenden tot de (betalingsdienstaanbieder van) de begunstigde.

Het spreekt voor zich dat niet-Europese handelaars en betalingsdienstaanbieders niet gebonden zijn door de Europese verplichtingen inzake sterke cliëntenauthenticatie. Wanneer de betaler het slachtoffer wordt van niet-toegestane betalingstransacties zonder sterke cliëntenauthenticatie ten gunste van niet-Europese handelaars, zal de betaler zich toch nog steeds op basis van artikel VII.44, §2 WER tot zijn betalingsdienstaanbieder kunnen richten om een volledige vergoeding van zijn schade te vragen. Zo oordeelde ook het College van experten van Ombudsfin, verwijzend naar artikel VII.2, §1, lid 3 WER, waarin het toepassingsgebied van de betrokken hoofdstukken in Boek VII WER geregeld wordt. Artikel VII.2, §1, lid 3 WER vermeldt immers dat betrokken regels van toepassing zijn op betalingstransacties in alle valuta waarbij slechts een van de betalingsdienstaanbieders zich in een lidstaat bevindt, met betrekking tot de delen van de betalingstransactie die binnen een lidstaat worden uitgevoerd.

4.3.3.2. Toepassing: de frauduleuze installatie van Apple Pay

In een niet gepubliceerd vonnis van 11 februari 2022 werd door de Nederlandstalige rechtbank van eerste aanleg van Brussel beslist dat er sprake is van sterke cliëntenauthenticatie in gevallen waarbij een fraudeur erin slaagt om een bancaire mobiele app, gekoppeld aan de rekeningen van zijn slachtoffer, te installeren op een eigen toestel (wat gebeurt door middel van één of meerdere met de bankkaart van het slachtoffer en een digipass gegenereerde responscode(s), dus met sterke cliëntenauthenticatie) en vervolgens met behulp van deze app frauduleuze verrichtingen te bevestigen door middel van een door de fraudeur bij installatie van de app gekozen code of een vinger- of gezichtsscan.

Voormeld vonnis belet echter niet dat Ombudsfin soms nog steeds geconfronteerd wordt met interessante cases waarbij in vraag kan worden gesteld of bepaalde verrichtingen die via een nieuw geïnstalleerde app uitgevoerd werden al dan niet met sterke cliëntenauthenticatie zijn bevestigd. In 2021 had Ombudsfin bijvoorbeeld interessante discussies met een bepaalde kredietinstelling inzake de installatieprocedure van Apple Pay bij betrokken bank. In de aan Ombudsfin voorgelegde dossiers was een fraudeur er in geslaagd om een betaalkaart van zijn slachtoffer aan de eigen Apple Pay-applicatie op een eigen (Apple-)toestel te koppelen, waarna hij vervolgens via deze applicatie zowel online als ter plaatse bij de handelaar frauduleuze betalingen kon uitvoeren. Betrokken verrichtingen kunnen via Apple Pay worden bevestigd door middel van een vooraf gekozen toegangscode (door de fraudeur) of door middel van een vinger- of gezichtsscan (van de fraudeur).

De vraag die zich in betrokken dossiers stelde, was of Apple Pay al dan niet met sterke cliëntenauthenticatie geïnstalleerd werd. Betrokken financiële instelling voorzag twee mogelijke installatieprocedures.[10]

(i) In sommige dossiers slaagde de fraudeur erin om eerst de mobile banking-app van de bank zelf te installeren op een eigen toestel, om vervolgens vanuit deze app de betaalkaart van het slachtoffer te koppelen aan de Apple Pay-applicatie van de fraudeur. De mobile banking-app van de bank wordt steeds minstens op basis van één of meerdere met de bankkaart, pincode en digipass gegenereerde code(s) geïnstalleerd. In deze gevallen was sprake van sterke cliëntenauthenticatie.

(ii) Daarnaast slaagden fraudeurs er eveneens in om de betaalkaart van hun slachtoffer aan de eigen Apple Pay-applicatie te koppelen vanuit de 'wallet'-applicatie op het toestel van de fraudeur. Dit was mogelijk op basis van de kaartgegevens en een activatiecode die veelal per sms naar het gsm-nummer van het slachtoffer verstuurd werd. In deze dossiers stelt Ombudsfin dat de betaalkaart niet met sterke cliëntenauthenticatie wordt gekoppeld. Rekening houdende met de opinie van de EBA van 21 juni 2019 dienen zowel de kaartgegevens als de per sms verstuurde activatiecode immers als bezitselementen beschouwd te worden. Deze activatiecode kan volgens de EBA niet als kenniselement beschouwd worden, aangezien volgens de EBA pas sprake is van een kenniselement indien dit reeds bestaat voorafgaand aan de initiatie van een transactie of online toegang.

[10] Let op: de installatieprocedure van Apple Pay kan verschillen van bank tot bank.

Ombudsfin stelt vast dat betrokken bank, rekening houdend met voorgaande elementen, nu steeds een tussenkomst aanbiedt in de fraudedossiers die onder de tweede installatieprocedure vallen.

4.3.4. Basisregel: aansprakelijkheid van de betalingsdienstaanbieder na aftrek van een franchise van 50 euro

Wat de aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties voorafgaand aan de kennisgeving en verlopen via sterke cliëntauthenticatie betreft, voorziet artikel VII.44, §1, lid 1 WER dat de betaler tot aan de kennisgeving het verlies slechts moet dragen tot een bedrag van ten hoogste 50 euro met betrekking tot alle niet-toegestane betalingstransacties die voortvloeien uit het gebruik van een verloren of gestolen betaalinstrument of uit het onrechtmatige gebruik van een betaalinstrument. De betaler draagt hier dus slechts een beperkt risico, namelijk een beperkte franchise van 50 euro. Deze franchise geldt voor de totaliteit van de niet-toegestane betalingstransacties die met een betaalinstrument plaatsvinden en dus niet per transactie. Wanneer een fraudeur erin slaagt om niet-toegestane betalingstransacties uit te voeren met meerdere betaalinstrumenten, zal deze franchise echter per betaalinstrument moeten worden toegepast.

Deze basisregel is uitsluitend van toepassing indien geen van de onder 3.5 en 3.6 besproken gevallen toepassing vindt. Één uitzondering, op basis waarvan de betaler geen enkele schade draagt wanneer het verlies veroorzaakt is door het handelen of nalaten van een werknemer, agent of bijkantoor van een betalingsdienstaanbieder of van een entiteit waaraan diens activiteiten werden uitbesteed, wordt niet verder toegelicht, aangezien Ombudsfin deze regel tot dusver in de praktijk nog niet heeft moeten toepassen.

4.3.5. Detecteerbaarheid van de fraude

4.3.5.1. Regeling en toepassing

Artikel VII.44, § 1, lid 2, 1° WER voorziet dat de betaler geen enkel verlies, dus ook niet de franchise van 50 euro, dient te dragen indien het verlies, de diefstal of het onrechtmatige gebruik van een betaalinstrument niet kon worden vastgesteld door de betaler voordat een betaling plaatsvond, tenzij de betaler zelf frauduleus heeft gehandeld. Dit betekent dus dat als het slachtoffer van een fraudegeval het onrechtmatige gebruik van zijn betaalinstrument vooraf niet kon detecteren, hij niet aansprakelijk gesteld kan worden voor de fraude.

De voorbereidende werken bij de wet stellen dat dit artikel bijvoorbeeld kan worden toegepast in bepaalde gevallen van hacking en phishing van persoonlijke beveiligingsgegevens of een skimming van kaarten. Verder wordt verduidelijkt dat het 'onrechtmatige gebruik' ook bijvoorbeeld gevallen dekt waarbij de betalingsgegevens ontvreemd zijn terwijl de betaler nog in het bezit is van zijn betaalinstrument (bv. bij phishing of cloning van het betaalinstrument).

De vraag naar de mogelijkheid tot het voorafgaandelijk detecteren van een fraudegeval moet worden beoordeeld rekening houdend met alle feiten. Het is bijgevolg niet zo dat een slachtoffer van bijvoorbeeld phishing automatisch een beroep kan doen op artikel VII.44, §1, lid 2, 1° WER en bijgevolg geen enkel verlies zal moeten dragen. In het licht van de concrete omstandigheden zal eerst moeten worden nagegaan of betrokken bepaling al dan niet toepassing

vindt. Indien deze bepaling niet van toepassing zou zijn, moet worden teruggevallen op de basisregel en dient een beoordeling van een eventuele grove nalatigheid te gebeuren.

Deze regel voorziet dus dat de betaler geen enkel verlies dient te dragen indien het onrechtmatig gebruik van het betaalinstrument niet kon worden vastgesteld voordat een betaling plaatsvond. Hierbij moet worden beoordeeld of, rekening houdend met alle omstandigheden van het geval, een gemiddelde betaler de phishing had moeten detecteren. De centrale vraag hierbij is dus of, rekening houdend met het gedrag van de gemiddelde betaler, sprake is van een (gewone) onzorgvuldigheid.

In de praktijk zal Ombudsfin bij de beoordeling van de detecteerbaarheid van de fraude met verschillende zaken rekening houden. Zo moet onder meer rekening gehouden worden met de wijze waarop het frauduleuze bericht is opgesteld en of dit al dan niet grammaticale of spellingsfouten bevat. Ook het door de fraudeur gebruikte emailadres, vanwaar de frauduleuze mail afkomstig was, is bepalend. Ook de gebruikte link en de URL van de frauduleuze website zijn relevant. Verder gaat Ombudsfin ook na of de betaler de fraude bijvoorbeeld kon vaststellen op basis van de te volgen procedure. Zo is de fraude bijvoorbeeld veelal detecteerbaar wanneer de klant met zijn bankkaart en digipass codes moet genereren voor de ontvangst van een bepaald bedrag. Wanneer aan een betaler gevraagd wordt om telefonisch bepaalde codes door te geven, om eender welke reden, maakt dit de fraude ook detecteerbaar. Verder zijn ook de concrete omstandigheden van het fraudegeval relevant. Zo kan de fraude bijvoorbeeld als detecteerbaar worden geacht wanneer men bijvoorbeeld reageert op een frauduleuze sms die zogezegd afkomstig is van itsme en de blokkering van het itsme-account van de ontvanger betreft, terwijl de betrokkene nog nooit van itsme gebruik heeft gemaakt. Verder kan de fraude bijvoorbeeld detecteerbaar zijn, doordat op de digipass van de bank bepaalde contextboodschappen verschijnen. Wanneer op de digipass een contextboodschap betreffende de installatie van een nieuwe app verschijnt, terwijl de betaler denkt dat hij door zijn handelingen bijvoorbeeld de ontvangst van een betaling bevestigt of een betaling uitvoert, zal de contextboodschap op de digipass, indien deze duidelijk is opgesteld, de fraude detecteerbaar maken. Ook sturen banken sinds enkele jaren verschillende sms'en na een nieuwe installatie van de mobiele app van de bank. Onder titel 3.7. wordt verder ingegaan op de impact van deze berichten op de aansprakelijkheidsverdeling.

Het WER regelt de bewijslast inzake de voorafgaandelijke detecteerbaarheid van de fraude door de betaler niet uitdrukkelijk. Daar artikel VII.44, §1, lid 2, 1° WER volgens Ombudsfin als uitzondering in het voordeel van de betaler moet beschouwd worden op de regel dat de betalingsdienstaanbieder het verlies dient te dragen, na aftrek van een franchise van 50 euro én rekening houdende met het gemeen bewijsrecht, is Ombudsfin van mening dat het aan de betaler is om elementen te leveren om te bewijzen dat de fraude op voorhand niet kon worden gedetecteerd.

