

FinTech, BigTech en de antiwitwaswetgeving

prof. dr. E.P.M. Joosen¹

In dit artikel ga ik in op de antiwitwaswetgeving vanuit het perspectief van de FinTech en BigTech bedrijven die rollen vervullen in het aanbieden van betaalproposities aan cliënten. Vaak zijn dergelijke ondernemingen in de opstartfase vrijgesteld van het financiële toezicht. Maar dat is niet het geval voor de regels van de Wwft, Sanctiewet 1977 of de Europese Verordening betreffende counter-terrorisme van 2011. Ik ga in op de moeilijk leesbare relatie tussen de bepalingen van de anti-witwasregelgeving en die van het financieel toezicht. Ik wijs ook op de onvolkomenheden van het systeem van Europese Paspoorten voor de betaaldienstverleners en elektronischgeldinstellingen, waarbij ik kritisch ben over de weg van de minste weerstand die op dit vlak door de BigTechs lijkt te worden gevolgd. Over welke mogelijkheden tot ingrijpen beschikken de Nederlandse autoriteiten op dit vlak? Die zijn, zoals ik zal bespreken, gering en een en ander kan als zorgelijk worden aangemerkt.

1. Inleiding

De laatste tijd staat de naleving van de wetgeving ter bestrijding van witwassen en financiering van terrorisme door, met name, in Nederland en in de Europees Economische Ruimte (hierna: EER) gevestigde banken en verzekeraars volop in de belangstelling. De zeer omvangrijke schikking die ING Bank met het Openbaar Ministerie is aangegaan en de daarop volgende berichten over de kritiek van De Nederlandsche Bank N.V. (hierna: DNB) op de naleving van de voorschriften van de Wet ter voorkoming van witwassen en financieren terrorisme² (hierna: Wwft) door enkele in Nederland gevestigde banken en verzekeraars wekken de indruk dat de problematiek zich voornamelijk afspeelt in deze onderdelen van de financiële sector.

De Wwft is echter van toepassing op een zeer grote groep ondernemingen en organisaties³, zowel binnen als buiten de financiële sector. Ik leg de focus in dit artikel op die ondernemingen, niet zijnde banken en verzekeraars, die door hun betrokkenheid bij het betalingsverkeer evenzeer te maken hebben met de naleving van de voorschriften van de Wwft of de equivalente

regelgeving die in andere lidstaten van de EER is vastgesteld op basis van de Vierde Witwasrichtlijn⁴ zoals gewijzigd door de Vijfde Witwasrichtlijn⁵ en de Zesde Witwasrichtlijn⁶.

Ik behandel in dit verband de problematiek vanuit het perspectief van betaalinstanties en elektronisch geldinstellingen. Deze soort financiële ondernemingen is vaak actief met producten en diensten in het betalingsverkeer als aanvulling op of ter vervanging van de proposities die banken op dit vlak aanbieden. Het is het werkkterrein van de FinTech ondernemingen die beogen nieuwe of verbeterde toegevoegde waarde te bieden aan de afnemers van betaalproducten en betaaldiensten.

1. Prof. dr. Bart Joosen is bijzonder hoogleraar Financieel Recht aan de Vrije Universiteit en verbonden aan het Zuidas Instituut voor Financieel recht en Ondernemingsrecht (ZIFO), advocaat te Amsterdam en lid van de redactie van het Tijdschrift voor Financieel Recht.

2. Wet van 15 juli 2008, houdende samenvoeging van de Wet identificatie bij dienstverlening en de Wet melding ongebruikelijke transacties, *Stb.* 2008, 303.

3. En met nadruk kan worden gezegd, alle gevallen waarin de samenleving sprake is van transacties waarmee (omvangrijke) sommen contant geld gemoed zijn.

4. Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie, *PbEU* L 141 van 5 juni 2015.

5. Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (Voor de EER relevante tekst), *PbEU* L 156 van 19 juni 2018.

6. Richtlijn (EU) 2019/2177 van het Europees Parlement en de Raad van 18 december 2019 tot wijziging van Richtlijn 2009/138/EG betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II), Richtlijn 2014/65/EU betreffende markten voor financiële instrumenten, en van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, *PbEU* L 334 van 27 december 2019.

Maar ook de BigTech spelers, zoals Facebook, Google en Apple hebben op dit vlak ambities.⁷ In dit artikel ga ik in op de knelpunten die de toepassing van de anti-witwasregelgeving voor FinTechs en BigTechs opleveren. Ik bespreek de definitie van Wwft-instellingen en ga daarbij in op de vraag in hoeverre bijvoorbeeld een betaalinstelling met vrijstelling desondanks aan de Wwft is onderworpen. Ik besteed daarna aandacht aan het toezicht op in Nederland gevestigde Wwft-instellingen en de mate waarin FinTech of BigTech bedrijven aan dit toezicht zijn blootgesteld. Ik verdiep me verder in het systeem van het Europees paspoort voor betaalinstellingen en elektronischgeldinstellingen, waarbij ik een kritische noot plaats bij dit systeem vanuit het perspectief van effectief toezicht in het kader van de witwasregelgeving. Het artikel sluit ik af met enkele opmerkingen over de vraag of er op het vlak van de toepassing en naleving van de anti-witwasregelgeving wel een level playing field bestaat voor banken, FinTechs en BigTechs.

