Fraude bij betaaldienstverlening

mr. drs. L. Stortelder[1]

1. Inleiding

Online fraude wordt door het ministerie van Justitie en Veiligheid aangeduid als een 'groeiend maatschappelijk probleem'[2] en fraude bij betaaldienstverlening komt regelmatig voor bij alle (groot)banken in Nederland. De vraag wie juridisch gehouden is om de schade van fraude bij betaaldienstverlening te dragen, is daarmee ook veelvuldig aan zowel de civiele rechter als het Klachteninstituut Financiële Dienstverlening (Kifid) voorgelegd. Ter illustratie: de commissies van het Kifid deden in de periode vanaf 1 januari 2020 tot ultimo augustus 2024 uitspraak in 306 zaken van consumenten die hun bank aansprakken tot vergoeding van geleden schade door fraude met hun betaalinstrument. Overigens werd slechts in 10 van deze zaken de vordering van de consument toegewezen.[3]

Cijfers van de Nederlandse Vereniging van Banken (NVB) laten zien dat de maatregelen die banken nemen om schade met afgegeven of gestolen bankpassen te voorkomen steeds beter werken, maar ook dat hierdoor de werkwijze van criminelen verschuift naar online fraude waarbij klanten worden overgehaald om zelf geld over te boeken. Klanten maken hierbij zelf geld over op instructie van een fraudeur of verschaffen de fraudeur via hun eigen computer of telefoon toegang tot hun bankomgeving.[4] Een klant klikt bijvoorbeeld op een malafide betaallink waarvan hij denkt dat deze door zijn bank is verzonden, de link leidt naar een vervalste bankwebsite waar een fraudeur inzage heeft in welke gegevens de klant invoert en de fraudeur is vervolgens in staat om met de prijsgegeven beveiligingsgegevens toegang te krijgen tot de betaalrekening van de klant. Uit de cijfers van de NVB blijkt ook dat schade als gevolg van fraude in het betalingsverkeer daalt, maar nog altijd omvangrijk is: het betrof een bedrag van € 36 miljoen in 2023.[5]

Net als bij 'traditionele' oplichting waarbij een klant fysiek zijn bankpas afgeeft, is ook bij online fraude de essentie dat klanten ten onrechte in de veronderstelling verkeren dat zij met medewerkers (en de digitale systemen) van hun eigen bank te maken hebben, terwijl het in werkelijkheid een fraudeur betreft. Extra pijnlijk is dat bij online fraude actieve medewerking van de betreffende klant noodzakelijk is om de fraude succesvol te voltooien. Op deze manier worden klanten van banken door fraudeurs ook vaak onder druk gezet middels *social engineering*. 'Social engineering' is een verzamelnaam voor misleidingstechnieken die gebruikt worden om mensen af te leiden en slachtoffer te maken van cybercrime en online fraude.[6] De fraudeur belt bijvoorbeeld een consument en doet zich voor als een medewerker van de bank die de klant informeert dat hij reeds slachtoffer is van fraude en hem helpt zijn geld veilig te stellen, terwijl in werkelijkheid de fraude op dat moment (mede door het handelen van de klant naar aanleiding van de schrikreactie die dat bericht teweeg brengt) door de fraudeur in gang wordt gezet.

Fraudeurs maken misbruik van het vertrouwen dat klanten hebben in (de medewerkers van) hun bank. Daardoor heeft fraude bij betaaldienstverlening niet alleen vermogensschade tot gevolg, maar ook beschadiging van het vertrouwen van klanten in de bancaire dienstverlening (en de financiële sector als geheel). Slachtoffers van online fraude stellen enerzijds dat zij zich 'dom' voelen[7] omdat zij in een oplichtingstruc zijn getrapt, anderzijds spreken slachtoffers ook veelal hun bank aan om de door de fraude geleden schade te verhalen. De vraag is of dat terecht is.

In dit artikel ga ik in op de aansprakelijkheid van banken bij niet-toegestane betalingstransacties, verschillende vormen van (digitale) fraude bij betaaldienstverlening en de zorgplicht van banken bij fraude bij betaaldienstverlening.

2. Aansprakelijkheid bij betaaldienstverlening

De Nederlandse regelgeving met betrekking tot betalingstransacties is geregeld in titel 7B van boek 7 BW. In deze titel is de herziene richtlijn betaaldien-

1. mr. drs. L. Stortelder is advocaat bij Hart advocaten N.V. in Amsterdam.
2. Ministerie van Veiligheid en Justitie, "Actieplan Integrale Aanpak Online Fraude" februari 2023, p. 3.
3. Uitsprakenregister Klachteninstituut Financiële Dienstverlening, raadpleegbaar op: https://www.kifid.nl/uitspraken/
4. NVB publicatie d.d. 8 april 2022: "Online-oplichters richten zich steeds meer op de klant" (raadpleegbaar op:https://www.nvb.nl/nieuws/online-oplichters-richten-zich-steeds-meer-op-de-klant/).
5. NVB publicatie d.d. 11 maart 2024: "Schade bankhelpdeskoplichting daalt met 45%" (raadpleegbaar op: https://www.nvb.nl/nieuws/schade-bankhelpdeskoplichting-daalt-met-45/
6. Rapport 'Campagne-effectonderzoek Social engineering: veilig internetten' 16 januari 2024, in opdracht van Ministerie van Justitie en Veiligheid.
7. NRC Handelsblad d.d. 30 juni 2020, "Meer meldingen WhatsApp-fraude: 'Hee mam, maak je geld over?"

sten PSD2[8] (en diens inmiddels ingetrokken voorganger PSD1[9]) geïmplementeerd. PSD2 (en dus ook titel 7B van boek 7 BW) bevat een eigen aansprakelijkheidsregime waarin een vergaande aansprakelijkheid van betaaldienstverleners is geregeld bij de uitvoering van niet-toegestane betalingstransacties, onjuist uitgevoerde transacties of niet tijdig uitgevoerde betalingsopdrachten.[10] Ik beperk mij in dit artikel tot aansprakelijkheid bij niet-toegestane betalingstransacties.

Een betalingstransactie mag alleen worden uitgevoerd wanneer de betaler (de klant) met deze transactie heeft ingestemd.[11] Deze instemming wordt verleend volgens de tussen de klant en de bank overeengekomen vorm en procedure.[12] Deze procedure stelt de bank in staat te 'authenticeren', hetgeen betekent dat de bank de identiteit van een klant dan wel de validiteit van het gebruik van een specifiek betaalinstrument verifieert.[13]De overeengekomen vorm en procedure houden in de praktijk bijvoorbeeld in dat de klant de betaling initieert door bepaalde handelingen in de digitale applicatie van de bank uit te voeren. Vervolgens accordeert de klant de betaling middels sterke cliëntauthenticatie[14]. De bank authentiseert vervolgens de gegevens en voert de transactie uit, mits de identiteit van de klant/het betaalinstrument correct zijn.

Indien een transactie door de bank wordt uitgevoerd zonder dat sprake is van instemming, wordt een betalingstransactie aangemerkt als 'niet-toegestaan'.[15] Indien een bank een niet-toegestane transactie heeft uitgevoerd, verplicht artikel 7:528 lid 1 BW de bank om het bedrag van een niet-toegestane betalingstransactie onmiddellijk terug te betalen aan de klant. De terugbetaling dient in elk geval uiterlijk aan het einde van de eerstvolgende werkdag nadat de bank bekend is geworden met de desbetreffende transactie te geschieden.[16] De klant dient de bank hiervoor wel onverwijld en uiterlijk dertien maanden na de valutadatum waarop zijn rekening is gedebiteerd, in kennis te stellen van de desbetreffende transactie.[17]

2.1. Toegestane en niet-toegestane betalingstransacties

Het verschil tussen een toegestane en niet-toegestane betalingstransactie is relevant omdat voor beide categorieën een apart wettelijk aansprakelijkheidsregime geldt. Bij een toegestane betalingstransactie dient eventuele schade in beginsel te worden gedragen door een klant, bij een niet-toegestane betalingstransactie door de bank. De eerste stap[18] in de beoordeling of een bank aansprakelijk is voor schade voortkomend uit een betalingstransactie, is derhalve dat vastgesteld dient te worden of sprake is van een toegestane of een niet-toegestane betalingstransactie.

Een toegestane betalingstransactie is een transactie waarmee een klant heeft ingestemd.
Een transactie waarmee een klant niet heeft ingestemd betreft een niet-toegestane betalingstransactie. Ook een transactie waarvan de bank bij betwisting dat dit een toegestane betalingstransactie betreft niet in staat is om het bewijs te leveren dat de betalingstransactie is geauthentiseerd, juist is geregistreerd en geboekt en niet door een technische storing of enig ander falen van de betaaldienstverlener is beïnvloed, betreft een niet-toegestane betalingstransactie.