De betaler die zich wenst te beroepen op de regel in artikel VII.44, §1, lid 2, 1° WER zal dus elementen moeten aanleveren om aan te tonen dat de fraude op voorhand niet kon worden gedetecteerd. Ombudsfin wordt vaak geconfronteerd met klachten waarbij de betaler bijvoorbeeld geen kopie van het frauduleus bericht of de communicatie met de fraudeur (bv. via Messenger of WhatsApp) kan voorleggen omdat hij dit verwijderd heeft. In deze gevallen zal de betaler ook vaak niet meer weten op welke frauduleuze link hij geklikt heeft. In deze dossiers zal de betaler zich niet succesvol kunnen beroepen op artikel VII.44, §1, lid 2, 1° WER.

4.3.5.2. Ongeacht grove nalatigheid

Onder titel 3.6. staat uitgelegd dat op de basisregel nog een andere uitzondering voorzien is voor gevallen van grove nalatigheid in hoofde van de betaler. Artikel VII.44, §1, lid 4 WER voorziet immers dat de betaler alle verliezen in verband met niet-toegestane betalingstransacties dient te dragen indien de betaler deze heeft geleden doordat hij door grove nalatigheid bepaalde verplichtingen niet is nagekomen.

Ombudsfin stelt vast dat de manier waarop artikel VII.44, §1 WER is opgesteld (volgorde van de verschillende hypotheses) onduidelijkheid schept over de verhouding tussen het tweede en vierde lid van artikel VII.44, §1 WER. De vraag stelt zich met andere woorden of de uitzondering bij grove nalatigheid al dan niet geldt voor gevallen die onder artikel VII.44, §1; lid 2, 1° WER vallen. Met andere woorden, indien vaststaat dat de betaler de fraude op voorhand niet kon

vaststellen, zal hij in dergelijk geval automatisch op basis van artikel VII.44, §1, lid 2, 1° WER de betalingsdienstaanbieder kunnen aanspreken tot terugbetaling van de volledige schade, ongeacht enige grove nalatigheid, of moet eerst worden onderzocht of de betaler al dan niet grof nalatig geweest is?

In de rechtsleer wordt over het algemeen het standpunt ingenomen dat het al dan niet bestaan van een grove nalatigheid in hoofde van het slachtoffer van de fraude in de hypothese dat de betaler de fraude voorafgaandelijk niet kon detecteren, geen rol speelt. Dit betekent dat wanneer betrokken wetsartikel (art. VII.44, § 1, lid 2, 1° WER) van toepassing is, de betaler geen enkel verlies zal moeten dragen, ook wanneer hij grof nalatig is geweest. Dergelijke invulling blijkt immers uitdrukkelijk uit de bewoordingen van de wet aangezien de wet bij deze hypothese geen expliciete uitzondering voorziet voor grove nalatigheid. Bovendien wordt in het vierde lid van artikel VII.44, §1 WER (inzake grove nalatigheid) uitsluitend afgeweken van het eerste, en dus niet van het tweede, lid. Bovendien kan ter verdediging van dit standpunt verwezen worden naar overweging 71 van PSD II, waar vermeld staat dat er geen aansprakelijkheid mag zijn indien de betaler zich niet van het verlies, de diefstal of het onrechtmatig gebruik van het betaalinstrument bewust kon zijn.

Ombudsfin stelt vast dat in de rechtspraak vaak weinig of geen aandacht wordt gegeven aan dit vraagstuk. In een vonnis van 23 maart 2021 heeft de ondernemingsrechtbank van Leuven wel uitdrukkelijk bevestigd dat lid 2 van artikel VII.44, §1, lid 2 WER een bijzondere regel vormt die voorrang heeft op het vierde lid. Dit werd eveneens bevestigd in een vonnis van de ondernemingsrechtbank van Antwerpen.

Anderzijds sprak de Nederlandstalige rechtbank van eerste aanleg van Brussel in een vonnis van 4 april 2022 bovenvermelde stelling tegen. Hierbij vermeldde de rechtbank dat het tweede en vierde lid van artikel VII.44, §1 WER ieder een eigen, zelfstandige uitzondering, in tegengestelde richting, vormen op het principe van artikel VII.44, §1, lid 1 WER.

Rekening houdend met het principe dat de regeling in artikel VII.44 WER in geval van twijfel in het voordeel van de betaler geïnterpreteerd moet worden, is Ombudsfin van mening dat de eerste stelling, volgens dewelke de uitzondering bij grove nalatigheid dus niet speelt voor gevallen die onder artikel VII.44, §1, lid 2 WER vallen, het voordeel geniet.

Het belang van deze discussie mag echter niet worden overschat, aangezien de gevallen waarin het slachtoffer grof nalatig was terwijl de fraude tegelijkertijd niet voorafgaandelijk kon worden gedetecteerd, volgens de ervaring van Ombudsfin uiterst zeldzaam zijn.

4.3.6. Grove nalatigheid, fraude of opzet in hoofde van de betaler

Wanneer artikel VII.44, §1, lid 2, 1° WER geen toepassing vindt, doordat vaststaat dat fraude op voorhand door de betaler kon worden vastgesteld of de betaler onvoldoende elementen levert om aan te tonen dat de fraude op voorhand niet kon worden gedetecteerd, moet worden teruggevallen op de basisregel in artikel VII.44 WER. Op

basis hiervan dient de betalingsdienstaanbieder tussen te komen in de schade, na aftrek van een franchise van 50 euro.

Artikel VII.44, §1, lid 4 WER voorziet dat de betaler, in tegenstelling tot hetgeen voorzien wordt door de basisregel, alle verliezen dient te dragen indien hij verlies ten gevolge van niet-toegestane betalingstransacties geleden heeft doordat hij frauduleus heeft gehandeld of opzettelijk of door grove nalatigheid bepaalde verplichtingen genoemd in artikel VII.38 WER niet is nagekomen.

4.3.6.1. Beoordeling grove nalatigheid

Artikel VII.38 WER legt volgende verplichtingen op aan de betaler:

- De betaler dient het betaalinstrument overeenkomstig de voorwaarden die op de uitgifte en het gebruik van het betaalinstrument van toepassing zijn te gebruiken. Deze voorwaarden worden contractueel vastgelegd. Ze moeten objectief, niet-discriminerend en evenredig zijn. De voorbereidende werken bij de wet verduidelijken dat dit laatste vooral de bepalingen tot het veilig bewaren van de betaalinstrumenten en de persoonlijke beveiligingsgegevens betreft.
- De betaler is verplicht de betalingsdienstaanbieder of de door hem aangeduide entiteit onverwijld op de hoogte te brengen, van zodra hij het verlies, de diefstal of het onrechtmatige gebruik van zijn betaalinstrument vaststelt.
- Teneinde voorgaande verplichtingen na te leven, dient de betalingsdienstgebruiker alle redelijke maatregelen te nemen om de veiligheid van het betaalinstrument en de persoonlijke beveiligingsgegevens ervan te waarborgen. Dit van zodra hij het betaalinstrument ontvangen heeft.

PSD II en het WER bevatten geen definitie voor het begrip 'grove nalatigheid'. In overweging 72 bij PSD II staat wel uitdrukkelijk vermeld dat een grove nalatigheid meer dan louter een nalatigheid dient in te houden. Het moet gaan om gedrag dat een aanzienlijke mate van onvoorzichtigheid vertoont. Bijgevolg mag men niet te licht tot het bestaan van een grove nalatigheid besluiten. Daar deze regel, waarbij de betaler dus de volledige schade dient te dragen indien hij door grove nalatigheid bepaalde verplichtingen niet heeft nageleefd, een uitzondering vormt op het hoge beschermingsniveau dat PSD II beoogt te voorzien, dient het concept 'grove nalatigheid' in ieder geval eng te worden ingevuld. Het moet gaan om een zware fout of onzorgvuldigheid, die dermate excessief is dat ze niet begrijpelijk is voor een redelijk persoon. Het moet gaan om een gedraging die een redelijk zorgvuldig betaler nooit zou stellen. Ook in de rechtspraak wordt gebruik gemaakt van deze of een soortgelijke definitie. Voor de beoordeling van de grove nalatigheid zal Ombudsfin rekening houden met dezelfde elementen als bij de beoordeling van de detecteerbaarheid van de fraude, zij

het dat hier moet worden nagegaan of sprake is van een zeer zware onzorgvuldigheid, in plaats van een 'gewone' onzorgvuldigheid.

Artikel VII.44, §4, lid 3 WER bepaalt dat voor de beoordeling van de nalatigheid rekening moet worden gehouden met het geheel van de feitelijke omstandigheden. Dit betekent dat een globale beoordeling moet gebeuren van alle relevante feitelijke gegevens. Zo kan een reeks van feitelijke elementen die op zichzelf niet noodzakelijk een grove nalatigheid vormen toch in hun geheel beschouwd worden als een grove nalatigheid. De beoordeling van de grove nalatigheid moet volledig gebeuren, wat betekent dat men deze ook niet mag laten afhangen van één enkel feitelijk element.

Verder bevat artikel VII.44, §4, lid 2 WER een niet-limitatieve opsomming van gedragingen die als grove nalatigheid moeten worden beschouwd. Dit betreffen louter voorbeelden van grove nalatigheid, wat dus betekent dat ook andere gedragingen als grove nalatigheid beschouwd kunnen worden. Het WER geeft volgende voorbeelden:

- Het feit, voor de betaler, zijn gepersonaliseerde veiligheidsgegevens, zoals zijn identificatienummer of enige andere code in een gemakkelijk herkenbare vorm te noteren, en met name op het betaalinstrument of op een voorwerp of een document dat de betaler bij het instrument bewaart of met dat instrument bij zich draagt;
- Het feit van de betalingsdienstaanbieder, of de door laatstgenoemde aangeduide entiteit, niet onverwijld in kennis te hebben gesteld van het verlies of de diefstal.

In de memorie van toelichting bij de wet wordt echter benadrukt dat ook in de hierboven opgesomde gevallen voor de beoordeling van de grove nalatigheid rekening gehouden moet worden met alle feitelijke omstandigheden. Men kan dus stellen dat in bovenvermelde gevallen in de regel sprake is van een grove nalatigheid, maar dat feitelijke omstandigheden met zich kunnen brengen dat uiteindelijk toch niet tot een grove nalatigheid wordt besloten.

Ombudsfin stelt verder vast dat vele financiële instellingen in hun algemene voorwaarden contractueel vastleggen welke gedragingen als grove nalatigheid moeten worden bestempeld. Ombudsfin is van mening dat dergelijke bedingen de beoordelingsvrijheid niet mogen uitsluiten. De gedragingen die door de reglementen van de bank als grove nalatigheid worden aangeduid, mogen bijgevolg volgens Ombudsfin niet automatisch als grove nalatigheid worden beschouwd. Ook in deze gevallen dient bij de beoordeling van de grove nalatigheid dus rekening gehouden te worden met het geheel van de feitelijke omstandigheden. De bepalingen inzake de aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties zijn immers van dwingend recht. Dit brengt mee dat de rechten van de betaler niet kunnen worden ingeperkt. De algemene voorwaarden van een financiële instelling kunnen de aansprakelijkheid van de betaler niet uitbreiden.