2. Knelpunten in de toepassing van de anti-witwasregels

FinTechs en BigTechs lopen vaak aan tegen de beperkingen van de witwasregeling om tot een optimalisering van de door deze onderneming ontworpen nieuwe betaalproposities te kunnen komen. Niet zelden is het gedachtengoed van deze ondernemingen gebaseerd op een wens om bij het betalingsverkeer de monopolypositie van banken te kunnen doorbreken. Zou het bijvoorbeeld niet geweldig zijn als je met zijn allen in het café staat te borrelen, ter plekke een betaalapp op je Smartphone kunt downloaden en meteen met elkaar de rekening te kunnen delen zodanig dat iedereen binnen een seconde zijn aandeel uitbetaalt of betaald krijgt? En het liefste zonder dat een en ander verloopt via de betaalinfrastructuur van de banken, omdat de baten van dergelijke proposities dan zouden moeten worden gedeeld met de exploitanten van die betaalinfrastructuur. Dat een dergelijke propositie vaak niet (onmiddellijk) kan en zal voldoen aan de Wwft-eisen om nieuwe cliënten te identificeren en hun identiteit te verifiëren (het 'cliëntenonderzoek')⁸ wordt bij de ontwikkeling van de plannen in de praktijk door FinTechs vaak over het hoofd gezien

en leidt dan vervolgens tot grote problemen bij de doorontwikkeling van dergelijke betaalmethoden. Want zou nog gezegd kunnen worden dat bij een relatief 'onschuldige' transactie in de sfeer van consumptie van levensmiddelen, het niet ontoelaatbaar zou zijn om het cliëntenonderzoek af te ronden nadat de zakelijke relatie is aangegaan en de 'eerste' transactie is aangegaan⁹, de nieuwe cliënt (de groep cafébezoekers in mijn voorbeeld¹⁰), zal spoedig na die eerste transactie alsnog door de molen van het cliëntenonderzoek moeten gaan wil de aanbieder van de betaalapp zijn innovatieve betaalproduct verder kunnen exploiteren bij de nieuwe cliënten (dat wil zeggen, meer en andere soorten betaaltransacties doen verlopen via de betaalapp).

Een ander knelpunt vanuit het perspectief van de witwasregelgeving betreft de grootschalige en laagdrempelige (vaak of uitsluitend online) werving van nieuwe deelnemers aan propositities die met betalingsverkeer niets van doen hebben. Als dan aan diezelfde groep gebruikers 'gereguleerde' betaalproposities worden aangeboden, zullen de gebruikers door de molen van het cliëntenonderzoek moeten gaan. Indien bijvoorbeeld de exploitant van een social media-platform de gebruikers in staat wil stellen, via de App, betalingen aan elkaar of aan derden te doen verrichten, kan dat leiden tot het uitgeven of distribueren van elektronisch geld of het aanbieden van een van de in Bijlage I bij PSD2¹¹ genoemde betaaldiensten. Dit is een probleem waar BigTechs ongetwijfeld mee te kampen hebben. Waar het BigTechs vooral te doen is om het werven van zoveel als mogelijk gebruikers zonder dat het enige moeite kost voor die gebruikers om zich aan te sluiten en de toetredingsdrempel zo laag als mogelijk wordt gehouden, zal de bruikbaarheid van de databases met informatie over die gebruikers in het kader van het aanbieden van betaaldiensten of het uitgeven en verwerken van elektronisch geld gering zijn. Gebruikers met hun 'micky.mouse@gmail.com' of 'rene.kerkh88@icloud.com' accounts zullen deugdelijk moeten worden geverifieerd, en omdat het om online onboarding gaat, geldt in zijn aard bovendien een 'verscherpt cliëntenonderzoek'¹².

Tenslotte leveren de vereisten voor transactiemonitoring zoals geregeld in,

7. Zo is ApplePay inmiddels ook in Nederland gemeengoed geworden en heb ik in 2019 kennisgenomen van de ambities van Facebook om met LIBRA een 'eigen' virtual currency te lanceren. Zie over het laatste initiatief: Dirk A. Zetsche, Ross P. Buckley en Douglas W. Arner, 'Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses', European Banking Institute Working Paper Series 2019/44, raadpleegbaar via papers.ssrn.com, referentie 3414401.

8. Zie: art. 3 e.v. Wwft.

9. Zie: art. 4(2) Wwft.

10. Aannemende dat iedere cafébezoeker na het eerste gebruik van de betaal App uiteraard er nog verder gebruik van wil maken.

11. Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG, PbEU L. 182.

12. Zie: art. 8(1)(a) Wwft en Bijlage III Richtlijn (EU) 2015/849, paragraaf 2(c): 'zakelijke relaties op afstand of transacties op afstand, zonder sommige garanties, zoals elektronische handtekeningen'.

onder meer¹³, art. 15 e.v. Wwft, in de praktijk vaak knelpunten op. Dat heeft verschillende achtergronden.

Ten eerste rust de Wwft de verplichting tot transactiemonitoring in beginsel op iedere 'instelling' zoals bedoeld in art. 1(1) Wwft, waaronder betaalinstanties die één van de betaaldiensten bedoeld in Bijlage I van PSD2 verrichten, betaaldienstagenten en elektronischgeldinstellingen. Bijvoorbeeld betaaldienstverleners die de betaalinitiatiedienst verlenen zijn niet, per definitie, uitgezonderd van de verplichtingen van art. 15 Wwft. Dat betekent dat in de voorbereidende werkzaamheden voor het initiëren van de betaaltransactie, transactiemonitoring dient plaats te vinden, terwijl bij de uitvoering van die betaaltransactie (geïnitieerd door de PSP¹⁴ die de betaalinitiatiedienst verleent) door de rekeninghoudende betalingsdienaar¹⁵ eveneens transactiemonitoring dient plaats te vinden. Mag de door de ene partij in de betaalketen uitgevoerde transactiemonitoring, de invulling van dezelfde verplichting door een andere partij vervangen? Ik meen dat daarvoor geen duidelijke aanknopingspunten bestaan, en ga er van uit dat iedere PSP in de keten zelfstandig verantwoordelijk is voor transactiemonitoring.

Ten tweede geldt, dat veel van de proposities van FinTechs en wellicht ook BigTechs een snelle transactieverwerking beloven. Vaak zijn proposities gebaseerd op een verwerking van betaaltransacties 'real time', dat wil zeggen de betaler zal bij de uitvoering van de transactie onmiddellijk worden gedebiteerd, terwijl de begunstigde van de transactie onmiddellijk wordt gecrediteerd. Hoezeer dergelijke proposities in de Nederlandse markt met de invoering in 2019 van de 'instant payment' routines door de banken¹⁶ niet veel toegevoegde waarde zullen hebben, blijft voor andere markten waarin dergelijke 'near real time'¹⁷ transactieverwerking routines nog niet zijn ingevoerd een propositie die versnelling van transactieverwerking belooft uiteraard interessant.