Daarnaast geldt dat indien de transactie wel volgens de juiste vorm en procedure is gedaan maar het niet de klant zelf is die een betalingstransactie verricht, er ook sprake kan zijn van een niet-toegestane betalingstransactie. De Hoge Raad overwoog in het arrest *ING Bank / Van den Hurk* dat ingeval een derde op onrechtmatige wijze maar met toepassing van de tussen de betaler en zijn betaaldienstverlener overeengekomen vorm en procedure (op grond waarvan de betaaldienstverlener tot authenticatie kan overgaan) gebruikmaakt van het betaalinstrument, ook sprake kan zijn van een niet-toegestane betalingstransactie.[19] Deze situatie moet worden onderscheiden van de situatie waarin de klant wel zelf de betaling heeft geïnitieerd en de beveiligingsgegevens heeft ingevoerd die tot de overboeking hebben geleid, ook indien (op een later moment) blijkt dat een klant is misleid en onder invloed van die misleiding heeft ingestemd met een betaling: onder het huidige recht is dan in juridische zin ook sprake van een toegestane betalingstransactie. Er rust bij een toegestane betalingstransactie geen wettelijke vergoedingsplicht op de bank. Sterker nog, als betaaldienstverlener is de bank op grond van artikel 7:533 lid 4 BW verplicht om gehoor te geven aan een correct opgegeven betaalopdracht.[20]

8. Richtlijn (EU) 2015/2366Richtlijn 2007/64/EG.
9. Richtlijn 2007/64/EG, de richtlijn betaaldiensten (Payment Service Directive).
10. Artikel 71 lid 1, 73 en 74 PSD2, geïmplementeerd in art. 7: 526 e.v. BW.
11. Artikel 7:522 lid 1 BW.
12. Artikel 7:522 lid 2BW.
13. Artikel 7:514 sub a BW.
14. Artikel 7:514 sub ab: "*sterke cliëntauthenticatie: 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 de 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*".
15. Artikel 7:522 lid 2BW.
16. Artikel 7:528 lid 1 BW.
17. Artikel 526 lid 1 BW.
18. Het HvJEU overwoog in het arrest *ZG/Beobank* ook dat een nationale rechter eerst dient vast te stellen of sprake is van een toegestane danwel een niet-toegestane betalingstransactie (zie hierover paragraaf 2.1).
19. Hoge Raad 21 mei 2021, ECLI:NL:HR:2021:749 (*ING / Van den Hurk*), r.o. 3.2.2.
20. Zie bijvoorbeeld Geschillencommissie Kifid 27 juni 2024, nr. 2024-0542.

2.2. Verschillende vormen van fraude

In de praktijk bestaan er diverse vormen van fraude, deze worden aangeduid met verschillende begrippen zoals *spoofing* en *phishing*. Dit zijn begrippen die niet wettelijk zijn gedefinieerd en ook wettelijk geen betekenis hebben omdat in juridische zin alleen de vraag relevant is of een betaling een toegestane of niet-toegestane transactie is. Ook geldt dat in de praktijk vaak meerdere vormen van fraude tegelijkertijd plaatsvinden. Bijvoorbeeld worden eerst gegevens van een klant verkregen middels phishing, waarna de klant wordt misleid door een telefoontje dat van zijn bank afkomstig lijkt met een gespoofd telefoonnummer.

Voor een goed begrip volgt hierna een korte aanduiding van de verschillende soorten fraude die in dit artikel genoemd worden. Het betreft allemaal categorieën van fraude waarbij klanten worden opgelicht 'op afstand' en doordat een fraudeur misbruik maakt van de digitale diensten die klanten gebruiken voor het uitvoeren van transacties of het doen van bankzaken.

2.2.1. Bankhelpdeskfraude

Bankhelpdeskfraude is volgens recente cijfers van het CBS nog steeds de meest voorkomende vorm van online fraude.[21] Bij bankhelpdeskoplichting belt een fraudeur slachtoffers zogenaamd namens de bank. De fraudeur doet zich voor als een medewerker van de bank en vertelt de rekeninghouder dat zijn bankrekening niet meer veilig zou zijn. De rekeninghouder wordt misleid om zelf zijn banksaldo met één of meer overboekingen over te zetten naar een zogenaamd 'veilige rekening'. Soms wordt de rekeninghouder ook overtuigd om de betaalpas af te geven waarmee dan direct geld wordt opgenomen.[22]

2.2.2. Phishing

Bij phishing gaat het om alle vormen van online oplichting waarbij de fraudeur zich voordoet als iemand anders (een persoon of bedrijf) en via allerlei kanalen personen benadert met valse verhalen met als doel om geld te krijgen. Vaak worden veel personen tegelijk benaderd; soms wordt een phishing SMS of een phishingmail naar honderden telefoonnummer of mailadressen tegelijk verzonden.[23]

Bij phishing 'vissen' fraudeurs aan de telefoon of via valse berichten of brieven naar vertrouwelijke informatie. Deze valse berichten kunnen komen via e-mail, per telefoon, via sms of via een chatapp zoals WhatsApp. Phishing via sms wordt ook wel smishing genoemd.[24]

2.2.3. Spoofing

Bij spoofing wordt er door de fraudeur een andere identiteit aangenomen om de klant te misleiden om een bepaalde handeling uit te voeren.[25] Fraudeurs bootsen bij spoofing het telefoonnummer van een bank na en sturen daarmee een sms of bellen rekeninghouders om hen te overtuigen dat zij een betaling moeten doen. Een belangrijk verschil tussen spoofing en het hierboven aangeduide phishing, is dat spoofing veelal resulteert in een toegestane betalingstransactie omdat het de klant zelf is die de betaling initieert en de beveiligingscodes invoert. Dit betekent dat bij spoofing vaak geen schadevergoedingsplicht voor de bank ontstaat.

De bovenstaande begrippen worden overigens in de praktijk ook wel door elkaar gebruikt. Zo noemt de NVB in het persbericht over het NVB coulancebeleid bankhelpdeskfraude 'een vorm van spoofing'.[26] Het onderscheidende criterium in het kader van coulance is uiteraard of er wel of geen niet-toegestane transactie tot stand komt. Het coulancebeleid geldt alleen indien er geen sprake is van een niet-toegestane betalingstransactie en er dus geen wettelijke schadevergoedingsplicht op de bank rust (zie hierover ook paragraaf 7 van dit artikel).

3. Een exclusief aansprakelijkheidsregime

De tekst van titel 7B BW is vrijwel gelijkluidend aan de tekst uit de (PSD1 en) PSD2-richtlijn. De reden hiervoor is dat de Europese wetgever met (PSD1 en) PSD2 heeft willen voorzien in maximum harmonisatie. Van PSD2 kunnen de lidstaten dus niet afwijken, tenzij hier in de richtlijn expliciet ruimte voor is gegeven.[27] Ten aanzien van het aansprakelijkheidsregime van PSD2, geldt dat de richtlijn de lidstaten hierin geen ruimte heeft gegeven. Het is de lidstaten dus niet toegestaan om af te wijken van het aansprakelijkheidsregime van PSD2.[28]

21. Centraal Bureau voor de Statistiek, "Veiligheidsmonitor 2023", d.d. maart 2024, p. 48.
22. NVB publicatie d.d. 8 april 2022: https://www.nvb.nl/nieuws/online-oplichters-richten-zich-steeds-meer-op-de-klant/
23. Veiligheidsmonitor 2023 d.d. maart 2024,p. 49.
24. Website Veiligbankieren.nl, raadpleegbaar op: https://www.veiligbankieren.nl/fraude/phishing/.
25. Kamerbrief minister van Financiën d.d. 18 december 2020 (TK, vergaderjaar 2020–2021, 32 545, nr. 128).
26. https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing/
27. Artikel art. 107 lid 1 PSD2 en *Kamerstukken II* 2008/09, 31 892, nr. 3, p. 16.
28. Artikel 107 lid 1 PSD2: "*Onverminderd artikel 2, artikel 8, lid 3, artikel 32, artikel 38, lid 2, artikel 42, lid 2, artikel 55, lid 6, artikel 57, lid 3, artikel 58, lid 3, artikel 61, leden 2 en 3, artikel 62, lid 5, artikel 63, leden 2 en 3, artikel 74, lid 1, vierde alinea, en artikel 86 mogen de lidstaten, in zoverre deze richtlijn geharmoniseerde bepalingen bevat, geen andere bepalingen handhaven of vaststellen dan die welke in deze richtlijn zijn vervat.*" De artikelen in PSD2 op grond waarvan in art. 7: 526 e.v. BW de aansprakelijkheidsregeling voor niet-toegestane betalingstransacties is geïmplementeerd, behoren niet tot de bepalingen genoemd in art. 107 lid 1 PSD2.