Contractuele bedingen waarin bepaald wordt welke gedragingen als grove nalatigheid worden beschouwd, kunnen echter wel relevant zijn bij de beoordeling van de grove nalatigheid door de rechter. Door contractueel bepaalde gedragingen als grove nalatigheid te bestempelen, wordt de betaler als het ware gewezen op het risicogehalte van deze gedragingen.

Tot slot oordeelde het hof van beroep van Antwerpen dat de grove nalatigheid moet worden beoordeeld volgens het criterium van de veronderstelde gedragswijze van een normaal zorgvuldig en omzichtig betaler geplaatst in dezelfde concrete externe omstandigheden. Het hof van beroep voegde hier uitdrukkelijk aan toe dat hierbij geen rekening gehouden mag worden met kenmerken eigen aan de betaler, zoals in casu de leeftijd van de betaler. Dit betekent met andere woorden dat de grove nalatigheid in abstracto beoordeeld moet worden. Volgens Ombudsfin betekent dit echter niet dat geen rekening gehouden mag worden met de professionele ervaring en historiek van de klant (bv. 'recidive': betaler die tweemaal slachtoffer wordt van een identiek fraudegeval).

De beoordeling van de grove nalatigheid zal steeds geval per geval moeten gebeuren. Het is dan ook moeilijk om eenduidig conclusies te trekken uit de tamelijk beperkte rechtspraak. Men kan nooit garanderen wat de rechter zal beslissen. Bovendien is deze beoordeling ook in zekere zin onderhevig aan evolutie. Vandaag weet de gemiddelde betaler immers meer over phishing dan bijvoorbeeld 3 jaar geleden.

4.3.6.2. Bewijslast

Artikel VII.44, §4, lid 1 WER bepaalt dat de bewijslast inzake bedrog, opzet of grove nalatigheid aan de betalingsdienstaanbieder toekomt. Verder stelt artikel VII.44, §4,

lid 3 WER dat het gebruik van het betaalmiddel met de code die enkel door de betalingsdienstgebruiker gekend is geen voldoende vermoeden vormt van nalatigheid vanwege deze laatste. Zoals vermeld, voorziet de wet dat het gebruik van een betaalinstrument, dat door de betalingsdienstaanbieder is geregistreerd, op zichzelf niet noodzakelijkerwijze afdoende bewijst dat de betalingstransactie door de betaler is toegestaan of dat de betaler frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen niet is nagekomen. Verder dient de betalingsdienstaanbieder sinds 9 augustus 2018 ondersteunend bewijs te leveren om fraude of grove nalatigheid van de zijde van de betaler te bewijzen.

In de memorie van toelichting staat uitdrukkelijk dat geen vermoeden van grove nalatigheid gehanteerd mag worden, in toepassing waarvan de betaler aan zijn verplichtingen zou hebben verzaakt, of een grove nalatigheid zou hebben begaan, of bedrieglijk zou hebben gehandeld. Een dergelijk vermoeden zou immers in belangrijke mate afbreuk doen aan de bescherming die de wet aan de betaler biedt. Het verbod om een vermoeden van grove nalatigheid te hanteren, verhindert echter niet dat andere ernstige en met elkaar overeenstemmende vermoedens worden gebruikt om tot de aanwezigheid van een grove nalatigheid te besluiten.

In de praktijk wordt Ombudsfin vaak geconfronteerd met fraudegevallen waarbij het feitenrelaas van de betaler over het fraudeverloop niet volledig overeenstemt met de technisch gegevens van de bank. Zo is het bijvoorbeeld mogelijk dat de betaler verklaart geen met digipass gegenereerde codes op de frauduleuze website te hebben ingevoerd, terwijl de bank bijvoorbeeld kan aantonen dat fraudeur voor iedere betwiste verrichting een dergelijk responscode heeft ingevoerd. Een ander voorbeeld betreft gevallen waarbij de bank kan aantonen dat de fraudeur een mobiele app, gekoppeld aan de rekeningen van zijn slachtoffer geïnstalleerd heeft en er voor de activatie van deze app een activatiecode per sms naar het door de bank gekende nummer van de betaler werd verstuurd, maar de betaler ontkent een dergelijke code te hebben ontvangen of gebruikt. In deze gevallen zou op basis van ernstige en met elkaar overeenstemmende vermoedens kunnen worden vermoed dat de betaler toch betrokken codes ingevoerd heeft op de frauduleuze website. Op basis van dit vermoeden kan vervolgens, afhankelijk van de concrete omstandigheden besloten worden tot een grove nalatigheid. Ombudsfin past dit in de praktijk echter niet toe. Daar Ombudsfin de verklaringen van de klant niet kan controleren en verder niet uitsluit dat de fraudeur toch technisch op één of andere, niet gekende, wijze de codes kan hebben onderschept, spreekt Ombudsfin zich voorzichtigheidshalve in dergelijke gevallen niet uit over een eventuele grove nalatigheid.

4.3.7. Toepassingsgeval bij detecteerbaarheid van de fraude en grove nalatigheid: berichten verstuurd naar aanleiding van de nieuwe installatie van de mobiele bankapp

In sommige gevallen slaagt een fraudeur erin om aan de hand van de verkregen of onderschepte gegevens een mobiele app, gekoppeld aan de rekeningen van zijn slachtoffer, op een eigen toestel te installeren. Via deze app krijgt de fraudeur vervolgens toegang tot de rekeningen van zijn slachtoffer, waarna hij vervolgens frauduleuze betalingen en overschrijvingen kan bevestigen door middel van een door de fraudeur bij installatie van de app gekozen code. In deze dossiers kan de schade vaak zeer hoog oplopen.

Doorheen de jaren hebben financiële instellingen bepaalde maatregelen genomen om de schade in dergelijk gevallen hetzij te voorkomen, hetzij zo veel mogelijk te beperken. Zo stelt Ombudsfin onder meer vast dat steeds meer banken, conform de aanbevelingen van Ombudsfin, de laatste jaren de installatieprocedure voor hun mobiele app hebben aangepast door met extra activatiecodes of -linken te werken, die per sms of mail naar het door de bank gekende gsm-nummer of emailadres worden verstuurd. Toch zijn er anderzijds ook nog steeds bepaalde financiële instellingen die ervoor kiezen om louter een bericht met informatie over de installatie van een nieuwe app te versturen, zonder een bijkomende handeling van de betaler te vragen om betrokken applicatie te activeren.

Hieronder wordt ingegaan op de impact van de door de bank verstuurde berichten inzake de frauduleuze installatie en/of activatie van een nieuwe mobiele app.

a) <u>Uitsluitend bericht met informatie over de installatie van een nieuwe app – geen activatiecode of -link</u>

Sommige financiële instellingen kiezen ervoor om na de installatie van een nieuwe mobiele applicatie uitsluitend een bericht te versturen naar de betaler om deze te informeren

over de installatie van deze app. Betrokken bericht wordt in dergelijk geval per sms of mail gestuurd naar het in de systemen van de bank geregistreerde gsm-nummer of emailadres van de klant. Deze berichten bevatten vaak ook instructies voor de betaler indien hij deze app niet zelf geïnstalleerd zou hebben. Deze instellingen sturen dus geen (tweede) bericht met een extra activatiecode of –link.

Dergelijke kennisgeving over de installatie van een nieuwe mobiele applicatie zal uiteraard in bepaalde gevallen voor meer alertheid bij de betaler zorgen, maar biedt logischerwijs minder bescherming dan wanneer een extra activatie van de nieuw geïnstalleerde mobiele app gevraagd wordt. Het is immers steeds mogelijk dat de betaler betrokken bericht niet meteen ziet, waardoor de fraudeur in tussentijd toch reeds zijn slag kan slaan.

Indien het vaststaat dat de betaler betrokken kennisgeving inzake de nieuwe installatie van een mobiele app (meteen) gezien heeft, doordat hij dit bijvoorbeeld zelf aan de bank of politie verklaart, kan hiermee rekening worden gehouden bij de beoordeling van de voorafgaandelijke detecteerbaarheid van de fraude en de grove nalatigheid. In dergelijk geval zal de kennisname van dit bericht of het niet opvolgen van de instructies in dit bericht echter niet noodzakelijkerwijs betekenen dat respectievelijk de fraude voorafgaandelijke detecteerbaar was of de klant grof nalatig geweest is. Voor deze beoordeling moet steeds rekening gehouden worden met de concrete omstandigheden van het fraudegeval. Indien de betaler bijvoorbeeld gereageerd heeft op een phishingmail volgens dewelke de betaler zogezegd zijn bankapp opnieuw moet installeren en activeren, zal op basis van betrokken kennisgeving bijvoorbeeld niet tot de detecteerbaarheid van de fraude of een grove nalatigheid besloten kunnen worden. Betrof de phishingmail daarentegen bijvoorbeeld de aanvraag van een nieuwe digipass dan maakt betrokken bericht de fraude wel detecteerbaar. Bij de beoordeling of het niet opvolgen van de instructies inzake de blokkering van de mobiele app al dan niet een grove nalatigheid vormt, moet onder meer rekening worden gehouden met alle omstandigheden van het fraudegeval en de plausibiliteit van de verklaring van de betaler voor het uitblijven van enige reactie. Ook moet worden nagegaan of betrokken kennisgeving al dan niet voldoende duidelijk was opgesteld, door bijvoorbeeld op een mogelijke fraude te wijzen.

Anderzijds is het mogelijk dat de betaler verklaart betrokken kennisgeving over de installatie van een nieuwe app niet te hebben ontvangen of niet tijdig te hebben gelezen. De betalingsdienstaanbieder zal hier in dergelijk geval zeer moeilijk het tegendeel kunnen bewijzen. In deze gevallen kan volgens Ombudsfin geen rekening worden gehouden met betrokken kennisgeving bij de beoordeling van de detecteerbaarheid van de fraude en de grove nalatigheid. De betalingsdienstaanbieder draagt dus het risico van zijn keuze om louter met een informatiebericht, dus zonder activatiecode of –link, te werken.

De rechtspraak is verdeeld op dit punt. In een vonnis van 11 februari 2022 stelde de rechtbank dat het niet onmiddellijk reageren op betrokken bericht niet als grove nalatigheid kan worden beschouwd. De rechtbank motiveerde dit door te stellen dat noch de wet, noch de zorgvuldigheidsnorm gebiedt om op elk moment zijn gsm bij zich te hebben. In een vonnis van 4 april 2022 stelde de rechtbank daarentegen dat het gedurende lange tijd onbereikbaar zijn, in casu door de batterij van de smartphone niet op te laden, niet verzoenbaar is met het gedrag van een normaal zorgvuldig huisvader in de huidige maatschappij. Ombudsfin is van mening dat dit laatste standpunt veel te streng is en sluit zich aan bij de eerste stelling.