Transactiemonitoring uitvoeren in omstandigheden van een snel transactieverloop

is uiterst ingewikkeld en uiterst kostbaar.¹⁸ FinTechs zullen met de beperkte budgetten die zij vaak ter beschikking hebben onvoldoende mogelijkheden hebben om te investeren in de noodzakelijke compliance organisatie en vaak daarbij noodzakelijkerwijs toe te passen (extreem) kostbare technologie.¹⁹ Desondanks, zullen ook dergelijke ondernemingen onderworpen zijn aan de desbetreffende regels, ook wanneer zij een 'real time' betalingsverwerking in het vooruitzicht stellen.²⁰

13. In aanvulling hierop gelden voorts de regels van de Sanctiewet 1977, die eveneens binnen het systeem van transactiemonitoring moeten worden ingepast, en die in hun aard zelfs vereisen dat instellingen in staat zijn om transacties die mogelijk leiden tot een inbreuk op de regels, tegen te houden, en eventuele daarmee gemoeide gelden of andere activa te 'bevriezen'.

14. Payment Services Provider, een onderneming die een of meer van de betaaldiensten verleent als omschreven in Bijlage I PSD2.

15. Zie de definitie van art. 4(17) PSD2.

16. Zie www.betalvereniging.nl/zoeken/instant+payments.

17. De Nederlandse banken committeerden zich aan een verwerking van de betaaltransactie binnen 5 seconden.

18. Zie voor een overzichtartikel op dit vlak: Henry Balani, 'What faster payments means for anti-money laundering compliance', *Journal of Financial Compliance*, Vol. 1, No. 3 2017, p. 245–254.

19. Mij is in de praktijk een geval bekend van een aspirant elektronischgeldinstelling die een alternatieve wijze van betalen wilde introduceren gebaseerd op de verwerking van elektronisch geld transacties. Deze verwerking diende real time te gebeuren. Dat betekende dat de transactiemonitoring eveneens real time diende te geschieden. Dergelijke real time verwerking kan in feite alleen plaatsvinden door gebruik te maken van 'self learning' (artificiële intelligentie) oplossingen. Dit speelde in de tijd dat dergelijke systemen nog niet op de plank lagen van de gespecialiseerde software huizen (zoals tegenwoordig bijvoorbeeld de INFORM proposities van RiskShield uit Duitsland). De uiteindelijke ontwikkeling van een maatwerkoplossing voor deze onderneming heeft vele miljoenen euro's gekost, waar de start up bij het vaststellen van de oorspronkelijke budgetten in het geheel niet op had gerekend.

20. Een en ander vloeit voorts voort uit de op dergelijke ondernemingen rustende regels van PSD2, eenmaal dat deze ondernemingen over een vergunning als betaalinstantie beschikken. Zie het antwoord van EBA of Q&A 2018_4090 op een vraag over deze kwestie: 'Article 2(1) of the Commission Delegated Regulation (EU) 2018/389 (RTS on Strong customer authentication and secure communication) requires that 'Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions' and Article 2(2) refers to 'transaction monitoring mechanisms' for the purpose of the Delegated Regulation. Further, Article 18(1) of the RTS on the transaction risk analysis exemption requires not only for PSPs to have 'transaction monitoring mechanisms referred to in Article 2' in place but also Article 18(2)(c) of the RTS requires PSPs to perform a 'real time risk analysis'. Accordingly, for payments service providers to be able to benefit from the transaction risk analysis exemption under Article 18 of the RTS, they have to go beyond the general monitoring requirements required under Article 2 of these RTS and have mechanisms in place that enable 'real time risk monitoring', in other words a monitoring before the transaction is authorised. The general monitoring mechanism under Article 2 of these RTS does not require enabling 'real time risk monitoring' and is usually carried out 'after' the execution of the payment transaction.'

3. De definitie van Wwft-instellingen

In de praktijk komt het vaak voor, dat startende ondernemingen die zich richten op het ontwikkelen van proposities in het betalingsverkeer, in de aanloop naar de groei van de onderneming tot een zekere omvang gebruik maken van de in artikelen 1a (betaaldienstverleners) of 1d (elektronischgeldinstellingen) Vrijstellingsregeling Wft²¹ opgenomen vrijstelling van vergunningplicht. Dat geeft deze ondernemingen de mogelijkheid om zonder onderworpen te zijn aan de vergunningplicht uit hoofde van de Wet op het financieel toezicht (hierna: Wft) reeds werkzaamheden aan te vangen en de nieuwe propositie aan te bieden. Zijn dergelijke ondernemingen dan ook vrijgesteld van de verplichtingen uit hoofde van de Wwft of de Sanctiewet 1977? Ik meen dat dat niet het geval is, en die visie wordt gedeeld door de toezichthouder.²² Ten eerste moet in dit verband worden genoemd dat de verplichtingen om de Wwft toe te passen gelden voor de 'instellingen' zoals gedefinieerd in art. 1(1) Wwft. De regelingen van de Sanctiewet 1977 richten zich in beginsel tot eenieder in Nederland²³, en toepassing van die wet is niet afhankelijk van het type onderneming of activiteit die wordt verricht. Wat naar mijn mening hier verwarrend is, is de regeling van art. 10, tweede lid Sanctiewet 1977. Hierin is de competentieregeling gegeven voor het toezicht op de naleving van de Sanctiewet 1977, waarbij DNB en AFM krachtens de Ministeriële regeling van 2002²⁴ zijn aangewezen als toezichthouders voor de in art. 10, tweede lid genoemde 'financiële ondernemingen'. In de tekst van die bepaling wordt, bijvoorbeeld in (j) en (k) gerefereerd aan 'financiële ondernemingen die ingevolge de Wet op het financieel toezicht in Nederland het bedrijf van elektronisch geldinstelling respectievelijk betaaldienstverlener mogen uitoefenen.' Maar dat geldt op zijn minst ook voor de desbetreffende ondernemingen, voor zover zij krachtens de Wft van toepassing van de vergunningplicht zijn vrijgesteld.