Dit is bevestigd door het Europese Hof van Justitie (HvJ EU). De hoogste rechter in burgerlijke en strafzaken in Frankrijk (Cour de Cassation) heeft in 2021 aan het HvJ EU de prejudiciële vraag gesteld of de bepalingen van PSD volledig zijn geharmoniseerd '*zodat de lidstaten geen speelruimte hebben met betrekking tot de aansprakelijkheid van de partijen bij een betalingstransactie* (...)".[29] De feitelijke gang van zaken in deze Franse rechtszaak was dat de bank ná de vervaltermijn van 13 maanden in kennis was gesteld van een niet-toegestane betalingstransactie en aansprakelijk werd gesteld voor terugbetaling van het betreffende bedrag. De vraag aan het HvJ EU hield in of de bank toch aansprakelijk was op basis van een aansprakelijkheidsgrond uit het Franse nationale recht, ondanks het feit dat de vervaltermijn van 13 maanden uit PSD2 was overschreden.[30]

Het HvJ EU heeft bevestigd dat een lidstaat dergelijke speelruimte inderdaad niet heeft:

> *"41.Er dient te worden opgemerkt dat artikel 86 van richtlijn 2007/64, met als opschrift „Volledige harmonisatie", bepaalt: „Onverminderd [meerdere bepalingen van die richtlijn] mogen de lidstaten, in zoverre deze richtlijn geharmoniseerde bepalingen bevat, geen andere bepalingen handhaven of vaststellen dan die welke in deze richtlijn zijn vervat." De artikelen* ***58, 59 en 60*** *van deze richtlijn* ***behoren niet tot de bepalingen waarvoor artikel 86 de lidstaten bij de tenuitvoerlegging ervan speelruimte laat****.*
>
> *42. Hieruit volgt dat de aansprakelijkheidsregeling voor betalingsdienstaanbieders die is neergelegd in artikel 60, lid 1, van richtlijn 2007/64 en in de artikelen 58 en 59 van die richtlijn,* ***volledig is geharmoniseerd, zodat de lidstaten geen parallelle aansprakelijkheids- regeling voor hetzelfde feit in stand kunnen houden.***
>
> *"(..)"*
>
> *45. Naast de bij richtlijn /64 vastgestelde geharmoniseerde aansprakelijkheidsregeling voor niet-toegestane of foutieve transacties kan een andere, op dezelfde feiten en grondslag gebaseerde aansprakelijkheidsregeling van nationaal recht* ***enkel worden toegepast indien daardoor geen afbreuk wordt gedaan aan de bij deze richtlijn vastgestelde regeling, noch aan de doelstellingen en het nuttig effect van deze richtlijn.***[31]

Een parallelle (nationale) aansprakelijkstelling op grond waarvan de bank door een betaler wordt aangesproken tot terugbetaling van een niet-toegestane transactie terwijl de kennisgevingstermijn van dertien maanden uit PSD2 is overschreden, is daarom niet toegestaan.

Het HvJ EU heeft voorgaande nogmaals bevestigd in een uitspraak van 16 maart 2023.[32] In deze zaak werd de Belgische Beobank door een klant aansprakelijk gesteld voor terugbetaling van een niet-toegestane betalingstransactie op grond van een vermeende schending van een informatieplicht (Beobank had bepaalde informatie omtrent de begunstigde van de uitgevoerde betalingstransactie niet aan de klant verstrekt).

Het HvJ EU overweegt dat vanwege de volledige harmonisatie van het aansprakelijkheidsregime uit PSD, een nationale rechter zich pas kan uitspreken over een verzoek tot terugbetaling van een transactie nadat de rechter heeft vastgesteld of sprake is van een toegestane danwel niet-toegestane betaling. Dat de bank bepaalde informatie niet aan een klant heeft verstrekt kan
– kort gezegd – niet als grondslag dienen voor een aanspraak van een klant tot terugbetaling van een niet-toegestane betalingstransactie.

PSD staat immers in de weg aan terugbetaling van een niet-toegestane transactie op grond van een andere grondslag dan de aansprakelijkheidsregeling in (destijds) artikel 58 t/m 60 PSD:

> *"39. Zoals de advocaat-generaal in de punten 53 en 60 van zijn conclusie heeft opgemerkt, kan een nationale rechter dus niet voorbijgaan aan het onderscheid dat in richtlijn 2007/64 met betrekking tot betalingstransacties wordt gemaakt naargelang deze al dan niet toegestaan zijn.* ***Hij kan zich dus pas uitspreken over een verzoek tot terugbetaling van de in het hoofdgeding aan de orde zijnde betalingen nadat hij deze heeft gekwalificeerd als betalingen die toegestaan dan wel niet-toegestaan zijn.***
>
> *Artikel 60, lid 1, van richtlijn 2007/64, gelezen in samenhang met artikel 86, lid 1, van deze richtlijn, staat er namelijk aan in de weg dat een betalingsdienstgebruiker de betalingsdienstaanbieder aansprakelijk stelt omdat deze zijn in artikel 47, lid 1, onder a), van die richtlijn neergelegde informatieplicht niet is nagekomen, voor zover deze aansprakelijkheid betrekking heeft op de terugbetaling van betalingstransacties.*
>
> *40. Hieruit volgt dat, anders dan de verwijzende rechter lijkt aan te nemen, de eventuele niet-nakoming door Beobank van haar verplichting om de in artikel 47, lid 1, onder a), van richtlijn 2007/64 bedoelde informatie te verstrekken, waarop de prejudiciële vragen betrekking hebben,* ***op zich niet kan resulteren in een verplich-***

29. Concl. A-G H. Saugmandsgaard Øe 8 juli 2021, ECLI:EU:C:2021:564 (*DM en LR/CRCAM*), r.o. 3.
30. HvJ EU 2 september 2021, ECLI:EU:C:2021:671 (*DM en LR/CRCAM*).
31. HvJ EU 2 september 2021, ECLI:EU:C:2021:671 (*DM en LR/CRCAM*), r.o. 41, 42.
32. HvJ EU 16 maart 2023, ECLI:EU:C:2023:215 *(ZG / Beobank SA).*

ting tot terugbetaling van de in het hoofdgeding aan de orde zijnde betalingen."[33]

Uit het voorgaande volgt derhalve ook dat de aansprakelijkstelling van een betaaldienstverlener door een klant op grond van (enkel) artikel 6:162 BW niet mogelijk is (indien daarmee afbreuk wordt gedaan aan de aansprakelijkheidsregeling van PSD2).

4. Bewijslast

Titel 7B van boek 7 BW kent een eigen regeling ten aanzien van de bewijslastverdeling bij niet-toegestane betalingstransacties die afwijkt van de hoofdregel van artikel 150 Rv. Indien een klant zich op het standpunt stelt dat hij niet met de betaling heeft ingestemd of aanvoert dat de betalingstransactie niet correct is uitgevoerd, rust de bewijslast om aan te tonen dat de betalingstransactie is geauthentiseerd, juist is geregistreerd en geboekt en niet door een technische storing of enig ander falen van de betaaldienstverlener is beïnvloed, op de betaaldienstverlener.[34] Als de bank niet slaagt in het leveren van dit bewijs, wordt aangenomen dat de instemming ontbreekt en wordt de betalingstransactie aangemerkt als niet-toegestaan.[35]

De bewijslast van de betaaldienstverlener wordt voorts verzwaard doordat uit artikel 7:527 lid 2 BW volgt dat het enkele feit dat het gebruik van een betaalinstrument door de betaaldienstverlener is geregistreerd niet noodzakelijkerwijs afdoende bewijs is dat met de betalingstransactie is ingestemd, of dat de betaler frauduleus heeft gehandeld of grof nalatig is geweest. De Commissie van Beroep van het Kifid oordeelde in een uitspraak uit 2020 dat het enkele feit dat een consument de betaling zelf geaccordeerd had met zijn pas, pincode en Rabo Scanner – niet wetende dat dit een transactie naar de fraudeur (een familielid, hierover later meer) betrof – geen afdoende bewijs was dat de consument ook daadwerkelijk met deze transactie had ingestemd.[36] De bewijslast om aan te tonen dat sprake is van frauduleus of grof nalatig handelen door de klant, ligt eveneens bij de betaaldienstverlener.[37]

5. Uitzondering bij frauduleus handelen en grove nalatigheid

Het aansprakelijkheidsregime van PSD2 kent een uitzondering op de terugbetalingsverplichting van de bank indien sprake is van een niet-toegestane betalingstransactie. De betaaldienstverlener is niet aansprakelijk voor verliezen die voortvloeien uit niet-toegestane betalingstransacties die zijn veroorzaakt door frauduleus handelen of opzettelijk of met grove nalatigheid niet nakomen van één of meer verplichtingen uit artikel 7:524 BW door de betaler.[38] De verplichtingen voor een klant houden – kort gezegd – op grond van artikel 7:524 in:

i. De klant handelt conform de op de betaaldienstverlening van toepassing zijnde (algemene) voorwaarden; en
ii. De klant stelt de bank onverwijld in kennis van verlies, diefstal of onrechtmatig gebruik van het betaalinstrument (zoals de bankrekening, de bankapplicatie of een betaalpas).

Oftewel, als een klant 1) zelf frauduleus heeft gehandeld of 2) opzettelijk of met grove nalatigheid in strijd handelt in strijd met zijn verplichtingen uit de toepasselijke (algemene) voorwaarden, of 3) de bank niet onverwijld in kennis heeft gesteld, moet hij zelf de schade dragen. Ten aanzien van de kennisgevingsverplichting oordeelde de Hoge Raad in *ING Bank / Van den Hurk* dat deze verplichting eerst aanvangt op het moment dat de klant (subjectieve) bekendheid heeft van de niet-toegestane transactie.[39] In dit arrest overwoog de Hoge Raad voorts dat op een betaaldienstgebruiker die consument is, geen plicht rust om bankafschriften direct na ontvangst te controleren, ook niet als dit in de algemene voorwaarden van de desbetreffende bank is bepaald.[40]

In het procesdebat is vaak het punt van discussie of sprake is van punt 2, namelijk of de klant met grove nalatigheid in strijd heeft gehandeld met de toepasselijke voorwaarden. Het is – zoals hiervoor opgemerkt – aan de bank om aan te tonen dat sprake is van grof nalatig handelen van de klant.