Aan financiële instellingen die er toch voor kiezen om louter en alleen een informatief bericht te versturen betreffende de installatie van een nieuw app raadt Ombudsfin aan om betrokken app gedurende een aantal uren inactief te laten. Op die manier krijgt de betaler toch in zekere zin de mogelijkheid om binnen een redelijke termijn kennis te nemen van betrokken bericht en alsnog gepast te reageren. Zo zal schade in verschillende gevallen toch kunnen worden voorkomen.

b) Bericht met activatiecode of -link

Steeds meer financiële instellingen voorzien in de installatie-procedure van een nieuwe mobiele app een extra stap waarbij een activatiecode of –link per sms of mail naar de klant verstuurd wordt. Dergelijke activatiestap zorgt uiteraard voor een extra veiligheid en heeft bovendien als voordeel dat de bank zich er door middel van betrokken sms'en en mails van zal vergewissen dat het de klant zelf is die betrokken handelingen stelt. Hoewel dit voor extra veiligheid zorgt, zal dit fraude echter nooit volledig doen verdwijnen. Fraudeurs spelen hier immers op in en passen voortdurend hun verhaal en modus operandi aan opdat zij

toch de voor de activatie noodzakelijke gegevens kunnen onderscheppen of verkrijgen.

Indien betalers erkennen betrokken berichten te hebben ontvangen en de activatielink of –code hebben gebruikt, moet hiermee uiteraard rekening worden gehouden bij de beoordeling van de detecteerbaarheid van de fraude en de grove nalatigheid. Opnieuw zal dit niet automatisch leiden tot de aansprakelijkheid van de betaler. In geval het phishingbericht de installatie van de bankapp betreft, zal de invoer van de activatiecode op zich geen grove nalatigheid vormen. Betreft het phishingbericht echter de ontvangst van één of andere premie, kan hierover anders geoordeeld worden. Opnieuw moet worden nagegaan of de door de betalingsdienstaanbieder verstuurde berichten al dan niet voldoende duidelijk zijn.

Wanneer de betalingsdienstaanbieder werkt met een activatiecode of –link, zal de betaler minder makkelijk kunnen ontkennen dat hij de door de bank verstuurde berichten ontvangen heeft of stellen dat hij de ontvangen code of link niet gebruikt heeft. De app werd immers actief gebruikt.

Rekening houdende met voorgaande, beveelt Ombudsfin de financiële instellingen nog steeds aan om tijdens de installatieprocedure van de mobiele app een extra activatie van de betaler te vragen. Dit verhoogt niet alleen de veiligheid voor de klant, maar heeft ook positieve gevolgen voor de betalingsdienstaanbieder wat de beoordeling van de aansprakelijkheidsverdeling op basis van artikel VII.44 WER betreft. Ook in artikel 25 van de Gedelegeerde Verordening SCA kan steun gevonden worden voor het argument van een voorafgaande activatie. Artikel 25 bepaalt dat betalingsdienstverleners ervoor moeten zorgen dat wanneer de levering van persoonlijke beveiligingsgegevens buiten de bedrijfsruimten van de betalingsdienstverlener of via een communicatiemiddel op afstand geschiedt (in casu de installatie van de betaalapplicatie), de geleverde persoonlijke beveiligingsgegevens en authenticatie-apperatuur of -software geactiveerd moeten worden voordat ze kunnen worden gebruikt.

Ombudsfin stelt tevens vast dat fraudeurs er na de installatie van de mobiele app of een aanmelding in het internetbankieren van welbepaalde banken in slagen om eerst het gsm-nummer of emailadres van het slachtoffer aan te passen in een eigen gsm-nummer of emailadres, waarna de betrokken activatiecode wordt verstuurd naar een gsm-nummer van de fraudeur. Dit kan de fraudeur dan veelal doen met behulp van één of meer met bankkaart en kaartlezer gegenereerde codes. Ombudsfin is van mening dat betrokken banken hierdoor tekortkomen in het veiligheidsmechanisme van een extra per sms verstuurde activatie- of bevestigingscode. Het nut van een sms of mail met extra code bestaat er volgens Ombudsfin immers in dat de bank zich ervan kan vergewissen dat de klant zélf bezig is met het uitvoeren van een verrichting of de installatie van een mobiele app. De fraudeur zal zijn slachtoffer veelal in eerste fase reeds kunnen hebben misleiden en ertoe kunnen aanzetten op bijvoorbeeld een valse website met kaartlezer gegenereerde codes in te voeren. Het zal dan ook voor een fraudeur eenvoudiger zijn om zijn slachtoffer via deze website extra met kaartlezer gegenereerde codes te laten invoeren dan het slachtoffer ervan te overtuigen

een code in te voeren, die het slachtoffer per sms ontvangt en waarbij de sms duidelijk stelt dat dit een activatiecode betreft die zeker met niemand gedeeld mag worden. Ombudsfin beveelt de betrokken banken bijgevolg aan om bij wijziging van het gsm-nummer van de klant de nodige maatregelen te nemen om soortgelijke situaties te vermijden en minstens de legitimiteit van het aangepaste gsm-nummer bij de klant te controleren. Een alternatief zou kunnen zijn dat de aanpassing van bepaalde gegevens gedurende een bepaalde termijn na de installatie van een nieuwe app onmogelijk gemaakt wordt.

4.4. Fraudedetectiesystemen

Op basis van artikel 2 van de Gedelegeerde Verordening SCA zijn betalingsdienstverleners ertoe gehouden mechanismen te voorzien voor het monitoren van transacties. Verder vermeldt deze bepaling een reeks risicofactoren waarmee deze fraudedetectiesystemen van de betalingsdienstaanbieder moeten rekening houden. De betalingsdienstaanbieder zal bijgevolg bepaalde parameters instellen om zo eventueel verdachte transacties te detecteren. Indien de fraudedetectiesystemen van de betalingsdienstaanbieder bepaalde verrichtingen als verdacht, dus mogelijk frauduleus, aanmerken, dient de betalingsdienstaanbieder de betrokken verrichtingen tegen te houden. De betalingsdienstaanbieder zal vervolgens contact opnemen met de betaler om af te stemmen of deze daadwerkelijk de betrokken verrichting wenst te laten doorgaan. Op deze manier kunnen frauduleuze verrichtingen vaak voorkomen worden en wordt de schade aldus beperkt. Bij het instellen van de verschillende parameters in de fraudedetectiesystemen zal de betalingsdienstaanbieder steeds een afweging moeten maken tussen veiligheid en gebruiksgemak. Een te strenge fraudedetectie kan er immers toe leiden dat bepaalde betalingstransacties ten onrechte worden tegengehouden.

In welke mate kan een betalingsdienstaanbieder aansprakelijk worden gesteld wanneer diens fraudedetectiesystemen kennelijk tekortgeschoten hebben? Zo wordt Ombudsfin soms geconfronteerd met gevallen waarbij een fraudeur erin slaagt om, vaak na de installatie van een nieuwe mobiele app, (vaak) binnen een relatief korte tijdsspanne tientallen verrichtingen voor een (soort)gelijk bedrag en naar eenzelfde begunstigde uit te voeren. In dergelijke gevallen is Ombudsfin van mening dat de fraudedetectiesystemen van de betalingsdienstaanbieder de fraude toch hadden moeten detecteren (bijvoorbeeld na een vijftal verrichtingen). Het is belangrijk om hierbij te benadrukken dat fraudedetectie een inspanningsverbintenis betreft. Bovendien is fraudedetectie geen exacte wetenschap.

Noch PSD II, noch de Gedelegeerde Verordening SCA voorzien een sanctie voor het geval dat de fraude-detectiesystemen van de betalingsdienstaanbieder onvoldoende performant zijn. Bovendien zou op basis van het reeds vermelde arrest van het Hof van Justitie van 2 september 2021 geoordeeld kunnen worden dat de aansprakelijkheidsregeling in artikel VII.44 WER definitief is, waardoor een aanvullend beroep op de zorgplicht in hoofde van de betalingsdienstaanbieder om deze alsnog aansprakelijk te stellen niet mogelijk is. Het Hof van Justitie oordeelde immers dat een aanvullend beroep op een andere aansprakelijkheidsregeling dan deze die voorzien is in PSD I niet in overeenstemming is met de maximaal harmoniserende werking van de richtlijn. Aangezien ook PSD II een maximale harmonisatie beoogt, zou dit arrest overeenkomstig kunnen worden toegepast op de huidige regelgeving.

Toch zal Ombudsfin in het kader van haar bemiddelings-opdracht steeds nagaan of de fraudedetectiesystemen al dan niet voldoende performant gewerkt hebben. Wanneer volgens Ombudsfin vaststaat dat de fraudedetectiesystemen kennelijk tekortgeschoten hebben, zal Ombudsfin, op basis van de zorgplicht in hoofde van de betalingsdienstaanbieder, aan de betrokken betalingsdienstaanbieder vragen om tussen te komen in alle schade die is ontstaan, nadat de fraude volgens Ombudsfin ten laatste door de systemen van de bank had moeten zijn gedetecteerd. Ook in de rechtsleer ontstaat de roep om de aansprakelijkheidsregeling voor niet-toegestane betalingstransacties die hebben plaatsgevonden met sterke cliëntenauthenticatie niet uitsluitend te laten afhangen van het gedrag van de betaler, maar hierbij ook rekening te houden met de inspanningen van de betalingsdienstaanbieder, zowel wat betreft recuperatie als fraudedetectie.

4.5. Maatregelen om het aantal fraudegevallen en de ermee gepaard gaande schade te beperken

De banken proberen het aantal internetfraudegevallen en de schade die hieruit voortvloeit in te perken door bijvoorbeeld de betaalprocessen en de installatieprocedure van de mobiele bankapp aan te passen. Zo volgden verschillende banken de aanbeveling van Ombudsfin op door bij de installatie van de mobiele app een extra stap te voorzien door een activatielink of –code per sms of mail naar het bij de bank gekende gsm-nummer of emailadres te sturen. Ook bieden bepaalde financiële instellingen een soort van fraudeverzekering aan, waarbij ook bepaalde fraudegevallen gedekt zijn waarvoor de betaler op basis van artikel VII.44 WER (mogelijk) geen aanspraak zou kunnen maken op een tussenkomst.

Ook vanuit de politiek wordt gevraagd om bepaalde systemen te voorzien of bestaande processen te optimaliseren opdat internetfraude in bepaalde gevallen kan worden voorkomen of de eventuele schade ten gevolge van internetfraude kan worden beperkt. Zo werkt de Belgische banksector aan de invoer van de IBAN-naamcontrole, een controle van de overeenstemming tussen het bankrekeningnummer en de titularis van de rekening, is er de vraag om de procedure inzake de kennisgeving van de fraude te vereenvoudigen voor de betaler, en meer recent de vraag naar de invoer van een zogenaamd 'traag bankieren'-profiel.

a) IBAN-naamcontrole

Artikel VII.55/2, §1 WER voorziet dat betalingsdienstaanbieder, die verantwoordelijk is voor de uitvoering van een betalingsopdracht, niet gehouden is de overeenstemming tussen het opgegeven bankrekeningnummer en de vermelde begunstigde te controleren. De betalingsdienstaanbieder is op basis van deze bepaling uitsluitend aansprakelijk voor de uitvoering overeenkomstig de correcte unieke identificator, ofwel het rekeningnummer. Toch werkt de Belgische bankensector op dit moment, naar het voorbeeld van Nederland en het Verenigd Koninkrijk, aan een IBAN-naamcontrole, die in de loop van volgend jaar in voege zou moeten treden. Deze zal inhouden dat de bank bij de invoering van een overschrijvingsopdracht zal controleren of het rekeningnummer en de naam van de begunstigde overeenstemmen. Indien dit niet het geval zou zijn, zal de betaler een melding hiervan ontvangen en vervolgens de keuze krijgen om de overschrijvingsopdracht al dan niet te bevestigen. Om de weigering van te veel verrichtingen te voorkomen, zal het systeem hierbij in zekere mate rekening houden met mogelijke variaties in de schrijfwijze van voor- en achternamen.