De Sanctiewet 1977 geldt om die reden, mijns inziens, zowel voor vergunninghoudende als op grond van de Vrijstellingsregeling Wft vrijgestelde betaalinstanties en elektronischgeldinstellingen. Getwijfeld kan

worden of dat ook geldt voor ondernemingen die krachtens art. 1:5a Wft van de toepassing van de Wft zijn uitgezonderd. Dergelijke ondernemingen worden niet geacht (op grond van de redactie van art. 1:5a Wft) 'betaaldiensten' te verlenen, waardoor ook niet wordt toegekomen aan toepassing van de regels van de Wft, zoals de bepalingen die de vergunningplicht van betaaldienstverleners of elektronischgeldinstellingen regelen. Er hoeven in dat geval geen werkzaamheden van de onderneming te worden vergund, en vrijstelling van bepalingen van de Wft is evenmin aan de orde. De Sanctiewet 1977 richt zich echter tot 'eenieder', wat de kwalificatie van die onderneming dan ook is. Via die uitgebreide reikwijdte van de Sanctiewet 1977, kom ik tot de conclusie dat die regelgeving ook voor op grond van art. 1:5a Wft uitgezonderde ondernemingen geldt. Dat is eveneens het geval voor de hierna nog te noemen Counter-Terrorisme Verordening.

Betaalinstanties en betaaldienstagenten (niet zijnde banken of financiële instanties die van oudsher in art. 1 Wwft als 'instelling' zijn gedefinieerd) zijn als 'Wwft-instelling' aan de in art. 1 Wwft opgenomen opsomming toegevoegd bij gelegenheid van de implementatie van de eerste richtlijn betaaldiensten in 2009.²⁵ De definitie 'betaalinstelling' is tegenwoordig opgenomen in de beschrijving van 'financiële ondernemingen' in art. 1a(3)(b) Wwft als:

'degenen die, geen bank zijnde, in hoofdzaak hun bedrijf maken van het verrichten van betaaldiensten als bedoeld in bijlage I bij de richtlijn betaaldiensten'.

Hieruit vloeit voort dat de onderneming die een of meer van de betaaldiensten als opgenomen in Bijlage I PSD2 feitelijk verleent, als een Wwft-instelling zal kwalificeren, door de verwijzing in de definitie 'instelling' in art. 1(1) Wwft naar financiële onderneming en de eigen definitie van 'financiële onderneming' in art. 1a(3)(b) Wwft. Niet is bepaald dat het moet gaan om ondernemingen die beschikken over een vergunning zoals verleend op grond van art. 2:3a Wft. Een zuivere lezing van de bepalingen van de Wwft brengt aldus met zich mee dat ondernemingen aan de toepassing van die wet zijn onderworpen, voorzover zij zich in feitelijke zin bezig houden met de verlening van één of meer van de betaaldiensten van Bijlage I PSD2. Dat geldt ook indien krachtens art. 1:5a Wft de verlening van de betaaldiensten niet als 'betaaldienst' in de zin van de Wft moet worden aangemerkt, of wanneer

21. *Stcrt.* 2006, 229.

22. Zie DNB Factsheet 'Vrijstelling Vergunningplicht' referentie 01950 van 19 februari 2019: 'DNB benadrukt ook dat een vrijgestelde betaaldienstverlener binnen de reikwijdte van de Wet ter voorkoming van witwassen en het financieren van terrorisme (Wwft) valt. Dit brengt onder meer met zich mee dat een vrijgestelde betaaldienstverlener ongebruikelijke transacties moet melden bij de Financiële Inlichtingen Eenheid (FIU-NL) en cliëntenonderzoek moet uitvoeren.'

23. Zie ook DNB Leidraad Wwft en Sw, versie december 2019, op p. 4: 'Een ieder in Nederland heeft zich te houden aan de Sw.'

24. Regeling van 5 juni 2002, *Stcrt.* 2002, 106.

25. *Kamerstukken II* 2008/09, 31892, Wijziging van de Wet op het financieel toezicht, het Burgerlijk Wetboek en de Wet inzake geldtransactiekantoren en intrekking van de Wet op het grensoverschrijdend betalingsverkeer ter implementatie van richtlijn nr. 2007/64/EG van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt en tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG (*PbeuL* 319).

de desbetreffende onderneming gedurende een bepaalde periode gebruik kan maken van de vrijstelling van vergunningplicht zoals geregeld in art. 1a Vrijstellingsregeling Wft.

Dat van de toepassing van de Wft op grond van art. 1:5a Wft uitgezonderde betaaldienstverleners, desondanks aan de Wwft zijn onderworpen, vloeit mijns inziens, *ten eerste*, voort uit de definitie van ‘elektronischgeldinstelling’ van art. 1a(3)(e) Wwft, waar de Wwft van toepassing wordt verklaard voor zover deze onderneming andere transacties verricht dan bedoeld in art. 1:5a, tweede lid, onderdeel k Wft. Dus indien door de elektronischgeldinstelling één van de uitzonderingen van art. 1:5a, tweede lid, onderdelen (a) tot en met (o) Wft (met uitzondering van (k)) wordt toegepast, zal de elektronischgeldinstelling wel aan de Wwft zijn onderworpen. A fortiori geldt dat dus voor op grond van art. 1:5a Wft uitgezonderde betaaldienstverleners, ook wanneer deze betrokken zijn bij de handelingen zoals beschreven in art. 1:5a(2)(k) Wft. *Ten tweede* vloeit dit voort uit het hierna te bespreken regime voor betaaldienstagenten.