5.1. Verzwaarde stelplicht van de klant

Wel geldt dat door het Kifid en de civiele rechter een vaste lijn wordt gehanteerd dat er – indien door de bank het standpunt wordt ingenomen dat sprake is van grof nalatig handelen door de klant – op de desbetreffende klant een verzwaarde stelplicht rust. Deze verzwaarde stelplicht houdt in dat een klant niet kan volstaan met het antwoord 'Ik weet niet wat er is gebeurd', maar hij zal inzicht moeten geven ten aanzien van de wijze waarop het betaalinstrument in onbevoegde handen zou kunnen zijn geraakt, zodat de bank zich daarover een beeld kan vormen. Ook moet de klant zo concreet mogelijk moeten stellen en onderbouwen hoe hij gebruik heeft gemaakt van zijn betaalinstrument.

Een andersluidende regel zou banken voor onaan-

33. HvJ EU 16 maart 2023, ECLI:EU:C:2023:215 *(ZG / Beobank SA)*, r.o. 37-38.
34. Artikel 7:527 lid 1 BW.
35. Artikel 7:522 lid 2 BW.
36. Commissie van Beroep Kifid 15 juni 2020, nr. 2020-027, r.o. 5.25.
37. Zie onder meer Rechtbank Amsterdam 20 december 2023, ECLI:NL:RBAMS:2023:8673 en Rechtbank Amsterdam 29 juli 2024, ECLI:NL:RBAMS:2024:4973.
38. Artikel 7:529 lid 1 BW.
39. Hoge Raad 21 mei 2021, ECLI:NL:HR:2021:749 (*ING / Van den Hurk*), r.o. 3.3.2.
40. Aangezien op grond van 7:550 BW niet ten nadelen van de betaaldienstgebruiker die een consument is van het bepaalde bij Titel 7B van Boek 7 BW kan worden afgeweken.

vaardbare risico's van misbruik plaatsen, zo overwoog het Kifid:

> *"Alhoewel het aan de Bank is om te bewijzen dat sprake is van grove nalatigheid aan de zijde van Consument, rust op Consument een* ***'verzwaarde stelplicht'****. Zie Geschillencommissie Kifid nrs. 2019-308, 2019-733 en 2020-853. Dat betekent dat Consument* ***tenminste enig inzicht dient te geven in de wijze waarop haar gegevens in onbevoegde handen zouden kunnen zijn geraakt, zodat de Bank zich daarover een beeld kan vormen.*** *Een andere regel zou de Bank voor onaanvaardbare risico's van misbruik plaatsen. Zie Geschillencommissie Kifid nrs. 2014-144 en 2019-733.*
>
> *Dat betekent dat Consument* ***zo concreet mogelijk zal moeten stellen en onderbouwen wanneer en op welke wijze zij gebruik maakte van haar digitale omgeving en hoe zij de veiligheid daarvan garandeerde. Voorts kan van haar worden verwacht dat zij zo goed mogelijk een verklaring zal moeten bieden voor de omstandigheid dat haar gegevens kennelijk bij derden bekend zijn geraakt. Daarbij kan Consument niet volstaan met te stellen dat zij dat niet weet****, maar zal zij in dat geval ook moeten onderbouwen waarom zij die informatie niet kan geven. Zie ook Geschillencommissie Kifid nr. 2015-322."*[41]

En:

> *"Dat betekent dat Consument tenminste* ***enig inzicht dient te geven*** *in de wijze waarop de inlogcode in onbevoegde handen zou kunnen zijn geraakt, zodat de Bank zich daarover een beeld kan vormen. Een andere regel zou de Bank voor onaanvaardbare risico's van misbruik plaatsen. Zie Geschillencommissie KiFiD nrs. 2014-144 en 2019-733.* ***Dat betekent dat Consument zo concreet mogelijk zal moeten stellen en onderbouwen wanneer en op welke wijze zij gebruik heeft gemaakt van het betaalinstrument en de daarbij behorende inlogcode en daarbij ook zo goed mogelijk een verklaring zal moeten bieden voor de omstandigheid dat de inlogcode kennelijk bij derden bekend is geraakt. Daarbij kan Consument niet volstaan met te stellen dat zij dat niet weet****, maar zal zij in dat geval ook moeten onderbouwen waarom zij die informatie niet kan geven."*[42]

De rechtbank Amsterdam heeft met zoveel woorden bevestigd dat een klant in dit verband niet kan volstaan met een enkele, niet verder onderbouwde betwisting dat hij niet weet hoe een ander de beschikking heeft verkregen over zijn inlogcodes en andere beveiligingsfeatures.

De klant dient aanknopingspunten te verstrekken over de wijze waarop hij de digitale bankomgeving en zijn apparaten heeft gebruikt en hoe de fraudeur toegang heeft weten te krijgen tot zijn rekeningen.[43] Indien een klant niet aan zijn verzwaarde stelplicht voldoet, wordt overgegaan tot afwijzing van zijn vordering.

5.2. Grove nalatigheid

De preambule van PSD2 vermeldt dat, om te kunnen beoordelen of er sprake is van nalatigheid of grove nalatigheid, alle omstandigheden in aanmerking moeten worden genomen en dat het bewijs voor en de mate van de beweerde nalatigheid moet volgens het nationale recht worden beoordeeld.[44] Verder vermeldt de preambule dat grove nalatigheid meer inhoudt dan louter nalatigheid, dus gedrag dat een aanzienlijke mate van onvoorzichtigheid vertoont; bijvoorbeeld het bewaren van de voor het verlenen van toestemming voor een betalingstransactie gebruikte beveiligingsgegevens naast het betaalinstrument in een open en voor derden gemakkelijk op te sporen formaat.[45] De rechtbank Rotterdam hanteerde in een uitspraak uit 2015 het maatmancriterium en overwoog dat onder grove nalatigheid in de zin van artikel 7:529 BW wordt verstaan een handelen met aanzienlijke mate van onvoorzichtigheid dat buiten de reikwijdte valt van *"hetgeen van een normaal geïnformeerde en redelijk oplettende betaaldienstgebruiker verwacht mag worden"*.[46] Een concrete invulling van deze norm is per definitie afhankelijk van de casuïstiek, maar uit de verschillende, met name Kifid-uitspraken zijn wel een aantal terugkerende overwegingen te destilleren.

5.2.1. Wanneer wel grof nalatig

Hierna volgen drie voorbeelden van situaties waarin gedragingen van rekeninghouders (meermaals) in de jurisprudentie of uitspraken van het Kifid als grof nalatig handelen zijn gekwalificeerd:

1. Het laten meekijken van derden via 'meekijksoftware' zoals AnyDesk (zoals bij helpdeskfraude) kwalificeert als grof nalatig handelen.[47] Door op deze wijze persoonlijke bankgegevens te delen en toe te staan dat derden toegang te verkrijgen, is volgens de Geschillencommissie van het Kifid 'evident in strijd met de veiligheidsregels' uit de toepasselijke voorwaarden:

41. Geschillencommissie Kifid 4 december 2020, nr. 2020-994, r.o. 3.7.
42. Geschillencommissie Kifid 21 oktober 2020, nr. 2020-853, ro 4.5
43. Rechtbank Amsterdam 20 december 2023, ECLI:NL:RBAMS:2023:8673, r.o. 4.3.
44. Preambule 72 PSD2.
45. Preambule 72 PSD2.
46. Rb. Rotterdam 5 november 2015, ECLI:NL:RBROT:2015:9378 (*X/Rabobank*), r.o. 5.4.
47. Onder meer: Geschillencommissie Kifid 11 maart 2022, nr. 2022-0935, Geschillencommissie Kifid 28 februari 2023, nr. 2023-0171.

> *"Uit de processtukken blijkt dat de consument* ***de oplichter toegang heeft gegeven tot zijn iPad nadat deze hem had bewogen het programma AnyDesk op zijn iPad te downloaden****. Daarna heeft de consument op verzoek van de oplichter internetbankieren opgestart. Eerst op zijn computer, en toen dat niet lukte, op zijn iPad. Vervolgens heeft hij de oplichter toegang verleend tot zijn iPad. Naar het oordeel van de commissie heeft de consument daarmee gehandeld in strijd met de veiligheidsregels, hiervoor opgenomen onder 2.6. Nadat de consument het programma AnyDesk had gedownload, heeft hij de oplichter in staat gesteld om op afstand een bedrag van de betaalrekening over te maken naar een andere betaalrekening.*
>
> ***De commissie is van oordeel dat de consument hiermee evident in strijd met de hem verstrekte veiligheidsregels voor (internet) bankieren als hiervoor onder 2.6 vermeld, heeft gehandeld en bovendien (eerder) argwaan had moeten krijgen dat er iets niet klopte en dat hij de betalingstransactie had kunnen voorkomen. Door dat niet te doen kan zijn handelen als grof nalatig in de zin van de wet worden gekwalificeerd****."*[48]

De Geschillencommissie wijst er in een andere uitspraak tevens op dat van consumenten mag worden verwacht dat zij in dergelijke situaties op een enig moment argwaan krijgen:

> *"Nadat de consument het programma AnyDesk had gedownload, heeft hij in opdracht van de oplichter diverse bedragen van de spaarrekening naar de rekening-courant overgemaakt en vervolgens vanaf de rekening-courant naar de betaalrekeningen van twee voor hem volstrekt onbekende begunstigden. De commissie is van oordeel dat de consument hiermee* ***evident in strijd met de hem verstrekte veiligheidsregels voor (internet)bankieren heeft gehandeld en bovendien (eerder) argwaan had moeten krijgen dat er iets niet klopte en dat hij de betalingstransacties had kunnen voorkomen****. Door dat niet te doen kan zijn handelen als grof nalatig in de zin van de wet worden gekwalificeerd."*[49]

2. Het delen van vertrouwelijke gegevens door phishing nadat de consument indringend was gewaarschuwd voor de gevaren van phishing, is gekwalificeerd als grof nalatig handelen.[50] In het algemeen geldt overigens ook dat voor het beoordelen van de vraag of sprake is van grof nalatig handelen, van belang is in hoeverre de consument was voorgelicht over de gevaren van de desbetreffende fraudemethode:

> *"De vraag die moet worden beantwoord is of de fraude die zich heeft voorgedaan in dit geval mogelijk is gemaakt doordat Consument grof nalatig heeft gehandeld ten aanzien van de veiligheidsvoorwaarden. De Commissie stelt daarbij voorop dat van consumenten die gebruik maken van het betalingsverkeer mag worden verwacht dat zij voldoende zorgvuldigheid betrachten ten aanzien van de verstrekte betaalinstrumenten en veiligheidscodes. Bij de toepassing van deze maatstaf komt het aan op alle omstandigheden van het geval, waarbij dient te worden uitgegaan van de gemiddelde consument. Tevens dient er rekening mee te worden gehouden dat criminelen steeds nieuwe uiterst geraffineerde trucs bedenken om de beveiligingssystemen van banken te omzeilen, waarbij zij de medewerking van consumenten proberen te verwerven.* ***Daarom is mede van belang in hoeverre consumenten zijn voorgelicht over vormen van criminaliteit die zij zonder deze voorlichting niet hadden behoeven te doorzien.*** *(..)*
>
> ***De Commissie is van oordeel dat Consument ten tijde van het incident afdoende was gewaarschuwd voor phishing.*** *Zij had hetzij via Rabo Internetbankieren gekoppeld aan andere rekeningen die Consument bij Aangeslotene aanhoudt, hetzij via de website van Aangeslotene, hetzij via de media op de hoogte dienen te zijn van het gevaar van phishing. Hieraan doet niet af dat Aangeslotene deze vorm van fraude niet expliciet onder de aandacht van Consument heeft gebracht tijdens de gesprekken die tussen Consument en Aangeslotene hebben plaatsgevonden nu reeds in het algemeen voldoende informatie over phishing is verstrekt en hiervoor ook voldoende indringend is gewaarschuwd.* ***De omstandigheid dat Consument de inhoud van de waarschuwingen kennelijk niet tot zich heeft genomen, is een omstandigheid die voor haar risico dient te blijven*** *zodat het standpunt van Consument dat geen van de waarschuwingen van Aangeslotene haar bekend is in het oordeel van de Commissie geen verandering kan brengen."*[51]

Van consumenten mag dus ook worden verwacht dat zij kennisnemen van de desbetreffende waarschuwingen van de bank en op basis hiervan ook hun handelingen afstemmen.

3. Het negeren van waarschuwingen en het nalaten van het treffen van schadebeperkende maatregelen is gekwalificeerd als grof nalatig handelen. De rechtbank Amsterdam oordeelde dat het enkele klikken op een phishing-

48. Geschillencommissie 11 maart 2022, nr. 2022-0935.
49. Geschillencommissie Kifid 28 februari 2023, nr. 2023-0171.
50. Geschillencommissie Kifid 20 augustus 2019, nr. 2019-600 en Geschillencommissie Kifid 9 december 2013, nr. 2013-355. Het Kifid oordeelde in één zaak overigens dat het klikken op een phishinglink in de desbetreffende zaak wel als 'nalatig' kwalificeerde, maar vanwege de omstandigheden van dat geval niet als 'grof nalatig'.
In deze zaak is de vordering van de consument toegewezen: zie Geschillencommissie 14 juli 2023, nr. 2023-0531.
51. Geschillencommissie Kifid 9 december 2013, nr. 2013-355.

link kon worden gezien als een '*menselijke fout die ook anderen had kunnen overkomen*' maar dat vervolgens het negeren van waarschuwingen door de bank en het nalaten van het treffen van schadebeperkende maatregelen, maakte dat sprake was van grove nalatigheid:

> *"De rechtbank volgt het beroep van de Bank op grove nalatigheid aan de kant van [eisende partij] vanwege het volgende. Op zich is invoelbaar dat [eisende partij] na ontvangst van het phishing-bericht (7 juli 2022, 19:54 uur) op de link heeft geklikt in de veronderstelling dat ze met de Bank van doen had.* ***Dit kan als een menselijke fout gezien worden die ook anderen had kunnen overkomen. Maar vervolgens had [eisende partij] haar fout kunnen inzien en herstellen en dit had ook van haar verwacht mogen worden.*** *Daar gaf het systeem van de Bank [eisende partij] namelijk voldoende tijd en gelegenheid voor. [eisende partij] ontving dezelfde avond (22: 20) het bankbericht over een new device terwijl daar bij [eisende partij] geen sprake van was. Vervolgens heeft de Bank dezelfde avond om 22: 45 uur [eisende partij] gemaild met het waarschuwingsbericht dat er met een nieuwe iPhone was ingelogd. [eisende partij] had toen 24 uur de tijd om deze signalen op te pakken en zich te realiseren dat er iets met een nieuw apparaat gebeurde, terwijl [eisende partij] geen nieuw apparaat probeerde te koppelen. Na deze afkoelingsperiode werd het in de avond van 8 juli 2022 voor de fraudeur mogelijk om op de nieuw gekoppelde iPhone in te loggen met [eisende partij] persoonlijke codes, haar e-mailadres te wijzigen en transacties van boven de 500 te verrichten als gevolg waarvan [eisende partij] haar volledige saldo verloor."*[52]

En in een soortgelijke zaak oordeelde de rechtbank Amsterdam dat de klant door niet te reageren op waarschuwingen van de bank over mogelijke fraude, niet voldeed aan zijn schadebeperkingsplicht:

> *"In de voorwaarden van [bank] staat dat [eiser] geen inlogcodes en andere beveiligingsfeatures mag delen met anderen en dat hij deze strikt geheim moet houden. Ook staat er dat hij onregelmatigheden direct moet melden. Vast staat dat hij een e-mail heeft ontvangen van [bank] en dat er een nieuw apparaat gekoppeld was (zie 2.3),* ***dat hij die e-mail ook twee keer heeft geopend vóór de niet toegestane betalingstransacties, maar daar niets mee heeft gedaan. Het feit dat de persoonlijke pincode én de Magic Link bij de fraudeur terecht zijn gekomen en de enige verklaring van [eiser] ten aanzien daarvan is dat hij niet weet hoe dit kan, plus het feit dat hij de waarschuwings e-mail heeft genegeerd, maakt dat er sprake is van grove nalatigheid*** *in de zin van artikel 7:529 en 524 lid 1 sub a BW.*
> (..)
>
> *Het negeren van de waarschuwings e-mail van [bank] maakt bovendien dat [eiser] niet heeft voldaan aan zijn schadebeperkingsplicht. [Bank] blokkeert standaard na het koppelen van een nieuwe telefoon betalingen van meer dan 500,00 voor de duur van 24 uur. Als [eiser] naar aanleiding van de waarschuwings e-mail actie had ondernomen, was er geen geld overgemaakt door de fraudeur.* ***Dat maakt dat [eiser] niet heeft voldaan aan zijn schadebeperkingsplicht****."*[53]

Uit al deze uitspraken blijkt met zoveel woorden dat in elke situatie alle omstandigheden van het desbetreffende geval moeten worden meegenomen, hetgeen het lastig maakt om 'vuistregels' te formuleren voor wanneer een klant wel of niet grof nalatig handelt.

Ter illustratie daarom ook een aantal voorbeelden uit jurisprudentie en uitspraken van het Kifid waarin is geoordeeld dat een klant niet grof nalatig heeft gehandeld, ondanks dat zijn beveiligingsgegevens in handen van derden terecht waren gekomen.

5.2.2. Wanneer niet grof nalatig

De Hoge Raad in het hiervoor aangehaalde arrest *ING / Van den Hurk* en de Commissie van Beroep het Kifid in een uitspraak uit 2020, kwamen in deze twee zaken tot het oordeel dat geen sprake was van grof nalatig handelen van de zijde van de consument hoewel wel beveiligingsgegevens van het betaalinstrument, in strijd met de voorwaarden van de bank, bij derden terecht waren gekomen.