De IBAN-naamcontrole heeft tot doel om fraudegevallen mee te helpen voorkomen. Hierbij moet worden opgemerkt dat een IBAN-naamcontrole alleen nuttig zal zijn voor het voorkomen van fraudegevallen waarbij de betaler zelf, dus niet de fraudeur, de overschrijving via zijn internetbankieren of mobiele bankapp invoert. Zo zal de IBAN-naamcontrole bepaalde gevallen van factuurfraude, kluisrekeningfraude en van whaling mee kunnen helpen voorkomen. In klassieke phishingdossiers, waarbij een fraudeur via een valse website bancaire gegevens en met bankkaart en kaartlezer gegenereerde codes onderschept om hiermee vervolgens zelf overschrijvingen en betalingen uit te voeren, zal de IBAN-naamcontrole uiteraard geen nut hebben.

Hoewel PSD II een maximaal harmoniserende werking heeft, waardoor lidstaten dus niet in bijkomende bescherming voor de betaler mogen voorzien, verzet PSD II zich er niet tegen dat betalingsdienstaanbieders onderling afspraken maken over een dergelijke IBAN-naamcontrole. Artikel 107 PSD II voorziet immers het volgende: "Betalingsdienstaanbieders mogen evenwel besluiten betalingsdienstgebruikers gunstiger voorwaarden te bieden." Op Europees niveau wordt verder overlegd om een verplichting inzake IBAN-naamcontrole in te voeren voor instant overschrijvingen.

b) Vereenvoudiging van de kennisgevingsprocedure: telefonische permanentie én één systeem om bankkaart, rekening en app te blokkeren

Eerder in dit artikel werd reeds de problematiek inzake de kennisgeving van de fraude aan de betalingsdienstaanbieder besproken. Wij hebben onderlijnd dat, alhoewel de banken in principe niet wettelijk verplicht zijn om een telefonische permanentie te voorzien, zolang het voor de betaler mogelijk is om te allen tijde kosteloos een kennisgeving van de fraude te doen, ze voortaan, vanaf 23 januari 2023, een klantendienst hebben die 24/7 bereikbaar is. Via de website van Card Stop kunnen de contactgegevens van deze diensten eenvoudig teruggevonden worden.

Wij hebben ook betreurd dat de betaler in sommige gevallen meerdere kennisgevingen van de fraude zal moeten doen om al zijn betaalinstrumenten te blokkeren. Een betere telefonische bereikbaarheid van de banken en een eenvoudigere kennisgevingsprocedure kunnen er uiteraard toe leiden dat betaalinstrumenten in geval van fraude sneller geblokkeerd worden, waarna de bank sneller de nodige recuperatiemaatregelen kan treffen.

De politieke wereld, door de stem van zijn twee laatste Staatssecretarissen voor Begroting en Consumentenbescherming, Mevrouwen Eva De Bleeker en Alexia Bertrand, heeft ook laten weten dit initiatief te ondersteunen.

c) Slow banking [11]

Verder wenste voormalig staatssecretaris Eva De Bleeker dat financiële instellingen aan consumenten een gebruikersprofiel zouden aanbieden om 'traag te bankieren'. Hierbij zou de consument ervoor kunnen kiezen om strenge daglimieten in te stellen, die vervolgens uitsluitend via het bankkantoor of de bankautomaat zouden kunnen worden verhoogd. Dergelijke maatregel zou niet leiden tot een vermindering van het aantal fraudegevallen, maar zou de schade in een groot aantal fraudegevallen wel kunnen beperken. Ook huidig staatssecretaris Alexia Bertrand wilt hier werk van maken.

4.6. Aanbevelingen

4.6.1. Algemene antifraudeaanbevelingen aan de consumenten

- Consulteer regelmatig https://safeonweb.be/. Daar vindt u heel veel nuttige tips en waarschuwingen over alle gekende fraudepraktijken op het internet.
- Controleer steeds het **volledige mailadres** of de **volledige URL** van een website. De kleinste schrijffouten of het gebruik van atypische domeinnamen of mailadressen wijzen op fraude. Bij de minste twijfel, stop uw handelingen of de communicatie en doe de nodige verificaties via extra opzoekingen.
- Wanneer iets te mooi lijkt om waar te zijn, dan is het waarschijnlijk ook het geval en is het dus fraude. Laat u niet verleiden en stop de communicatie of handelingen.
- Aan de hand van codes (aangemaakt door uw kaartlezer) kan een fraudeur van op afstand betalingen doen, overschrijvingen doen via uw homebanking of zelfs úw banking app installeren op zijn persoonlijke smartphone. **Communiceer dus nooit codes, aangemaakt door uw kaartlezer, aan een derde. Ook uw bankier vraagt dit nooit**.
- Gebruik nooit uw kaartlezer wanneer u een **betaling** moet ontvangen. Daarvoor is een kaartlezer **nooit** nodig.
- De toetsen en tekst op uw kaartlezer vertellen u al heel veel over de handelingen die u aan het doen bent. Op de knoppen staat niet voor niets "Buy", "Sign", "Identify", "M1 = Identify = Appli 1", "M2 = Sign = Appli 2". Wees u bewust van wat u doet en lees ook de tekst die eventueel verschijnt op uw kaartlezer.

4.6.2. Antifraudeaanbevelingen aan de sector

- Ombudsfin beveelt banken aan om ervoor te zorgen dat een blokkering van een betaalkaart via Card Stop verder fysiek gebruik van betrokken kaart compleet onmogelijk maakt. Het is immers niet logisch dat het bijvoorbeeld wel nog mogelijk is om met een geblokkeerde kaart online aan te melden en overschrijvingen uit te voeren.
- Ombudsfin raadt banken aan om hun sms na aanmaak van de mobile app zo duidelijk mogelijk op te stellen en de klanten mee te delen welke acties zij kunnen ondernemen om de mobile app te blokkeren, in het geval dat de klant deze niet zelf heeft geïnstalleerd.
- Banken lichten de klanten in bij de aanmaak van een mobiele app door onmiddellijk een sms naar de klant te sturen. Er wordt echter niet altijd een activatie van de mobiele app aan de betrokken klant gevraagd. Ombudsfin heeft vroeger reeds aan de banken aangeraden om een extra activatie van een pas geïnstalleerde app aan de klant te vragen. Dit zou in vele dossiers de fraude kunnen voorkomen. Aan banken die geen extra activatie vragen, maar louter werken met een kennisgeving inzake de installatie van een nieuwe app, wordt aangeraden om betrokken app gedurende een bepaalde beperkte termijn (bv. een aantal uren) inactief te laten zodat de betaler toch in zekere zin de mogelijkheid heeft om binnen een redelijke termijn kennis te nemen van betrokken bericht en alsnog gepast te reageren.
- Teneinde de veiligheid van het betaalverkeer te versterken dienen de banken hun monitoringsysteem aan te passen en ervoor te zorgen dat er een alarm afgaat wanneer er

[11] De bedoeling hiervan is te voorkomen dat geregistreerde betalingslimieten onmiddellijk worden verhoogd en particulieren te verplichten hiervoor een meer formele procedure te volgen.

vlak na elkaar een nieuwe app wordt geïnstalleerd en het gsm-nummer van de klant wordt gewijzigd. De 2de sms van de bank met de activatiecode komt hierdoor misschien niet bij de klant zelf terecht. In deze situatie moet voorzien worden dat er met de klant rechtstreeks contact wordt opgenomen vooraleer er verrichtingen doorgang kunnen vinden.

- Ombudsfin is verheugd dat verschillende banken thans aan de klant vragen om de installatie van de app zelf te activeren. Wel is het te betreuren dat de 2de sms met de activatiecode niet altijd duidelijk vermeldt dat het om de activatiecode voor de pas geïnstalleerde app gaat. We stellen vast dat sommige banken hier reeds bepaalde inspanningen geleverd hebben om betrokken sms'en te verduidelijken.
- Voorzie kennisgevings-, blokkerings- en recuperatie-procedures die zijn aangepast aan de snelheid waarmee verrichtingen momenteel worden uitgevoerd.
- Leg de klanten goed uit hoe het betalingsmechanisme werkt en wat de impact is van het gebruik van de kaartlezer.
- Wanneer een kaart gekoppeld is aan een online payment wallet, bijvoorbeeld Apple Pay, moet het blokkeren van de kaart maken dat de kaart ook binnen die online payment wallet onbruikbaar wordt.
- Het activeren van een koppeling van een kaart in een online payment wallet vereist een specifieke bijkomende actie van de klant. Een loutere kennisgeving van de activering, bijvoorbeeld via sms, volstaat niet.

5. BEEINDIGING KLANTENRELATIE

In 2022 kreeg Ombudsfin opnieuw te maken met talrijke gevallen van blokkering van rekeningen en/of eenzijdige beëindiging van de relatie met de cliënt door de financiële instelling (198 gevallen). Deze maatregelen zijn vaak een "hulpmiddel" om hen in staat te stellen te voldoen aan hun zorgvuldigheidsverplichtingen die zijn vastgelegd in de Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten. Gezien het recht van banken om de bankrelatie te allen tijde te beëindigen zonder dit besluit te moeten rechtvaardigen, blijft de rol van Ombudsfin in de praktijk beperkt tot het controleren of de overeengekomen vormen en termijnen voor het beëindigen van de bankrelatie zijn nageleefd. Op dit punt verwijst Ombudsfin naar zijn gedetailleerde verklaring in het jaarverslag 2021, blz. 13.

6. BEPERKING CASH VERRICHTINGEN

In ons vorige jaarverslag hebben wij reeds gewezen op de belemmeringen die sommige banken opwerpen voor het storten of opnemen van contant geld (zie punt 5.4. van het jaarverslag 2021). In de betrokken periode zijn wij enkele gevallen tegengekomen waarin klagers verbaasd waren dat zij hetzelfde (grote) geldbedrag, dat zij enige tijd eerder hadden opgenomen, niet opnieuw bij hun bank konden storten. De door de klagers aangevoerde argumenten zijn divers (de geplande operatie kon niet doorgaan, paniekerige afhalingen vanwege de oorlog in Oekraïne, enz.). De betrokken banken hebben de storting geweigerd onder verwijzing naar hun verplichtingen inzake de strijd tegen het witwassen van geld (en meer bepaald de verplichting om de herkomst van de gelden te controleren). Zij hebben ons meegedeeld dat zij hun cliënten er bij de opneming op hebben gewezen dat een latere storting van deze gelden een probleem zou kunnen vormen. Aangezien deze mededeling mondeling werd gedaan, kan Ombudsfin uiteraard niet nagaan of ze duidelijk genoeg was om de cliënt niet te misleiden.

In deze materie werden volgende aanbevelingen gedaan :

- Beperkingen die bij een bank gelden voor cash verrichtingen moeten zo duidelijk mogelijk bepaald staan in de algemene voorwaarden.
- Wanneer een bank niet langer toestaat cash afhalingen te doen aan het loket, moet het aangeboden alternatief (bijvoorbeeld automaten) voldoende veilig kunnen verlopen.

