FinTech & Wwft

Innovatie in het klantacceptatieproces: waarborgen en aandachtspunten

mr. T.W.G. de Wit*

Trefwoorden: innovatie, fintech-oplossingen, klantacceptatieproces

Innovatie in het klantacceptatieproces

Financiële dienstverlening is de laatste jaren in rap tempo gedigitaliseerd. Klanten worden tegenwoordig veelal online of mobiel bediend en zij verwachten snelle, goedkope en persoonlijke dienstverlening. Om aan die wensen te kunnen voldoen moeten marktpartijen onderling concurreren en innoveren. Met name ten aanzien van de inrichting van het klantacceptatieproces leidt dit niet zelden tot hoofdbrekens. Enerzijds moeten marktpartijen het klantacceptatieproces zo kostenefficiënt mogelijk inrichten en mag de klantacceptatie niet afdoen aan de beleving van de klant en snelheid waarmee deze bediend kan worden. Anderzijds brengt de digitale dienstverlening vanwege het gebrek aan fysiek contact juist nieuwe en verhoogde risico's en uitdagingen met zich mee voor de inrichting van het klantacceptatieproces. Dit stelt marktpartijen (hierna: 'Wwft-instellingen') voor een lastige uitdaging: de business faciliteren op een manier waarop naleving van de Wet ter voorkoming van witwassen en financieren van terrorisme ('Wwft') en de Sanctiewet 1977 voldoende is gewaarborgd. Dit is het moment waar innovatieve oplossingen voor het klantacceptatieproces om de hoek komen kijken en uitkomst kunnen bieden.

In dit artikel ga ik in op de mogelijkheden om dergelijke innovatieve oplossingen voor het klantacceptatieproces in te zetten voor een (kosten)efficiëntere naleving van de Wwft (hierna: 'FinTech-oplossing') en de aandachtspunten die daarbij gelden. Met FinTech-oplossing doel ik dan op een innovatieve tool of applicatie die een marktpartij kan integreren in het klantacceptatieproces of de transactiemonitoring, vaak om naleving van de Wwft (kosten)efficiënter in te richten en de klantbeleving te verhogen. Ik bespreek de aandachtspunten aan de hand van een recente opinie van de European Supervisory Authorities[1] ('ESA's').

* Tim de Wit is advocaat bij Finnius in Amsterdam.

1 De ESA's bestaan uit de European Banking Authority ('EBA'), de European Insurance and Occupational Pensions Authority ('EIOPA') en de European Securities and Markets Authority ('ESMA').

2 JC 2017 81, 23 January 2018, Opinion on the use of innovative solutions by credit institutions and financial institutions in the customer due diligence process.

3 Richtlijn (EU) 2015/849.

Recent hebben de ESA's zich voor het eerst uitgesproken over de mogelijkheden om FinTech-oplossingen te integreren in het klantacceptatieproces en de daarbij te treffen maatregelen

De Opinie

Recent hebben de ESA's zich voor het eerst uitgesproken over de mogelijkheden om FinTech-oplossingen te integreren in het klantacceptatieproces en de daarbij te treffen maatregelen. Het standpunt van de ESA's is neergelegd in een opinie: '*Opinion on the use of innovative solutions by credit institutions and financial institutions in the customer due diligence process*'[2] (de 'Opinie'). Zoals zal blijken is de Opinie niet alleen relevant bij de beoordeling van de specifieke kenmerken van een FinTech-oplossing, maar biedt deze ook een interessante inkijk in het niveau van maatregelen die de ESA's van marktpartijen verwachten voor naleving van de Wwft. De maatregelen reiken verder dan alleen het beoordelen van een FinTech-oplossing, maar raken ook de hele inrichting van de bedrijfsvoering en governance rond naleving van de Wwft. Bij nadere bestudering blijken hier ook zeer interessante overwegingen in te staan die ook zonder het gebruik van een FinTech-oplossing relevant zijn voor de inrichting van het klantacceptatieproces. Hieronder ga ik nader in op de Opinie en de door de ESA's geformuleerde maatregelen.

Reikwijdte van de Opinie

De Opinie is geadresseerd aan de toezichthouders die bevoegd zijn toezicht te houden op naleving van de nationale implementatie van de Vierde Anti-witwasrichtlijn[3] ('AMLD4') (in Nederland zijn dit De Nederlandsche Bank ('DNB') en de Autoriteit Financiële Markten ('AFM')). Wwft-instellingen die FinTech-oplossingen willen integreren in hun klantacceptatieproces doen er dus goed aan deze Opinie te raadplegen, omdat hierin het toetsingskader voor DNB en de AFM is vastgelegd.