Wat opvalt aan deze twee uitspraken is dat dit beide uitspraken betreft waarin consumenten niet zijn opgelicht door een onbekende derde (middels digitale fraude), maar zijn misleid door een naast familielid waarop zij hadden vertrouwd.[54] De Commissie van Beroep overwoog in de desbetreffende zaak:

> *"De Bank heeft grove nalatigheid niet aannemelijk gemaakt.* ***Niet ieder tekortschieten in de voor de Consument geldende verplichtingen leidt automatisch tot de gevolgtrekking dat sprake is van grove nalatigheid****. Consument is weliswaar nalatig geweest maatregelen te treffen om te voorkomen dat de schoonzoon gedurende lange tijd zonder toestemming van Consument overboekingen naar zichzelf kon doen,* ***maar er is geen sprake van grove nalatigheid in de zin dat hij bewust roekeloos nalatig is geweest. Daarbij is van belang dat Consument***

52. Rechtbank Amsterdam 12 juni 2024, ECLI:NL:RBAMS: 2024:3461, r.o. 4.12.
53. Rechtbank Amsterdam 12 december 2023, ECLI:NL: RBAMS:2023:8673, r.o. 4.4.
54. Commissie van Beroep Kifid 15 juni 2020, 2020-027, Hoge Raad 21 mei 2021, ECLI:NL:HR:2021:749 (*ING / Van den Hurk*),

> ***in dit geval – naar achteraf bleek: ten onrechte – vertrouwde op de hulpvaardigheid van een familielid.***"[55]

Een andere uitspraak waarin de Geschillencommissie tot het oordeel kwam dat sprake was van nalatigheid, maar niet van grove nalatigheid terwijl wel beveiligingsgegevens en de bankpas door de consumenten waren vertrekt, was in de situatie dat een ouder stel – kennelijk – in het bankfiliaal door een medewerker werd opgelicht. De commissie kwam tot dit oordeel omdat naar haar oordeel de consumenten niet nalatig, maar juist erg voorzichtig waren met hun gegevens.[56]

Eenzelfde redenering werd gevolgd in een andere uitspraak waarin de Geschillencommissie oordeelde dat geen sprake was van grove nalatigheid, hoewel wel de gegevens en de bankpas waren afgegeven. De commissie was van oordeel dat er voldoende beveiligingsmaatregelen waren getroffen door de consumenten zodat er geen sprake was van grove nalatigheid:

> *"De commissie is van oordeel dat de bank onvoldoende feiten en omstandigheden heeft aangedragen om te kunnen concluderen dat de consumenten bewust roekeloos nalatig (en dus grof nalatig) hebben gehandeld. Niet vastgesteld kan worden dat de consumenten zich op enig moment daadwerkelijk bewust waren van het gevaar dat hun bankpas kon worden misbruikt door deze af te geven aan de fraudeur die zich als gemachtigde van de bank voordeed en dat de consumenten hun bankpas en pincode ondanks dit bewustzijn alsnog hebben afgegeven.*
>
> ***Hierbij is met name van belang dat de consumenten hun bankpas eerst hebben doorgeknipt om deze onbruikbaar te maken, voordat zij deze hebben afgegeven. De consumenten hebben daarmee de instructie opgevolgd die de bank bij een nieuwe betaalpas geeft en die op de website van de bank staat****. Uit de door de bank verstrekte informatie blijkt niet dat de bank in die instructie ook voorschrijft hoe de pas moet worden doorgeknipt om deze onbruikbaar te maken. Dit leidt naar het oordeel van de commissie tot de conclusie dat de consumenten niet grof nalatig hebben gehandeld door de pas af te geven nadat zij deze hadden doorgeknipt. Dit oordeel wordt niet anders doordat de consumenten ook de pincode hebben verstrekt. Zij gingen ervan uit en zij mochten er, gelet op de instructie van de bank, ook van uitgaan dat de doorgeknipte bankpas onbruikbaar was en met de pincode geen geld van de rekening kon worden overgeschreven of opgenomen."*[57]

Afgezien van de bovengenoemde zaken, is bij mijn weten het aantal zaken waarin is geoordeeld dat geen sprake is van grof nalatig handelen door de betaaldienstgebruiker bij niet-toegestane transacties indien beveiligingsgegevens in handen van onbevoegde derden zijn geraakt, gering.

5.3. Beperking aansprakelijkheid klant ondanks grove nalatigheid

Tot slot bevat artikel 7:529 lid 2 BW nog de mogelijkheid voor de rechter om de aansprakelijkheid van klanten die hun verplichtingen uit hoofde van artikel 7:524 niet zijn nagekomen (en voor wiens rekening derhalve in beginsel de schade komt), te beperken indien geen sprake is van frauduleus of opzettelijk handelen. Hoewel door consumenten regelmatig een beroep is gedaan op deze aansprakelijkheidsbeperking, is deze zelden gehonoreerd. De Geschillencommissie van het Kifid heeft een beroep op deze aansprakelijkheidsbeperking een enkele keer gehonoreerd omdat volgens de commissie geen sprake was van 'persoonlijke verwijtbaarheid' van de desbetreffende consument.

In een uitspraak uit 2023 beperkte de Geschillencommissie de aansprakelijkheid van de consument in een zaak waarbij de consument aantoonbaar mentaal in een kwetsbare positie verkeerde en als gevolg van afpersing, bedreiging en diefstal zijn beveiligingsgegevens had gedeeld. De Geschillencommissie overwoog:

> *"De commissie beslist tot beperking van de aansprakelijkheid van de consument en overweegt als volgt. Voor de commissie staat vast dat de consument niet frauduleus of opzettelijk heeft gehandeld.*
>
> *De consument heeft de omstandigheden waaronder derden in het bezit zijn gekomen van zijn bankpas, pincode en inlogcodes voor het online bankieren onderbouwd. Dit heeft hij gedaan met een afschrift van het proces-verbaal van de gedetailleerde politieaangifte en schermafbeeldingen van telefoonberichten die hij heeft ontvangen van de daders. De daders hebben in de periode van 18 december 2021 tot en met 24 februari 2022 misbruik gemaakt van zijn bankrekening en zijn gelden opgenomen.* ***De consument heeft met verklaringen van zijn professionele zorgverleners aangetoond dat sprake is van een kwetsbare geestestoestand.***
>
> ***Rekening houdend met deze omstandigheden en de mate van persoonlijke verwijtbaarheid van de consument zoals geschetst in de overwegingen 2.9 en 2.10, beperkt de commissie de aansprakelijkheid van de consument tot de helft van de schade****, zodat de helft voor rekening komt van de bank."*[58]

55. Commissie van Beroep Kifid 15 juni 2020, 2020-027.
56. Geschillencommissie 12 januari 2022, nr. 2022-0021.
57. Geschillencommissie 6 december 2022, nr. 2022-1032.
58. Geschillencommissie 17 oktober 2023, nr. 2023-0779.

In een andere zaak oordeelde de Geschillencommissie dat geen sprake was van persoonlijke verwijtbaarheid van een consument, vanwege een onduidelijke instructie van de desbetreffende bank:

> *"De commissie beslist tot beperking van de aansprakelijkheid van de consument en overweegt als volgt. De bank heeft de consument in de brief van 27 maart 2019 waarmee zij haar bankpas die gebruikt is bij de fraude heeft verstrekt de volgende instructie gegeven over de wijze waarop een bankpas kan worden weggegooid: Als u uw nieuwe pas eenmaal heeft gebruikt, blokkeren wij automatisch uw oude pas. U kunt uw oude pas bij de chip doorknippen en weggooien. De consument kreeg van de fraudeur de instructie de bankpas in de lengte en door een bepaald plaatje net onder het midden door te knippen. Hoewel deze twee instructies niet identiek zijn, kan niet zonder meer geconcludeerd worden dat deze instructies praktisch gezien van elkaar verschillen.* ***De instructie van de bank is namelijk op meerdere manieren uit te leggen.***
>
> ***Rekening houdend met deze omstandigheden kan niet worden gezegd dat dat de persoonlijke verwijtbaarheid van de consument zodanig is dat zij met het dragen van alle hiervoor beschreven schade – geheel - dient te worden belast.*** *Aldus beperkt de commissie de aansprakelijkheid van de consument tot de helft van de schade (..)."*[59]

Uit het voorgaande volgt dat het besluit tot beperking van de aansprakelijkheid afhangt van de vraag of – naar het oordeel van de rechter – de klant een persoonlijk verwijt kan worden gemaakt. Dit kan, gezien het voorgaande, zowel liggen in de persoonlijke omstandigheden van de klant maar ook in omstandigheden die door de bank zijn gecreëerd.

6. Zorgplicht van de bank bij fraude

Een bank kan uiteraard (ook) aansprakelijk worden gesteld op een andere gronden voor schade als gevolg van fraude. In het procesdebat stellen klanten die slachtoffer zijn geworden van fraude zich regelmatig op het standpunt dat de bank haar zorgplicht heeft geschonden doordat de bank – kort gezegd – de fraude niet heeft voorkomen dan wel dat de bank deze fraude niet op tijd heeft opgemerkt. Hierna ga ik in op de vraag of de zorgplicht van de bank een dergelijke plicht tot monitoring ter preventie van fraude met zich brengt.

6.1. Geen wettelijke plicht tot monitoring ter voorkoming van fraude

Allereerst zij opgemerkt dat op banken geen wettelijke plicht rust om transacties te monitoren teneinde fraude te voorkomen. Weliswaar rust op banken uit hoofde van artikel 2 van de Regulatory Technical Standards[60] (RTS) een wettelijke plicht om te beschikken over mechanismen voor het monitoren van transacties, maar dit betreft een analyse van reeds gedane betalingstransacties.[61] Een post-transactiemonitoringsplicht dus en geen monitoringsplicht die strekt tot het voorkomen van fraude op voorhand.