7. BETALINGEN – ANDERE PROBLEMATIEKEN

De sancties van de Europese Unie tegen Rusland, met name de bevriezing van Russische tegoeden van bepaalde personen en het verbod op betalingsverrichtingen van en naar Rusland, hebben aanleiding gegeven tot diverse klachten van consumenten. Sommigen vonden dat zij ten onrechte op een zwarte lijst waren geplaatst, terwijl anderen klaagden dat zij geen effectieve terugbetaling konden krijgen van bedragen die aan Russische bedrijven waren betaald voor diensten die als gevolg van de sancties niet konden worden verstrekt (bv. de betaling van vliegtickets voor een vlucht naar Moskou met de luchtvaartmaatschappij Aeroflot).

In het eerste geval deelde Ombudsfin de klagers mee dat ze, indien nodig, bij de Algemene Administratie van de Thesaurie van de FOD Financiën een vrijstelling konden aanvragen. In het tweede geval kon Ombudsfin enkel vaststellen dat de financiële instellingen handelden in overeenstemming met de hen opgelegde sancties.

Ombudsfin formuleerde volgende aanbevelingen in betalingsdossiers:

- Wanneer de uitvoering van een verrichting wordt uitgesteld, moet de bank de klant hiervan verwittigen.
- Betalingsinstellingen moeten identificatieprocedures voorzien die voldoende sluitend zijn om identiteitsfraude te voorkomen en moeten de begunstigde van een internationaal transfer bij afhaling voldoende identificeren.

8. KWETSBARE GROEPEN

Ombudsfin heeft in de loop van 2022 nogmaals veel signalen ontvangen van bepaalde sociale organisaties dat personen in een financieel en maatschappelijk kwetsbare positie steeds vaker op problemen botsen in hun zoektocht naar een dienstverlening bij de banken, die aangepast is aan hun behoeften.

Ombudsfin heeft nota genomen van de aangebrachte signalen. Ombudsfin is er zich van bewust dat deze problematiek leeft, maar kan deze vanuit zijn eigen werking niet als dusdanig bevestigen.

Wij moeten immers vaststellen dat, ook in 2022, weinig klachten werden ingediend door mensen toebehorend aan deze groepen. Dit is mogelijk te wijten aan een onvoldoende kennis van het bestaan en van de rol van onze dienst. Dit is uiteraard jammer. Bij deze wensen wij de OCMW 's en andere ondersteunende instellingen eraan te herinneren dat zij bij Ombudsfin een klacht kunnen indienen in naam en voor rekening van de mensen die zij helpen, weliswaar nadat zij de klacht eerst hebben voorgelegd aan de bevoegde klachtendienst van de betrokken bank.

In deze materie werden volgende aanbevelingen gedaan :

- De procedures moeten zo worden opgesteld dat een niet-begeleide minderjarige vluchteling (hierna: NBMV) niet onnodig lang geblokkeerd is op vlak van financiële verrichtingen. Als de NBMV niet samenwoont met de voogd (wat meestal het geval is), moet de bank voorzien dat de kaart naar de voogd wordt verzonden.
- Banken mogen in de praktijk bij de opening van een basis-bankdienst niet strenger zijn qua identiteitsvereisten dan de vereisten voorzien in de FAQ van Febelfin.

9. KREDIETEN

Zoals voorgaande jaren heeft Ombudsfin in 2022 ook een aantal klachten in verband met kredieten aan consumenten behandeld: zowel met betrekking tot hypothecaire kredieten als met consumentenkredieten.

Met betrekking tot de klachten aangaande kredieten, vestigen wij in het bijzonder de aandacht op volgende problematieken:

Hypothecair krediet - desolidarisatie

Ombudsfin heeft dit jaar opnieuw vastgesteld dat er in de hypothecaire kredietsector problemen ontstaan bij echtscheidingen tussen partners die gezamenlijk een lening hebben en mede-eigenaar zijn van een onroerend goed dat als zekerheid dient voor deze lening. Het komt vaak voor dat de medeschuldenaar die zijn aandeel in het onroerend goed overdraagt aan zijn voormalige partner, vergeet om de leningsvoorwaarden te regelen en toestemming te krijgen van de bank om van het krediet te worden vrijgesteld voordat hij zijn aandeel overdraagt. De medeschuldenaar denkt ten onrechte dat de afspraken tussen de voormalige partners voldoende zijn om hem van alle verplichtingen te ontheffen.

De bank is echter nooit verplicht een dergelijk verzoek tot desolidarisatie in te willigen. De aanvaarding ervan hangt vooral af van de financiële draagkracht van de partner die het onroerend goed en de lening overneemt. Een dergelijk verzoek vereist dat de kredietgever een nieuw kredietdossier samenstelt en een nieuwe analyse maakt van de financiële draagkracht van de overnemer, aangezien deze na de scheiding de volledige lening zal moeten terugbetalen.

Ombudsfin benadrukt het belang van het verkrijgen van dit schriftelijke akkoord tot desolidarisatie van de bank in geval van overdracht van onverdeelde rechten op een gehypothekeerd gebouw, omdat de persoon die zijn of haar rechten overdraagt niet langer de eigenaar is en als hij of zij geen schriftelijk akkoord van de bank heeft verkregen om gedesolidariseerd te worden van het krediet, is hij of zij nog steeds gebonden door het krediet. De gevolgen kunnen dramatisch zijn voor deze persoon, die geen reële rechten meer heeft op het onroerend goed en er niet langer van geniet, maar door de bank op elk moment kan worden aangesproken om de lening terug te betalen. Bovendien is zijn of haar financiële draagkracht verminderd en dit kan een belemmering vormen voor het verkrijgen van een andere lening om een ander onroerend goed te verwerven.

Daarom nodigt Ombudsfin de consumenten uit om actief te zijn in hun verzoek tot desolidarisatie en de banken om creatiever te zijn, zodat zij hun garanties kunnen behouden maar de dramatische gevolgen van deze situatie voor de persoon die geen eigenaar meer is, worden vermeden.

Consumentenkrediet - identiteitsdiefstal

De laatste jaren is identiteitsdiefstal op internet een veelvoorkomende vorm van oplichting. Dit komt doordat er op het internet veel persoonlijke informatie circuleert, wat het voor oplichters mogelijk en gemakkelijker maakt om persoonlijke informatie te verzamelen. Bij online identiteitsdiefstal verkrijgt de fraudeur voldoende persoonsgegevens van een slachtoffer om financiële transacties uit te voeren op naam van het slachtoffer, zoals het openen van een bankrekening, het aanvragen van een consumentenkrediet of het aanvragen van een nieuwe kredietkaart op een ander adres dan dat van het slachtoffer. De gevolgen van identiteitsdiefstal kunnen ernstig zijn, zoals het starten van incassoprocedures voor niet-betaalde bedragen, een negatieve registratie bij de Centrale voor Kredieten aan Particulieren en zelfs een gerechtelijke procedure.

Het is daarom van essentieel belang dat slachtoffers zo snel mogelijk reageren, door bij de politie aangifte te doen van identiteitsdiefstal en tegelijkertijd de bank of kredietverstrekker op de hoogte te brengen van het incident.

Sommige mensen klagen bij Ombudsfin wanneer ze geconfronteerd worden met een negatieve registratie of betalingsherinnering voor een consumentenkrediet waarvan ze niet op de hoogte zijn en waarvan ze niet hebben genoten. Wanneer deze slachtoffers ontdekken dat hun identiteit is gestolen om het krediet af te sluiten, dienen ze een klacht in bij de politie wegens identiteitsdiefstal. Ze vragen ook Ombudsfin om de kredietovereenkomst bij de kredietverstrekker te annuleren om te voorkomen dat ze moeten terugbetalen voor bedragen waarvan ze niet hebben genoten. Wanneer een klacht wordt ingediend bij Ombudsfin, aanvaarden de meeste banken om de inning van de geleende bedragen op te schorten in afwachting van het resultaat van de strafprocedure.

In de meeste gevallen wordt de strafzaak zonder gevolg afgesloten omdat de indringer onbekend blijft. Als uit de door beide partijen ingediende documenten blijkt dat de identiteitsdiefstal zeer waarschijnlijk is, verzoekt Ombudsfin de kredietverstrekker niettemin het slachtoffer de nietigverklaring van het consumentenkrediet en de schrapping van de negatieve registratie bij de Centrale voor Kredieten aan Particulieren toe te kennen. In de meeste gevallen wordt dit verzoek ingewilligd.

In andere gevallen ontdekken de klagers dat er online een rekening is geopend door het stelen van hun identiteit en dat er een debetkaart is gebruikt, waardoor de rekening in het rood staat als gevolg van ongeoorloofde transacties door de rekeninghouder. Klagers betwisten meestal dat zij een dergelijke debetkaart hebben aangevraagd en ontvangen. In dergelijke gevallen werd de kaart inderdaad vaak naar een ander adres gestuurd, dat van de usurpator of een medeplichtige.

Indien deze feiten duidelijk zijn vastgesteld, beroept Ombudsfin zich op artikel VII.39. 6° van het Wetboek van economisch recht, dat bepaalt dat de kredietverstrekker «het risico draagt dat verbonden is aan de verzending van een betaalinstrument aan de gebruiker van betalingsdiensten of van elk middel dat het gebruik ervan mogelijk maakt, met name alle gepersonaliseerde veiligheidsgegevens» en eist zij de terugbetaling van de aldus afgewende bedragen. Ombudsfin verzoekt de bank ook om de negatieve registratie bij de Centrale voor Kredieten aan Particulieren te verwijderen, ongeacht de strafrechtelijke uitkomst van de klacht.

10. BELEGGINGEN

Bij de klachten in verband met beleggingen springen vooral de volgende twee onderwerpen in het oog :

A. Onmogelijkheid om penny stocks te verhandelen via de bank

Houders van aandelen met een zeer beperkte beurswaarde, ook wel penny stocks genoemd, vinden het soms moeilijk om hun effecten te verkopen via de bank die ze in portefeuille heeft. Zij hebben geen andere keuze dan hun effecten over te dragen aan een andere financiële instelling die de handel in deze effecten accepteert. Helaas brengt een dergelijke overdracht kosten met zich mee en is het niet gemakkelijk een tussenpersoon te vinden die bereid is deze effecten in bewaring te nemen.

In 2022 behandelde het College van experten een klacht over de onmogelijkheid voor een cliënt om zijn aandelen bij zijn bank te verkopen.

In oktober 2021 wilde de klager zijn aandelen verkopen omdat ze een aanzienlijke tegenwaarde vertegenwoordigden. Hij tekende een verkooporder, maar een dag later zei de bank hem dat het niet mogelijk was dit aandeel te verkopen. Klager stelde dat de bank hem hiervan nooit op de hoogte heeft gebracht. Hij vroeg ook aan andere banken of zij in de aandelen konden handelen en het bleek dat de aandelen bij hen perfect verhandelbaar waren. De regels voor de overdracht van aandelen zijn echter sinds enkele jaren verstrengd. Hierdoor waren deze aandelen niet overdraagbaar.

Tijdens de bemiddeling heeft de bank bevestigd dat het mogelijk is dat bepaalde orders niet kunnen worden uitgevoerd onder meer omwille van specifieke regels en/of interne beleidskeuzes van de bank en/of haar eigen tussenpersonen (brokers). Dit is het geval voor penny stocks. Veel tussenpersonen weigeren namelijk orders op dit soort aandelen uit te voeren omdat het vaak gaat om aandelen van minder transparante ondernemingen waarover weinig informatie beschikbaar is en waar het risico op fraude en marktmisbruik zeer groot is.