De Wwft kent dus een ruimer toepassingsbereik dan de Wft omdat ondernemingen die zijn uitgezonderd van de Wft-bepalingen of daarvan zijn vrijgesteld, desondanks aan de bepalingen de Wwft zijn onderworpen. Deze lezing van de bepalingen van de Wwft wordt vaak over het hoofd gezien. Niet zelden verkeren startende ondernemingen in de sfeer van de betaaldienstverlening in de veronderstelling dat wanneer zij zich bijvoorbeeld kunnen beroepen op de vrijstelling van art. 1a Vrijstellingsregeling, dat dat ook betekent dat zij zich niet hoeven te houden aan de Wwft. Minder goed in de materie ingevoerde adviseurs, willen daarbij ook nog wel eens deze vergissing maken, en geven de desbetreffende onderneming dan het verkeerde advies.

Dat leidt vaak tot knelpunten, bijvoorbeeld doordat in de ontwikkeling van het betaalplatform of de geautomatiseerde omgeving waar de nieuwe betaaldienst-propositie wordt opgenomen, geen rekening wordt gehouden met aspecten van cliëntonderzoek of transactiemonitoring. De softwareprogrammering van het platform of het systeem is dan vanaf het begin onvolkomen en moet vaak in de ontwikkelingsfase in een versneld tempo worden bijgesteld om te voorzien in de aanvullende, op grond van de Wwft vereiste processen. A fortiori geldt dit voor de aanvullende processen die noodzakelijk zijn om de Sanctiewet 1977 toe te passen, die niet alleen ‘monitoring’ van transacties veronderstelt, maar ook een reële interventiemogelijkheid in de afwikkeling van lopende transacties die op het platform worden uitgevoerd. Dit punt wordt ook bevestigd door het toepassingsgebied van art. 2 van de counter-terrorisme verordening uit 2011²⁶

(‘Counter-Terrorisme Verordening’) die kort na ‘9-11’ is vastgesteld, en die aansluit bij de feitelijke transacties en niet bij de gereguleerde status van de onderneming die bij die transacties is betrokken.

Dat de Wwft derhalve van toepassing is op ondernemingen die zich bezig houden met de feitelijke toepassing van betaaldiensten zoals omschreven in Bijlage I PSD2, ook al zijn zij uitgezonderd of vrijgesteld van de verplichtingen van de Wft, kan ook worden gebaseerd op het feit dat de per definitie niet vergunningplichtige ‘betaaldienstagenten’, wel als een zelfstandige ‘financiële onderneming’ zijn opgenomen in de definitie van art. 1(3) Wwft. De definitie ‘betaaldienstagent’ luidt:

‘betaaldienstagenten als bedoeld in art. 1:1 van de Wet op het financieel toezicht’.

Betaaldienstagenten zijn ondernemingen die in opdracht van en doorgaans met een volmacht van onder toezicht staande betaaldienstverleners of elektronischgeldinstellingen, als tussenpersoon betrokken zijn bij de verwerking van betaaltransacties of transacties in elektronisch geld. Het is een in de praktijk veel voorkomende wijze van uitoefening van werkzaamheden door ondernemingen die betrokken zijn bij het in circulatie brengen van elektronisch geld of bij de verwerking van betaaltransacties. Daarbij kan bijvoorbeeld worden gedacht aan de dienstverlening door de ondernemingen die zogenaamde ‘geldtransfers’ verrichten (de betaaldienst genoemd in punt 6 van Bijlage I PSD2). Dit is een activiteit waarbij een verscherpt anti-witwastoezicht noodzakelijk is, omdat het een betaalmethode faciliteert waarbij betaler en begunstigde anoniem betaaltransacties kunnen verrichten. Het gaat om de mogelijkheid om met een bedrag in contanten, zonder gebruik te maken van een betaalrekening, een overboeking te doen naar het buitenland, waarbij de begunstigde zich met het unieke nummer dat aan de betaler wordt uitgereikt identificeert bij het lokale kantoor van de geldtransfer dienstverlener. Deze geldtransferdienstverlening wordt in Nederland bijna exclusief aangeboden door betaaldienstverleners met een vergunning verleend door een andere EER-toezichthouder en de Nederlandse kantoren van de geldtransferdienst zijn alle bij de dienstverlening betrokken als betaaldienstagent.

Deze betaaldienstagenten zijn zelfstandig onderworpen aan de vereisten van de Wwft, en zullen derhalve zelfstandig cliëntenonderzoek dienen te verrichten en transactiemonitoring. Zie hiervoor ook de separaat door de Financial Intelligence Unit Nederland (‘FIU-Nederland’) aangelegde ondernemingen-groep voor betaaldienstagenten.²⁷ Het bevestigt mijns inziens,

27 december 2001 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten met het oog op de strijd tegen het terrorisme, *PbEU L* 344 van 28 december 2001.

27. <https://www.fiu-nederland.nl/nl/meldergroep/287>.

26. Verordening (EG) Nr. 2580/2001 van de Raad van

dat de toepassing van de Wwft, de Sanctiewet 1977 en de Counter-Terrorisme Verordening plaats dient te vinden, ook al zijn de desbetreffende ondernemingen niet onderworpen aan de regels van het toezicht uit hoofde van de Wft.