Ook de plicht voor banken ingevolge de Wwft om ongebruikelijke transacties te identificeren en deze op grond van artikel 16 Wwft te melden bij de FIU, brengt geen monitoringsplicht met zich om transacties te monitoren om fraude te voorkomen. De reikwijdte van deze monitoringsplicht is immers beperkt tot het detecteren van transacties die mogelijk verband houden met de specifieke economische delicten van witwassen en financiering van terrorisme. De verplichting onder de Wwft strekt zich dus niet uit tot het detecteren van fraude of afwijkende transactiepatronen in algemene zin.

In dit kader wordt in het procesdebat door klanten ook regelmatig verwezen naar de poortwachtersrol die op banken rust, op grond waarvan van banken wordt verwacht dat zij witwassen en terrorismefinanciering tegengaan. Los van het feit dat een vordering jegens de bank op grond van de Wwft tevens afstuit op het relativiteitsvereiste[62], is in jurisprudentie bevestigd dat de poortwachtersrol van de bank geen algemene fraudepreventieplicht behelst:

> *"Banken vervullen in algemene zin een rol als poortwachter vanwege hun centrale positie in het betalingsverkeer en de dienstverlening ter zake, omdat zij op die gebieden bij uitstek deskundig zijn en ter zake beschikken over informatie die anderen missen.* ***Die rol houdt geen algemene wettelijke taak in tot bestrijding van alle vormen van fraude."***[63]

Verder geldt dat de regels ingevolge de integere en beheerste bedrijfsvoering voor een bank op grond van artikel 3:10 en 3:17 Wft jo. art. 10 en 14 Bpr Wft geen transactiemonitoringsplicht voor het tegengaan van fraude met zich brengen. Deze bepalingen schrijven weliswaar voor dat een bank – onder andere – dient te beschikken over effectieve procedu-

59. Geschillencommissie 11 december 2023, nr. 2023-0934.
60. Gedelegeerde verordening (EU) 2018/389 van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden (hierna: 'RTS').
61. Artikel 2 lid 2 RTS.
62. Rb. Amsterdam 9 mei 2018 (ECLI:NL:RBAMS:2018:2985 (*Chiron/ING*), r.o. 4.2.; Zie ook Rb. Amsterdam 9 mei 2018, ECLI:NL:RBAMS:2018:2984 (*Eiser/ABN Amro*), r.o. 4.5, 4.6, Rb. Amsterdam 1 april 2020, ECLI:NL:ECLI:NL:RBAMS:2020:2083, *JOR* 2021/3, m.nt. K. Frielink, r.o. 3.3, 4.7 en Rb. Amsterdam 12 mei 2021, ECLI:NL:RBAMS:2021:1805, r.o. 4.6.
63. Rb. Amsterdam 4 april 2024, ECLI:NL:RBAMS:2024:1948, r.o. 4.2.

res en maatregelen voor het analyseren van klantgegevens, maar deze maatregelen dienen ter bescherming van het vertrouwen in de financiële onderneming, de financiële markten en het bancaire bedrijf.[64]
De bedoeling van deze bepalingen is te voorkomen dat het bancaire systeem als geheel schade lijdt. Deze regels hebben niet tot doel om fraude te ontdekken die (toevallig ook) via een bankrekening plaatsvindt en deze regels verplichten de bank ook niet om (met dat doel) per klant of bankrekening afwijkende en ongebruikelijke transactiepatronen te signaleren.[65]

6.2. Zorgplicht houdt geen algemene monitoringsplicht in

Dan de vraag of de zorgplicht van de bank een monitoringsplicht met zich brengt teneinde fraude te voorkomen. Het is op zichzelf correct dat op banken in hun hoedanigheid als betaaldienstverlener een bijzondere zorgplicht rust. Deze plicht vindt zijn rechtvaardiging in de maatschappelijke rol van banken, die voortkomt uit hun centrale positie binnen het betalingsverkeer.[66] Het is vaste jurisprudentie van de Hoge Raad dat op grond van die zorgplicht van een bank kan worden gevergd dat de bank tot onderzoek overgaat, mits de bank op de hoogte is van ongebruikelijk betalingsverkeer en het daaraan verbonden gevaar.[67] Bepalend hiervoor is datgene waar de bank daadwerkelijk vanaf wist ('subjectieve kennis') en niet waar de bank vanaf behoorde te weten ('objectieve kennis').

De rechtbank Amsterdam over de bijzondere zorgplicht van de bank als betaaldienstverlener en het subjectieve gevaarsbewustzijn vereiste in een uitspraak van maart 2024:

> *"De vorderingen op de Bank houden verband met de bancaire zorgplicht. Op banken rust een bijzondere zorgplicht vanwege hun maatschappelijke functie en omdat zij bij uitstek beschikken over deskundigheid die anderen missen. Hoever die zorgplicht in een specifieke situatie reikt, is afhankelijk van alle omstandigheden van het geval.*
>
> *In dit geval gaat het om de rol van de Bank als betaaldienstverlener, waarbij de Bank erop toeziet dat er op de bij haar aangehouden bankrekeningen geen activiteiten plaatsvinden die een financieel gevaar vormen voor rekeninghouders (zoals [gedaagde 2]) of derden (zoals Zhung Kong). Als de Bank op de hoogte raakt van onregelmatigheden, zal zij tot actie moeten overgaan.* ***Dit wordt het subjectief gevaarsbewustzijn genoemd, wat wil zeggen dat het enkel 'behoren te weten' niet genoeg is om in te moeten grijpen.*** *Voorbeelden zijn de in rechtspraak bekende gevallen van (Ponzi-)zwendel of andere vormen van grove fraude of oplichting."*[68]

De bijzondere zorgplicht van banken behelst echter geen 'algemene monitoringsplicht' om fraude op te sporen. Dit is veelvuldig in de jurisprudentie bevestigd.[69] Van een bank kan – buiten gevallen van wetenschap of serieuze aanwijzingen voor onregelmatigheden – niet worden verlangd dat zij (nader) onderzoek doet naar mogelijke fraude. Het moet gaan om "subjectieve wetenschap" bij de bank van ongebruikelijke activiteiten en van het daaraan verbonden gevaar. Ter illustratie de volgende overweging van de Geschillencommissie van het Kifid:

> *"Gezien hetgeen hiervoor is overwogen, moet de commissie de vraag beantwoorden of de bank nader onderzoek had moeten verrichten naar de overboekingen. Daarbij merkt de commissie op dat zij reeds eerder heeft beslist dat van een bank mag worden verwacht dat zij zich redelijkerwijs inspant om fraude en misbruik van het betalingsverkeer te voorkomen. Naar het oordeel van de commissie kan een dergelijke verplichting echter pas worden aangenomen als voor de bank gegronde redenen aanwezig waren om te twijfelen aan de betaalopdracht.* ***Die verplichting wordt niet lichtvaardig aangenomen.***
>
> ***Een algemene monitoringsverplichting zou immers het proces van geautomatiseerde gegevensverwerking en het maatschappelijk belang dat daarmee gediend is, kunnen schaden****."*[70]

Het voorgaande is uiteraard anders indien de bank – ondanks het ontbreken van de monitoringsplicht – wél op de hoogte is van ongebruikelijke activiteiten op de bankrekening die een vermoeden van fraude oproepen (en er dus sprake is van subjectieve wetenschap). In dat geval kan van de bank worden verwacht dat zij tot onderzoek overgaat.[71]

Van belang in dit kader is ook dat de bank op grond

64. Staatsblad 2006, nr. 519, p. 107
65. Rechtbank Amsterdam 4 april 2024, ECLI:NL:RBAMS:2024:1948.
66. HR 27 november 2015, ECLI:NL:HR:2015:3399, *NJ* 2016/245, m.nt. Tjong Tjin Tai (*ABN Amro/Van den Berg*), r.o. 4.3.
67. HR 23 december 2005, ECLI:NL:HR:2005:AU3713 (*Safe Haven*) en HR 27 november 2015, ECLI:NL:HR:2015: 3399 (*ABN AMRO/ Van den Berg*).
68. Rb. Amsterdam 6 maart 2024, ECLI:NL:RBAMS:2024:1324, r.o. 4.11.
69. Rb. Amsterdam 18 november 2015, ECLI:NL:RBAMS:2015:9493, r.o. 4.4; Rb. Amsterdam 9 mei 2018, ECLI:NL:RBAMS:2018:2984, r.o. 4.4; Rb. Amsterdam 9 mei 2018, ECLI:NL:RBAMS:2018:2985, r.o. 4.6; Rb. Amsterdam 13 juli 2018, ECLI:NL:RBAMS:2018:4656, r.o. 8; Rb. Amsterdam 12 mei 2021, ECLI:NL:RBAMS:2021:1805, 4.6; Rb. Amsterdam 27 juli 2022, ECLI:NL:RBAMS:2022:4066 (*de Tinder Swindler*), r.o. 4.7; Rb. Amsterdam 13 juli 2022, ECLI:NL:RBAMS:2022:4357, r.o. 4.8; Rb. Amsterdam
70. Zie bijvoorbeeld: Geschillencommissie Kifid d.d. 3 maart 2022 (2022-0172), ro.3.8.
71. GC Kifid 2019-759.

van artikel 7:533 lid 4 BW verplicht is de door een klant geaccordeerde betalingen uit te voeren. In diverse uitspraken is bevestigd dat de rol van de bank jegens de consument als betaaldienstverlener in beginsel beperkt is tot het optimaliseren van het betalingsverkeer op de rekening van de consument.[72] De bank kan in haar rol van betaaldienstverlener geen verwijt worden gemaakt voor het uitvoeren van de betalingen zonder nadere monitoring. Een algemene monitoringsverplichting zou het proces van geautomatiseerde gegevensverwerking en het maatschappelijk belang dat daarmee gediend is, kunnen schaden.[73]

7. Vrijwillige vergoeding: coulance

Zoals hiervoor uiteengezet betekent het feit dat een betalingstransactie juridisch kwalificeert als 'toegestaan' niet altijd dat een betalingstransactie ook overeenstemt met de wil van de klant die met deze betalingstransactie heeft ingestemd. Wanneer een klant middels spoofing is misleid is er juridisch sprake van instemming, maar in feite heeft de klant deze transactie niet willen accorderen.