De bank heeft ons niettemin uitgelegd dat deze verkoopbeperkingen het recht om de stukken aan een andere financiële instelling over te dragen niet beïnvloeden. Hoewel verkoop door de bank dus niet mogelijk is, blijft overdracht van de effecten een mogelijk alternatief mits een instelling wordt gevonden die de betrokken effecten kan en wil aanvaarden.

Op juridisch vlak is de bank van mening dat zij niet aansprakelijk kan worden gesteld. Zij beroept zich met name op haar algemene voorwaarden, die bepalen dat de dienstverlener geen enkele resultaatsverbintenis op zich neemt met betrekking tot de verhandelbaarheid van de aandelen, alsook op het feit dat de dienstverlener niet aansprakelijk is bij een lichte fout.

Het College van experten meent dat de bank niet kan worden verweten dat de aandelen van klager niet meer verhandeld kunnen worden. Het College van experten is echter van oordeel dat de bank een grove fout heeft begaan door de cliënt niet tijdig te informeren over de toekomstige

onverhandelbaarheid van deze aandelen, via de bank, noch over de noodzaak om deze aandelen te transfereren (met het oog op hun verhandeling via een andere dienstverlener). Het verstrekken van duidelijke informatie over wijzigingen inzake de verhandelbaarheid van effecten (die de bank als professionele dienstverlener dient te kunnen inschatten) behoort immers tot de essentie van de zorgplicht die op de bewaarnemer rust. Het College van experten vindt dat het niet verstrekken van dergelijke essentiële informatie kan worden gekwalificeerd als grove fout en dat de bank derhalve niet kan ontsnappen aan haar aansprakelijkheid op grond van de algemene bankvoorwaarden, die haar aansprakelijkheid enkel uitsluiten bij lichte fout.

Het College merkt verder op dat, zelfs indien een andere entiteit waarop de dienstverlener beroep doet voor de uitvoering van orders een fout zou hebben gemaakt (quod non), de dienstverlener zich niet op deze fout kan beroepen om zijn aansprakelijkheid tegenover zijn cliënt te ontlopen. De dienstverlener is immers aansprakelijk voor fouten van de entiteiten waarop hij een beroep doet voor de uitvoering van de orders van zijn cliënten.

Het College oordeelde dat een forfaitaire schadevergoeding, naast de terugbetaling van het betaalde ereloon voor de bewaring van de betrokken aandelen, voor beide partijen een evenwichtige en billijke oplossing biedt. Het College meende immers dat het niet zeker was dat, indien klager tijdig was geïnformeerd, hij de mogelijkheid zou hebben gehad om de betreffende aandelen te transfereren en deze via een andere dienstverlener te verkopen aan de koers die gold op de datum waarop het onuitvoerbare verkooporder werd gegeven.

B. <u>Opschorting van transacties in certificaten van aandelen uitgegeven door een bank :</u>

In 2022 heeft Ombudsfin verschillende klachten behandeld over de opschorting van verkooporders van door een bank uitgegeven certificaten van aandelen. Het feit dat de betrokken effecten niet kunnen worden verkocht, veroorzaakt aanzienlijke schade voor de houders ervan, die niet meer over hun fondsen kunnen beschikken.

Dat komt omdat de certificaten van aandelen van de betrokken bank momenteel niet op een gereglementeerde markt of een besloten handelsplatform («Multilateral Trading Facility», ofwel MTF) zijn genoteerd. De bank faciliteert transacties in certificaten van aandelen en is daarmee de enige wederpartij voor inkoop- en verkooporders.

Het feit dat certificaten van aandelen niet beursgenoteerd zijn, heeft uiteraard gevolgen voor de verhandelbaarheid van deze certificaten, die een «liquiditeitsrisico» hebben.

Tot nu toe had de bank echter altijd de handel in certificaten mogelijk gemaakt, waarbij zij de enige wederpartij was voor inkoop- en verkooporders.

De handel in de certificaten is echter sinds januari 2021 geschorst. De bank geeft de volgende reden : «De reden voor deze schorsing is onder meer de marktvolatiliteit (met name in de context van de Covid-19 pandemie), een onevenwicht tussen koop- en verkooporders en de wettelijke limiet/beperking voor de inkoop van deze certificaten, namelijk 3% van het geplaatste kapitaal (in overeenstemming met de EU-verordening prudentiële vereisten voor kredietinstellingen, gekend als de CRR).

In de overtuiging dat het huidige systeem zijn grenzen heeft bereikt, heeft de bank besloten om de handel in certificaten niet langer te faciliteren, maar ze als wederpartij te noteren op een besloten handelsplatform, zijnde een MTF. Dit zou de verhandelbaarheid van de certificaten op basis van een door vraag en aanbod bepaalde prijs moeten verbeteren. Helaas zal deze notering pas over een aanzienlijke periode (meer dan een jaar) in werking treden wegens de juridische en technische beperkingen en de complexiteit van een dergelijk proces.

Ombudsfin merkt echter op dat zowel het liquiditeitsrisico als het risico van een mogelijke opschorting van de handel worden vermeld in het door de bank gepubliceerde prospectus. De bank kan dus op dit punt niets worden verweten.

Administratieve korting van 30%

De bank is wettelijk verplicht de economische waarde van de certificaten aan het eind van elk kalenderjaar aan te geven bij de bevoegde fiscale instanties en de houders van de certificaten.

Om aan de eisen van de fiscus te voldoen, heeft de bank de economische waarde van het certificaat per 31 december 2021 begroot, rekening houdend met de opschorting

van de handel sinds begin 2021 en de impact van deze opschorting op de liquiditeit van de certificaten. Daarbij hield de bank rekening met deskundig extern advies, precedenten in andere ondernemingen en haar eigen professionele beoordeling. Op basis hiervan besloot de bank een administratieve korting van 30% toe te passen op de waarde van de certificaten, wat een bedrag van 59 € geeft. Deze boekhoudkundige waarde geeft uiteraard geen indicatie over de prijs van de certificaten bij een toekomstige notering op een MTF.

Beperkt terugkoopprogramma

Op 15 februari 2022 heeft de bank details bekendgemaakt over een beperkt terugkoopprogramma van certificaten van aandelen. Dit programma zou de certificaathouders in staat hebben gesteld hun certificaten van aandelen te verkopen, zonder te hoeven wachten tot de handel op een MTF begint. De prijs voor deze terugkoop bedraagt eveneens 59 € per certificaat, zijnde dezelfde prijs als die welke om bovengenoemde fiscale en administratieve redenen werd vastgelegd. Deze prijs houdt dus rekening met een korting van 30% om de niet-liquiditeit van de markt weer te geven. Deze niet-liquiditeit is inderdaad een element dat een korting kan rechtvaardigen. De hoogte ervan is blijkbaar gebaseerd op objectieve elementen. Wij wijzen erop dat Ombudsfin geen kopie van de ontvangen adviezen heeft gekregen.

De bank heeft vervolgens aangekondigd het geplande terugkoopprogramma van certificaten van aandelen (voor een bedrag van 14,4 miljoen euro) in te trekken.

Na de intrekking van bovengenoemd plan kondigde de bank als tegenprestatie aan dat zij voorstelt een buitengewoon dividend van 1,01 € (vóór aftrek van eventuele belastingen) per certificaat uit te keren. In totaal zal een bedrag van 14,4 miljoen euro worden uitgekeerd, wat overeenkomt met de marge die de bank had voor de terugkoop van haar eigen certificaten van aandelen. Deze maatregel komt duidelijk niet tegemoet aan de wensen van de certificaathouders.

Besluit

Ombudsfin wil beleggers erop wijzen dat een belegging in aandelen altijd riskant is, ongeacht de emittent.

Ombudsfin kan alleen maar vaststellen dat de huidige situatie inderdaad vervelend is voor alle aandeelhouders, omdat zij hun aandelen niet tegen een eerlijke prijs kunnen verkopen. Ook de betrokken bank is zich hiervan bewust en probeert alternatieven te vinden om haar aandeelhouders te helpen. Jammer genoeg duurt het lang voordat deze alternatieven kunnen worden gerealiseerd.

Gelet op het voorgaande, het feit dat een aandeel een risicovol financieel instrument is en het feit dat de mogelijkheid om de handel in de effecten op te schorten uitdrukkelijk in het prospectus was voorzien, meende Ombudsfin dat er in dit stadium (nog) geen redenen waren om de bank te verzoeken op enigerlei wijze tussen te komen in de hierover ingediende klachten.

Uiteraard kan het advies van Ombudsfin worden herzien als de verschillende door de bank aangekondigde maatregelen niet binnen een redelijke termijn worden uitgevoerd.

11. VARIA

Zoals blijkt uit de statistieken, behandelde Ombudsfin ook heel wat nalatenschapsdossiers (49) en dossiers betreffende huurwaarborgen (24) in 2022. Hieronder bespreken wij enkele problematieken die regelmatig aan bod kwamen.

Huurwaarborgen

Wat betreft de dossiers huurwaarborgrekeningen wil Ombudsfin voor 2022 graag de aandacht vestigen op een specifieke problematiek, namelijk het ontbreken van bewijzen over het al dan niet verder bestaan van de rekening (langs de zijde van de bank) omwille van het verstrijken van 10 jaar sedert de beweerde afsluiting van de rekening.

Ombudsfin merkt dat er soms een conflict is tussen wat een (ver-)huurder naar voor brengt van documenten ter (begin van) bewijs van het nog steeds bestaan van een huurwaarborg en wat de bank nog ter beschikking heeft van bewijs over de huurwaarborg. In verschillende dossiers wierp de bank louter op dat de huurwaarborg waarop de (ver-)huurder nu aanspraak wou maken, meer dan 10 jaar geleden was afgesloten. De bank leidde dit af uit het feit dat er niets meer te vinden was over deze rekening en verwees daarbij naar de wettelijke bewaartermijnen van 10 jaar voor verrichtingen op de rekening en van 10 jaar na afsluiting van de rekening voor contractuele documenten. Dit standpunt van de bank, zonder concrete inbreng en zonder bewijs dat de verhuurder akkoord ging met de vrijgave van de rekening, bemoeilijkte een verdere exacte analyse van deze dossiers.

Wanneer de verzoeker de verhuurder is, is het vaak moeilijk of onmogelijk om aanvullende bewijzen aan te leveren (naast eventuele openingsdocumenten of niet-ingevulde vrijgave-documenten). Huurwaarborgrekeningen staan immers steeds op naam van de huurder, waardoor de verhuurder geen periodieke informatie krijgt over (het saldo van) de rekening en de aanhoudende blokkering ervan, eens de rekening geopend is. De verhuurder wordt in principe enkel actief betrokken bij de opening en bij de vrijgave van de tegoeden. Indien tussen de opening en gewenste vrijgave iets fout loopt, is de verhuurder hier niet per se van op de hoogte en gaat die er te goeder trouw van uit dat de huurwaarborg is blijven lopen gedurende de volledige huurperiode (wat bij woninghuur erg lang kan zijn, langer dan 10 jaar). Uit de dossiers die werden voorgelegd aan Ombudsfin blijkt dat dit vertrouwen onterecht kan zijn.