Voor elektronischgeldinstellingen gelden vergelijkbare conclusies. Ook dit type financiële onderneming is vermeld onder (e) in de lijst van ondernemingen van art. 1a, derde lid Wwft. Hiervoor geldt echter, dat de Wwft de uitgezonderde elektronischgeldinstellingen die transacties in elektronisch geld verrichten zoals bedoeld in art. 1:5a, tweede lid onder (k) Wft (bijvoorbeeld elektronisch geld voor het afrekenen van een zeer beperkte goederen en diensten of transacties binnen een beperkt netwerk) uitsluit van de definitie 'instelling' als bedoeld in de Wwft. In zoverre zullen bijvoorbeeld de aanbieders van producten zoals 'giftcards' of andere producten die leunen op de uitzondering van artikelen 1:5 juncto 1:5a, tweede lid onder (k) Wwft, zijn uitgezonderd van de toepassing van de Wwft. Ik sprak hiervoor al twijfel uit of dit ook geldt voor de Sanctiewet 1977 en een vergelijkbaar voorbehoud moeten we maken voor de regels van de Counter-Terrorisme Verordening. Maar een 'vrijgestelde' elektronischgeldinstelling die art. 1d Vrijstellingsregeling Wft kan toepassen valt, mede gezien de expliciete vermelding in art. 1a derde lid onder (e) Wwft van de regeling van art. 1:5a Wft, wel binnen het bereik van de regels van de Wwft en kwalificeert als een 'Wwft-instelling'. Voor zover de elektronischgeldinstelling met vergunning in een van de andere lidstaten van de EER, gebruik maakt van betaaldienstagenten met een vestiging in Nederland, zullen die laatstgenoemde ondernemingen ten volle zijn onderworpen aan de regels van de Wwft. Ook dat is een voor de praktijk zeer belangrijke constatering, omdat op dit moment slechts een handvol elektronischgeldinstellingen zijn gevestigd in Nederland met een vergunning van DNB, maar het aantal Nederlandse betaaldienstagenten die in opdracht en in naam van een in de EER vergunninghoudende elektronischgeldinstelling werkzaamheden verricht, loopt in de vele tientallen ondernemingen. Zij zijn alle aan te merken als Wwft-instelling en zij zijn evenzeer onderworpen aan de Sanctiewet 1977. Dat laatste geldt hoezeer art. 10 van de Sanctiewet 1977 deze ondernemingen niet noemt. We gaan er desondanks van uit dat dat artikel geen reikwijdte bepaling betreft maar een competentieverdeling voor het toezicht op de Sanctiewet 1977. Dat geldt, a fortiori, voor de Counter-Terrorisme Verordening die, zoals gezegd, niet zozeer kijkt naar de 'gereguleerde status' van de betrokken onderneming, maar veeleer naar de feitelijke werkzaamheden, bijvoorbeeld verrichtingen in het betalingsverkeer.

4. Toezicht op in Nederland gevestigde Wwft-instellingen

De kennis over het toezicht op Wwft-instellingen die zijn uitgezonderd of vrijgesteld van de vergunningplicht op grond van de Wft is niet wijdverbreid en berust veelal uitsluitend bij de gespecialiseerde externe adviseurs in de advocatuur. Wat we in de vorige paragrafen signaleerden aan knelpunten in de praktijk wordt naar mijn inzicht ook veroorzaakt door de onduidelijke regels op dit vlak. Zoals we zagen is bijvoorbeeld ten aanzien van de toepassing van de Sanctiewet 1977 volstrekt onduidelijk hoe de reikwijdte van die wet moet worden geïnterpreteerd. En hoezeer de Counter-Terrorisme Verordening zeer belangrijke regelgeving is ter bestrijding van terrorisme financiering, is in de praktijk de kennis over die regelgeving geen gemeengoed.

Het verbaast dan ook niet dat als gevolg van deze onduidelijkheden, ook in de praktijk de nodige misslagen plaatsvinden in de advisering en begeleiding van de nieuwe startende ondernemingen in het FinTech domein. Met enige moeite is nog wel uit te pluizen dat voor bepaalde betaaldiensten of verrichtingen van elektronischgeldinstellingen het bepaalde van de Wft niet van toepassing is (bijvoorbeeld omdat art. 1:5a Wft geldt), of dat er sprake is van een vrijstelling. De relatie van deze regels met het bepaalde in de Wwft, Sanctiewet 1977 of de Counter-Terrorisme Verordening wordt vaak over het hoofd gezien of verkeerd geïnterpreteerd. Vaak is dan het devies van onervaren niet gespecialiseerde adviseurs: 'u bent vrijgesteld van de Wft, en derhalve ook van andere wet- en regelgeving'.

Wat naar mijn inzicht ook bijdraagt aan de onduidelijkheid, betreft het gebrek aan sturing door de toezichthouders op dit vlak. Weliswaar is het tegenwoordig staand beleid van DNB om bij berichtgeving aan vrijgestelde betaalinstanties ook te wijzen op de verplichtingen uit hoofde van de Wwft en er is op de website van DNB ook wel enige duiding over dit onderwerp te vinden.²⁸ Desondanks meen ik dat er hier een verbeterslag zou moeten worden gemaakt. We gaven hiervoor het voorbeeld van de 'betaaldienstagenten' en de expliciete inkadering van die groep ondernemingen op de website van FIU-Nederland. De teksten die FIU-Nederland op zijn website bezigt zijn kristalhelder. Maar wanneer men nu naar de Wft-regelingen kijkt, zal, behoudens de definitie 'betaaldienstagent' in feite nauwelijks enige aanknopng vinden van de compliance verplichtingen voor die categorie ondernemingen en het op hen toepasselijke regime. Wanneer bijvoorbeeld de recente DNB Leidraad Wwft en Sw, versie december 2019 ('Leidraad'), er op wordt nageslagen, ziet men welgeteld één verwijzing naar deze ondernemingen in een opsomming voor welke

28. Zie voetnoot 22 voor de desbetreffende passage.

ondernemingen de ‘geldtransfer-indicator’ van het Uitvoeringsbesluit Wwft 2018 geldt.²⁹ Enige verdere guidance, bijvoorbeeld dat betaaldienstagenten zich dienen te melden bij FIU-Nederland, daar een aansluiting op het rapporteringssysteem dienen te regelen en ongebruikelijke transacties dienen te melden, ontbreekt.

Wie in de Leidraad op zoek gaat naar enige beschouwingen over de toepassing van de Wwftende Sw ten aanzien van vrijgestelde of van de toepassing van de Wft uitgezonderde betaalinstantellingen en elektronischgeldinstellingen, zal op dit vlak bitter weinig teksten terugvinden. Daarin zou naar mijn inzicht een verbeteringslag kunnen worden gemaakt, mede vanwege de complexiteit van het wettelijke systeem en de moeilijk leesbare reikwijdte bepalingen en definities van de Wwft, Sanctiewet 1977 en, het moet worden toegegeven, de Counter-Terrorisme Verordening.