Voor deze gevallen heeft de NVB in 2021 een coulanceregeling opgesteld teneinde schade vrijwillig te vergoeden wanneer rekeninghouders juridisch geen aanspraak maken op het wettelijke vergoeding van geleden schade omdat sprake is van een toegestane betalingstransactie. Aanleiding voor de coulanceregeling waren vragen van de SP, die resulteerden in een Tweede Kamerbrief van de minister van Financiën van 18 december 2020.[74]

Uit deze Kamerbrief volgt dat met de vier grootbanken (ABN AMRO, ING, Rabobank en Volksbank) afspraken zijn gemaakt omtrent een minimum afwegingskader bij spoofing. Het NVB-coulancebeleid is derhalve beperkt tot spoofing fraude. De minister van Financiën merkt op dat bij deze vorm van fraude toegestane betalingstransacties betreft, waarbij op een bank geen wettelijke plicht rust om tot terugbetaling over te gaan tenzij sprake is van grove nalatigheid door de klant.

Dit heeft geresulteerd in een door de NVB op 2 juni 2021 gepubliceerd toetsingskader. Het toetsingskader bestaat uit de volgende vier criteria:

1. Dat het slachtoffer aangifte heeft gedaan van spoofing;
2. Dat er sprake is geweest van spoofing van naam en/of het telefoonnummer van de eigen bank;
3. Dat het slachtoffer enige vorm van bewijs aandraagt dat er spoofing heeft plaatsgevonden; en
4. Dat het slachtoffer een niet-zakelijke klant is (en de fraude heeft plaatsgevonden op een particulier rekeningnummer).

Het uitgangspunt is dat slachtoffers 100% van de schade uit coulance vergoed krijgen tenzij het slachtoffer medeplichtig is aan fraude, al eerder een vergoeding heeft gehad bij dezelfde bank of als het slachtoffer onvoldoende meewerkt aan het fraudeonderzoek van de bank. Overigens zijn dit geen harde criteria, hetgeen ook blijkt uit het persbericht van de NVB.[75]

Indien een klant niet voldoet aan deze criteria komt de klant in beginsel niet voor vergoeding uit coulance in aanmerking. Overigens geldt dat coulance niet rechtens afdwingbaar is. Dit is door zowel het Kifid als de civiele rechter bevestigd.[76] De Geschillencommissie van het Kifid:

> *"De Commissie merkt op dat Consument zijn klacht heeft ingediend naar aanleiding van een tegemoetkoming van de Bank aan zijn neef. Dat de Bank de neef van Consument uit coulance is tegemoetgekomen, leidt op zichzelf niet tot het oordeel dat de Bank daartoe ook jegens Consument verplicht zou zijn. Een dergelijke vordering van Consument komt neer op een verzoek om coulance aan de Bank.* ***Een tegemoetkoming uit coulance is niet juridisch afdwingbaar.***"[77]

Een besluit van de bank om niet over te gaan tot coulance kan derhalve niet (succesvol) aan de rechter ter toetsing worden voorgelegd.

8. Korte blik vooruit: PSD3/PSR

Dan tot slot een korte vooruitblik. De Europese Commissie heeft in 2021 en 2022 PSD2 geëvalueerd en geconcludeerd dat PSD2 met betrekking tot veel van de doelstellingen ervan grotendeels succesvol is geweest, maar ook dat de doelstellingen van PSD2 op bepaalde gebieden niet volledig zijn verwezenlijkt. In de evaluatie is onder meer vastgesteld dat de toename van nieuwe vormen van fraude een punt van zorg is.[78] Na deze evaluatie presenteerde de Europese Commissie op 28 juni 2023 voorstellen voor een

72. Geschillencommissie Kifid 26 juli 2019, nr. 2019-531.
73. Geschillencommissie Kifid 2 oktober 2019, nr. 2019-759 onder 4.3
74. TK, 2020–2021, 32 545, nr. 128.
75. www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing/
76. Geschillencommissie Financiële Dienstverlening d.d. 9 september 2019 nr. 2019-659, r.o. 4.8 en Rb Midden-Nederland, 18 maart 2020, ECLI:NL:RBMNE:2020:986, r.o. 4.9.
77. Geschillencommissie Financiële Dienstverlening d.d. 4 augustus 2016 nr. 2016-350, r.o. 4.1.
78. Preambule 3 PSR.

nieuwe richtlijn[79] (PSD3) en een verordening[80] (Payment Service Regulation, PSR).

In het kader van dit artikel licht ik één belangrijke wijziging in het aansprakelijkheidsregime uit die PSR/PSD3 met zich brengt. Dit betreft een nieuw wetsartikel in de PSR dat de aansprakelijkheid van de bank uitbreidt door een wettelijke terugbetalingsplicht voor de betaaldienstverlener te introduceren bij toegestane betalingstransacties die het gevolg zijn van 'impersonatiefraude' (lees: spoofingfraude/helpdeskfraude). Dit artikel luidt als volgt:

> *"Wanneer een betalingsdienstgebruiker die consument is, onrechtmatig is gemanipuleerd door een derde partij die zich uitgeeft voor een werknemer van de betalingsdienstaanbieder van de consument door de naam, het e-mailadres of het telefoonnummer van die betalingsdienstaanbieder onrechtmatig te gebruiken, en die manipulatie aanleiding heeft gegeven tot daaropvolgende frauduleuze toegestane betalingstransacties, betaalt de betalingsdienstaanbieder de consument het volledige bedrag van de frauduleuze toegestane betalingstransactie terug, op voorwaarde dat de consument de fraude onverwijld aan de politie heeft gemeld en zijn betalingsdienstaanbieder daarvan in kennis heeft gesteld. "*[81]

Preambule 79 van de PSR vermeldt dat het feit dat met de komst van artikel 59 PSR het niet langer mogelijk is om terugbetaling te beperken tot niet-toegestane betalingstransacties, maar noemt een 'systematisch terugbetalingsrecht' voor betaaldienstverleners 'onevenredig en financieel zeer duur'. Ook noemt de preambule van de PSR het morele risico dat een dergelijk systematisch terugbetalingsrecht met zich zou brengen alsmede het mogelijke ongewenste effect dat dit de waakzaamheid van klanten verminderd. [82]

In de literatuur wordt opgemerkt dat artikel 59 PSR veel gelijkenissen vertoont met de NVB-toetsingscriteria voor coulance bij schade door bank helpdeskfraude. Van Sie en Hellegers verwachten daarom dat deze uitbreiding van de aansprakelijkheidsregeling onder PSD3/PSR in Nederland niet tot grote verandering zal leiden.[83] Dit is gezien de overeenkomst tussen de NVB toetsingscriteria en de tekst van artikel 59 PSR een begrijpelijke opmerking, maar mogelijk brengt dit nieuwe artikel wel een verandering voor betaaldienstverleners die niet zijn aangesloten bij de NVB.

Of de introductie van deze additionele terugbetalingsplicht van de bank in aanvulling op de reeds vergaande aansprakelijkheid van betaaldienstverleners in het PSD-aansprakelijkheidsregime daadwekelijk zal leiden tot een verandering in de praktijk – de gewenste nadere bescherming van consumenten bij spoofingfraude[84] – zal blijken uit de casuïstiek wanneer PSD3 en de PSR naar verwachting eind 2026[85] in werking zullen treden.

79. Voorstel voor een Richtlijn van de Europese Unie en de Raad betreffende betalingsdiensten en elektronische gelddiensten in de interne markt, houdende wijzing van richtlijn 98/26/EG en houdende intrekking van de richtlijn (EU) 2015/2366 en Richtlijn 2009/110/EG, COM(2023) 366 final.
80. Voorstel voor een verordening van het van het Europees parlement en de Raad betreffende betalingsdiensten in de interne markt en houdende wijziging van Verordening (EU) nr. 1093/2010, COM(2023) 367 final.
81. Artikel 59 PSR.
82. Preambule 79 PSR.
83. D.W.Y. Sie en D.P.C.M. Hellegers in *Contracteren,* "Fraude in het betalingsverkeer: invloed van de mate van nalatigheid op de verdeling van de schade tussen de betaaldienstgebruiker en de betaaldienstverlener in het licht van artikel 169 VWEU" (2024) nr. 2.
84. Preambule 85 PSR.
85. Tweede Kamer, vergaderjaar 2022–2023, 22 112, nr. 3763, p. 15.