In bepaalde dossiers kon de bank immers niets bewijzen (zich baserend op bewaartermijnen) en kon de (ver-)huurder toch enkele goede en zekere elementen opwerpen ter verdediging van zijn verzoek, namelijk het noodzakelijke herstel van de huurwaarborg, zodat die er zijn rechten kon op laten gelden. In de dossiers waarin, op basis van de aangevoerde argumenten en documenten van de verzoeker bij Ombudsfin minstens sterk kon worden vermoed dat de bank ergens in het proces een fout had gemaakt, bijvoorbeeld bij de volstorting van de waarborg, de blokkering van de rekening, de afsluiting van de rekening of de vrijgave van de tegoeden, heeft Ombudsfin een gepaste oplossing verkregen van de bank.

Ombudsfin vreest dat deze problematiek in de volgende jaren zal verder bestaan als de bewaartermijnen niet wordt aangepast wanneer het huurwaarborgrekeningen betreft.

Nalatenschap: notariële opdracht met kwijting van aansprakelijkheid, niet uitgevoerd

In 2022 heeft Ombudsfin vastgesteld dat bepaalde banken in erfeniszaken de instructies van de notaris niet altijd opvolgen, zelfs wanneer deze duidelijk aangeven dat de erfenis met kwijting van aansprakelijkheid moet worden overgedragen. In plaats daarvan eisen de banken dat de erfgenamen rechtstreeks met hen een overeenkomst sluiten en hun interne procedures volgen, zelfs als de notaris al een kwijting van aansprakelijkheid heeft afgegeven. Sommige banken stellen zelfs dat hun eigen formulieren gebruikt moeten worden en weigeren de opdracht uit te voeren als dat niet gebeurt.

Ombudsfin heeft zich hierover al meermaals uitgesproken en deelt het standpunt van de banken niet.

Ombudsfin herinnert eraan dat een notaris een openbaar ambtenaar is, benoemd door de Koning, die deze openbare functie uitoefent in het kader van een vrij beroep. Hij oefent dus een publiek ambt uit door authentieke akten op te stellen die kracht van gewijsde hebben, maar hij geeft ook advies en probeert conflicten te vermijden. Het is juist in die hoedanigheid dat hij opdrachten geeft onder kwijting van aansprakelijkheid voor de bank en dat hij derdenrekeningen en rekeningen op naam van zijn cliënten/erfgenamen/erfgenamen heeft.

Ombudsfin stelt helaas vast dat het formalisme dat de banken in naam van hun plicht tot zorgvuldigheid en voorzichtigheid toepassen, regelmatig leidt tot een verslechtering van de relaties tussen erfgenamen en soms resulteert in het langdurig blokkeren van de erfenis en de verdeling als gevolg van de weigering om de instructies van de notaris uit te voeren.

Spaarproducten

Het aandeel klachten over spaarproducten (16 dossiers) blijft ook in 2022 heel beperkt, niettegenstaande toch verschillende spaarders in 2022 ongewild geconfronteerd werden met de definitieve afsluiting van hun rekening. Rabobank Groep had immers in 2021 beslist de activiteiten van Rabobank.be stop te zetten en alle spaarrekeningen definitief af te sluiten tegen juli 2022. Een dergelijke stopzetting van activiteiten gaat vaak gepaard met heel wat vragen en klachten van klanten. Ombudsfin heeft echter maar 2 klachten moeten behandelen over deze stopzetting en durft aan te nemen dat dit te maken heeft met de tijdige, duidelijke en herhaaldelijke communicatie vanuit Rabobank.

Rabobank heeft immers de klanten ruim op voorhand (meer dan een jaar tevoren) geïnformeerd over deze stopzetting en over de impact ervan op hun spaargelden. Rabobank heeft er via een transitieperiode van 1 jaar (van juli 2021 tot juli 2022) alles aan gedaan om de klanten voldoende tijd te geven om alternatieven te zoeken, en heeft daarbij verschillende nuttige en eenvoudige tips gegeven om nadelige gevolgen voor de getrouwheidspremies te voorkomen. De spaarders werden begeleid doorheen dit proces via verschillende brieven en mails en duidelijke richtlijnen op de website over hoe de spaarder eenvoudig zelf zijn saldo naar een andere rekening kon overzetten en zijn rekening kon afsluiten op een gunstig moment, rekening houdend met de getrouwheidsperiodes.

12. FIN-NET : GRENSOVERSCHIJDENDE KLACHTEN

Ombudsfin maakt deel uit van FIN-NET, het Europese netwerk voor de regeling van grensoverschrijdende geschillen in verband met financiële diensten.

FIN-NET ziet toe op de samenwerking tussen de bemiddelingsdiensten van de financiële sector van het merendeel van de EU-lidstaten met het oog op de regeling van grensoverschrijdende geschillen. Voor België is behalve Ombudsfin ook de Ombudsman van Verzekeringen lid van het FIN-NET-netwerk.

Meer uitvoerige informatie over FIN-NET is beschikbaar op de website van de Europese Commissie: https://finance.ec.europa.eu/consumer-finance-and-payments/retail-financial-services/financial-dispute-resolution-network-fin-net_nl

12.1. Procedure

Indien bij Ombudsfin een dossier aanhangig wordt gemaakt dat bestemd is voor de ombudsdienst van een andere EU-lidstaat die bij FIN-NET aangesloten is, stuurt de dienst dat dossier naar de bevoegde instantie, op voorwaarde dat het voldoende gedocumenteerd is. Is het dossier onvolledig, dan zal Ombudsfin de contactgegevens van de bevoegde instelling meedelen.

Ieder land heeft zijn bijzonderheden en zijn eigen structuren voor alternatieve geschillenregeling. In bepaalde landen bestaan er verschillende instanties voor alternatieve geschillenregeling waarvan de bevoegdheid afhankelijk is van het type geschil of van het statuut van de betrokken financiële instelling. Het is ook mogelijk dat bepaalde bemiddelaars geen deel uitmaken van het FIN-NET netwerk. Desgevallend probeert Ombudsfin de verzoeker sowieso door te verwijzen naar de bevoegde dienst.

12.2. Praktische voorbeelden

In 2022 ontving Ombudsfin 1 dossier waarin de FIN-NET-procedure werd gebruikt. Dit dossier had betrekking op een Spaanse financiële instelling. De klacht ging over de voorwaarden en tarifering van een zichtrekening.

13. SAMENWERKING

13.1. BELGIE

13.1.1. Consumentenombudsdienst

De Ombudsdienst voor financiële diensten (Ombudsfin) is lid van het Directiecomité van de Consumentenombudsdienst, die werd opgericht door de wet van 4/04/2014 en als taak heeft:

- De consumenten in te lichten over de mogelijkheden voor een buitengerechtelijke regeling van consumenten-geschillen;
- De klachten in ontvangst te nemen en ze ofwel door te sturen naar de bevoegde entiteit, ofwel zelf te behandelen;
- Tussen te komen in de behandeling van de klachten waarvoor geen enkele gekwalificeerde entiteit bevoegd is.

Ombudsfin is een gekwalificeerde entiteit in de zin van de wet en blijft bevoegd op het domein van bank- beleggings-, krediet- en betalingsdiensten.

13.1.2. OMBUDSMAN.BE

Ombudsfin maakt deel uit van Ombudsman.be, het Belgische netwerk van ombudsmannen. Dit groepeert de openbare en privébemiddelaars die de basisprincipes van de functie van ombudsman hebben onderschreven.

Indien een consument zich tot een ombudsman wendt die niet bevoegd is om zijn probleem te regelen, zal laatstgenoemde ervoor zorgen dat het geschil kan worden voorgelegd aan de bevoegde ombudsman.

Meer uitvoerige informatie is beschikbaar op de site www.ombudsman.be

13.1.3. BELMED

Ombudsfin is aangesloten bij Belmed.

Belmed is een digitaal portaal, opgericht door de FOD Economie, dat volledige informatie biedt over bestaande bemiddelingsinstanties en de wijze waarop een geschil minnelijk geregeld kan worden. Er kan online een bemiddelingsaanvraag ingediend worden via onderstaande website: https://economie.fgov.be/nl/themas/online/belmed-onlinebemiddeling/belmed-uw-partner-alternatieve

13.2. EUROPA

13.2.1. FIN-NET

Ombudsfin neemt actief deel aan de twee FIN-NET-vergaderingen die de Europese Commissie elk jaar organiseert.

Voor bijkomende toelichting, wordt verwezen naar hoofdstuk 12 “FIN-NET: grensoverschrijdende klachten”.

13.2.2. ODR

Het ODR-platform is een platform dat in 2016 in het leven werd geroepen door de Europese Commissie en bestemd is voor consumenten en professionelen die online verrichtingen doen binnen de EU.

De bedoeling is om particulieren gratis te helpen om een klacht op te lossen over goederen of diensten die zij online kochten binnen de EU, zonder het gerecht te moeten inschakelen. In sommige landen is het ook mogelijk om als professioneel een klacht in te dienen tegen een consument. (https://webgate.ec.europa.eu/odr/main/?event=main.complaints.odrList)

13.3. INTERNATIONAAL

Ombudsfin is lid van INFO, het International Network of Financial Services Ombudsman Schemes, dat, op wereldniveau, alle diensten voor alternatieve geschillen-regeling op het financiële domein groepeert. Voor meer informatie: www.networkfso.org.

14. FINANCIELE MIDDELEN

De jaarrekening van het boekjaar 2022 van Ombudsfin vzw is bij publicatie van het jaarverslag 2022 nog niet goedgekeurd door de algemene vergadering. Zodra de jaarrekening zal zijn goedgekeurd, worden de hoofdlijnen ervan gepubliceerd op de website van Ombudsfin onder de vorm van een addendum bij het jaarverslag (www.ombudsfin.be – Publicaties – Jaarverslagen).

Wel is het mogelijk een beeld te geven van de begroting die werd opgesteld voor 2022:

	Begroting 2022
Ontvangsten	
Vaste bijdragen leden Ombudsfin vzw	657.083,50
Variabele bijdragen leden Ombudsfin vzw	657.083,50
Totaal ontvangsten	**1.314.167,00**
Uitgaven	
Personeelskosten + honoraria	1.162.551,00
Werkingskosten	136.616,00
Waardeverminderingen onbetaalde facturen + creditnota's	15.000,00
Totaal uitgaven	**1.314.167,00**

Bij het opstellen en goedkeuren van de begroting wordt steeds voor ogen gehouden dat Ombudsfin vzw, in het kader van haar onafhankelijkheid en onpartijdigheid als gekwalificeerde entiteit, over een eigen en specifiek budget moet beschikken dat toereikend is voor de vervulling van haar taken (zie artikel 2 van het Koninklijk Besluit van 16 februari 2015).

Het noodzakelijke budget wordt opgevraagd aan de leden van Ombudsfin vzw via vaste en variabele bijdragen die jaarlijks worden bepaald door het Bestuur en bekrachtigd door de algemene vergadering van Ombudsfin vzw. Elk lid van Ombudsfin vzw is een vaste bijdrage verschuldigd. Variabele bijdragen worden enkel opgevraagd bij leden waarvoor in het vorige kalenderjaar ontvankelijke klachten werden geregistreerd.

North Gate II
Koning Albert II-laan nr 8, bus 2
1000 Brussel

ombudsman@ombudsfin.be

www.ombudsfin.be