We menen dat wetgever en toezichthouders zich beter zouden moeten inspannen om op dit vlak aan de praktijk duidelijkheid te verschaffen. De doelstelling van de anti-witwasregelgeving is het bestrijden van criminaliteit in de sfeer van vermogensdelicten, fiscale fraude, maar vooral ook de bestrijding van het gebruik van het financiële stelsel voor terroristische motieven, ook dat deel van het stelsel dat om allerlei (proportionaliteits-) overwegingen niet onder financieel toezicht staat. De vrijgestelde of uitgezonderde delen van de financiële sector moeten zich strikt aan de anti-witwasregelgeving houden. Tenslotte doen zich de risico's van misbruik van het financiële stelsel, zeker als het bijvoorbeeld gaat om kwesties als geweldsmisdrijven of terroristische aanslagen, zich voornamelijk voor in het vrijgestelde of uitgezonderde deel van de financiële sector.

‘9-11’, of de terroristische aanslagen in Parijs, Brussel en andere vergelijkbare voorvallen zijn niet gefinancierd door middel van bankoverschrijvingen of transacties in het gereguleerde deel van de financiële sector. Er is meer dan voldoende bekend over het misbruik van de ‘geliberaliseerde’ delen van de financiële sector door personen met kwade bedoelingen. Het is ook dé aanleiding geweest om de Vierde Witwasrichtlijn aan te scherpen met de regels van de Vijfde Witwasrichtlijn, waar, onder meer de geliberaliseerde onderdelen van het toezicht op elektronisch geldtransacties zijn aangescherpt en de drempels van de uitzonderingen van toezicht verlaagd.

5. Toezicht op in de EER gevestigde instellingen

Een ander punt van zorg dat in dit verband moet worden uitgesproken, betreft het stelsel van vergunning en toelating tot de interne

markt in de Europese Unie, van ondernemingen die in één van de EER-lidstaten over een vergunning beschikken. We focussen ons andermaal op de betaaldienstverleners en de elektronischgeldinstellingen. Het beeld dat daar voor mij uit opdoemt is dat BigTech ondernemingen hierbij stelselmatig kiezen voor de strategie van de ‘weg van de minste weerstand’ als het gaat om het toezicht dat op de door hen opgerichte betaalinstantellingen en elektronischgeldinstellingen zal worden gehouden.

Facebook Payments International Limited beschikt over een in Ierland verleende vergunning als betaalinstantelling en elektronischgeldinstelling. Die onderneming heeft vervolgens, gebruik makend van de in PSD2 en de Richtlijn elektronischgeldinstellingen³⁰ (hierna: EGI-Richtlijn) gegeven ‘Europees Paspoort’ faciliteiten, een notificatie gedaan van het voornemen om in Nederland grensoverschrijdende (betaal-)diensten aan te bieden, respectievelijk elektronisch geld te kunnen uitgeven of daarin te kunnen bemiddelen. Ongetwijfeld is een en ander geregeld in het kader van de voorgenomen uitgifte van de ‘LIBRA’.³¹

Hetzelfde geldt Google Payment International Limited met een Ierse vergunning als betaalinstantelling en elektronisch geldinstelling. Daarnaast heeft Google Payment Lithuania UAB een door de Litouwse autoriteiten verleende vergunning als elektronischgeldinstelling en heeft deze vergunning naar Nederland genotificeerd.³² Ook hier gaat het over een notificatie van grensoverschrijdende dienstverrichting in Nederland door een betaalinstantelling uit de EER respectievelijk elektronischgeldinstelling.

Waar we onze mening klaar hebben staan over de toereikendheid van het toezicht in andere EER-lidstaten op banken, na de dure lessen die we hebben getrokken naar aanleiding van bijvoorbeeld het falen van de IJslandse banken en het falende toezicht daarop, is er weinig debat over de mate waarin we moeten kunnen vertrouwen op het stelsel van oversight door de toezichthouder van het thuisland voor andere financiële ondernemingen, zoals betaalinstantellingen en elektronischgeldinstellingen. Nog daargelaten de vraag in welke mate toereikend toezicht wordt gehouden op de naleving van PSD2 of de EGI-Richtlijn, speelt ook nog de mate waarin de desbetreffende buitenlandse toezichthouders effectief zullen toezien op de naleving van de anti-witwasregelgeving. Deze regels dienen,

29. Zie p. 57 linker kolom van de Leidraad.

30. Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (Voor de EER relevante tekst), *PbEU* L 267 van 10 oktober 2009.

31. Zie het DNB register uit hoofde van art. 1:107 Wft.

32. Zie het DNB register.

vanwege hun Europese oorsprong, evenzeer te worden toegepast door de onderneming in het thuisland (ook wat betreft de diensten die op basis van het Europese paspoort worden verleend) en gehandhaafd door de toezichthouder van het thuisland. Dat is in zoverre zorgelijk, omdat, zoals hiervoor gesignaleerd, met name ten aanzien van de BigTechs de ongemakkelijke situatie zal bestaan dat zij een radicaal andere benadering van hun 'gebruikers' zullen moeten volgen wat betreft de identificatie en verificatie van de identiteit van de gebruikers waaraan door deze ondernemingen als cliënt betaaldiensten worden verleend. Zou op dat vlak niet de situatie kunnen ontstaan, dat terwijl de 'reguliere' financiële ondernemingen, zoals banken en verzekeraars momenteel hard worden aangepakt om hun poortwachter functie op orde te krijgen en de transactiemonitoring effectief en nagenoeg waterdicht te laten zijn, er via de alternatieven voor betaaloplossingen die door de BigTechs worden aangeboden of zullen worden aangeboden, grote lekkages zullen of kunnen ontstaan wat betreft participatie in het betalingsverkeer door personen die het oogmerk hebben hun identiteit te verhullen?

Noch PSD2 noch de EGI-Richtlijn staan de toezichthouders van het gastland toe om bij een ontvangen notificatie van grensoverschrijdende dienstverrichting in Nederland door een betaalinstantie uit de EER respectievelijk elektronischgeldinstelling bezwaar te maken tegen de markttoegang van dergelijke elders in de EER gevestigde ondernemingen. En ook al zouden deze ondernemingen kiezen voor een vestiging van een bijkantoor of het gebruik van een betaaldienstagent, dan nog rijst de vraag of de toezichthouder van het gastland een dergelijke vestiging of gebruik zou kunnen tegenhouden, omdat een dergelijke weigering slechts kan worden gebaseerd op 'alle redelijke gronden tot ongerustheid mee wat betreft het witwassen van geld of de financiering van terrorisme', zie bijvoorbeeld art. 28, tweede lid PSD2. De toezichthouder van het land van vestiging van de betaalinstantie kan de door de toezichthouder van het gastland opgeworpen bezwaren echter vrij eenvoudig naast zich neerleggen.

Het is bekend dat als het gaat om de samenwerking tussen de Europese autoriteiten bij het toezicht om de anti-witwasregelgeving, er sprake is van zeer grote coördinatieproblemen en gebreken. Om die reden heeft de Europese Bankautoriteit (hierna: EBA) onlangs de exclusieve bevoegdheid gekregen om op dit vlak toezicht op de 'toezichthouders' te houden.³³

De meeste, zo niet alle, bepalingen van dit nieuwe toezicht- en coördinatieregime, zie bijvoorbeeld art. 9bis van de EBA-Verordening, betreffen zogenaamde 'financiëlesectordeelnemers' wat steeds en consequent is gedefinieerd als onder (prudentieel) toezicht staande financiële ondernemingen, derhalve vergunninghouders. Met moeite kan uit deze bepaling worden afgeleid dat EBA ook bevoegd is in haar werkzaamheden, sturing te geven aan de toepassing van de anti-witwasregelgeving ten aanzien van niet onder toezicht staande ondernemingen, bijvoorbeeld zij die zijn vrijgesteld of uitgezonderd van het toezicht, maar wel betrokken zijn bij de verlening van betaaldiensten, of de uitgifte en distributie van elektronisch geld.

6. Slotopmerkingen

De naleving van de anti-witwasregelgeving door de Nederlandse en Europese banken en verzekeraars is onderwerp van een stevig debat in de samenleving. De ongemakkelijke verhouding die de banken hebben met de samenleving en de politiek, leidt dan vaak tot, wat mij betreft, eenzijdig uitgebrachte kritiek over het (vermeende) gebrek aan naleving van de desbetreffende voorschriften. Ook andere onderdelen van de financiële sector zijn aan de anti-witwasregelgeving onderworpen. Vaak wordt over het hoofd gezien dat dat ook geldt voor de ondernemingen die (tijdelijk) van de toepassing van de financiële toezichtwetgeving zijn vrijgesteld. Er is, mijns inziens, onvoldoende sturing op dit vlak van de wetgever en van de toezichthouders.

Banken zijn de afgelopen jaren effectief geweest in het inrichten van hun anti-witwas beleid en procedures om te voldoen aan de counter-terrorisme maatregelen die sinds 9-11 grote aandacht hebben gekend. Het staat niet ter discussie dat terrorisme financiering of de financiering van zware criminaliteit niet exclusief verloopt via de reguliere kanalen, maar dat lieden met slechte bedoelingen hun weg hebben gevonden naar de zwakste schakels in de keten, veelal betaalproposities die kunnen worden aangeboden binnen 'geliberaliseerde' onderdelen van de financiële sector. Bijvoorbeeld geldt dat voor geanonimiseerde elektronisch geldproducten, of daarmee gelijk te stellen betaalproducten of -proposities, zoals cryptocurrencies.

33. Verordening (EU) 2019/2175 van het Europees Parlement en de Raad van 18 december 2019 tot wijziging van Verordening (EU) nr. 1093/2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), Verordening (EU) nr. 1094/2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), Verordening (EU) nr. 1095/2010 tot oprichting van een Europese

toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), Verordening (EU) nr. 600/2014 betreffende markten in financiële instrumenten, Verordening (EU) 2016/1011 betreffende indices die worden gebruikt als benchmarks voor financiële instrumenten en financiële overeenkomsten of om de prestatie van beleggingsfondsen te meten, en Verordening (EU) 2015/847 betreffende bij geldovermakingen te voegen informatie, *PbEU* L 334 van 27 december 2019.

Als blije belastingbetaler ben ik natuurlijk ontstemd over de gelegenheid die kon worden gegeven aan personen met het oogmerk om belasting te ontduiken, door rammelende compliance door de banken (en verzekeraars) met de anti-witwasregelgeving. Naar mijn mening is de scherpe aandacht en prioritering de afgelopen decennia voor bestrijden van terrorismefinanciering, mensenhandel, kinderporno en andere vormen van zware criminaliteit mogelijk een factor geweest die de aandacht voor de 'klassieke' doelstelling van de witwasregelgeving, namelijk het bestrijden van fiscale delicten, heeft doen verslappen. Laten de banken vooral niet ophouden met versterking van beleid, procedures en processen op dit vlak.

Maar als gewone burger vind ik het wellicht belangrijker om veilig op straat te kunnen lopen, en dat de samenleving wordt beschermd tegen aanvallen tegen de rechtstaat en de persoonlijke veiligheid. Om deze reden vind ik het noodzakelijk dat wetgevers en toezichthouders duidelijker worden over de toepassing van de anti-witwasregels door vrijgestelde of uitgezonderde betaaldienstverleners en elektronisch geldinstellingen, en dat er kritisch wordt gekeken naar de wijze waarop lekkages in het systeem kunnen ontstaan, door de toepassing van het stelsel van Europese paspoorten door de BigTechs. Deze ondernemingen hebben er uiteraard geen belang bij om de miljoenen gebruikers van hun applicaties opnieuw aan een deugdelijk cliëntenonderzoek te onderwerpen voordat deze gebruikers als cliënt de betaalproposities van deze BigTechs mogen benutten. Het zal een sterke toezichthouder vergen, om opgewassen te zijn tegen de macht van de BigTechs die het liefst, niet gehinderd door enige compliance met Europese wet- en regelgeving, hun proposities aan een zo groot mogelijke groep gebruikers willen aanbieden, zonder kritisch te zijn wie die gebruikers nu daadwerkelijk zijn.