In Nederland is AMLD4 overigens nog niet geïmplementeerd. De verwachting is dat dit in de loop van 2018 zal gebeuren. AMLD4 wordt geïmplementeerd in

de Wwft[4] en het Uitvoeringsbesluit Wwft 2018.[5] De Opinie is dus relevant voor uitleg van de verplichtingen uit hoofde van AMLD4, die in Nederland nog niet gelden. Niettemin is naar mijn mening deze Opinie ook nu al relevant voor de uitleg van de verplichtingen uit hoofde van de huidige Wwft (die overigens primair gebaseerd is op de voorganger van AMLD4, de Derde Anti-witwasrichtlijn[6] ('AMLD3')).

In de Opinie geven de ESA's de factoren mee die de AFM en DNB zouden moeten meewegen

In de Opinie geven de ESA's de factoren mee die de AFM en DNB zouden moeten meewegen wanneer: (i) zij de effectiviteit van de klantacceptatieprocessen toetsen waarin Wwft-instellingen FinTech-oplossingen hebben geïntegreerd en (ii) zij de controlemechanismen beoordelen aan de hand waarvan Wwft-instellingen de risico's mitigeren die gepaard gaan met de FinTech-oplossing(en).

Type innovatieve oplossingen

De ESA's constateren dat Wwft-instellingen zich bij de keuze voor bepaalde FinTech-oplossingen met name laten leiden door een verbeterde klantbeleving en kostenbesparingen. De meeste oplossingen zijn dus hierop gericht. Grofweg zien de ESA's twee type FinTech-oplossingen die momenteel gebruikt worden:

1. Oplossingen die voorzien in niet-fysieke verificatie van de identiteit van de klant op basis van diens traditionele identiteitsdocumenten (zoals een paspoort of rijbewijs) met behulp van bijvoorbeeld een *smartphone*.
2. Oplossingen die voorzien in verificatie van de identiteit van de klant op een andere manier, zoals via een centrale bewaarplaats van identiteitsdocumenten (*central identity documentation repository*). Zo'n centrale bewaarplaats is dan veelal een samenwerking van verschillende marktpartijen die binnen het bereik van AMLD4 vallen. Het doel van zo'n bewaarplaats is dat informatie maar één keer hoeft te worden opgevraagd en daarna kan worden gedeeld met de deelnemers van de bewaarplaats.

Er zijn inderdaad verschillende initiatieven op dit vlak waarneembaar. Bepaalde dienstverleners voorzien in de behoefte om alleen de verificatie van de identiteit op afstand te faciliteren, door daar bijvoorbeeld een tool voor te ontwikkelen (i) voor de smartphone waarbij de klant een foto van zijn of haar identiteitsbewijs kan maken of (ii) die live videochats of videoconferences mogelijk maken met de klant.[7] Andere dienstverleners richten zich juist op het vergemakkelijken van het hele klantacceptatieproces, door een tool te ontwikkelen waarbij de klant in een online of mobiele applicatie al zijn of haar verplichte gegevens en documentatie kan invoeren.

De ESA's zien ook een toenemend gebruik van FinTech-oplossingen om de relatie met de klant en diens transacties te monitoren. Dat soort oplossingen werken dan veelal op basis van *artificial intelligence* en bepaalde algoritmen, die de Wwf-instellingen in staat stellen om grote hoeveelheden data van verschillende bronnen te verwerken. De FinTech-oplossing blijft zichzelf continue verbeteren aan de hand van data uit het verleden en als de oplossing goed is geïntegreerd, kan deze bijdragen aan:

- Het monitoren van risico's die verbonden zijn aan een klant of bepaalde transacties, door zowel interne informatie (zoals rekeningdetails en verrichte transacties) als externe informatie (zoals UBO-registers, bepaalde media of Google en PEP-lijsten) mee te wegen (waaronder bijvoorbeeld ook in verschillende talen).
- Het verder automatiseren van monitoringsystemen, zodat de capaciteit en inzet van medewerkers van de Wwft-instelling uit kan gaan naar analyse van de data.
- Een verbeterde besluitvorming ten aanzien van mogelijke ongebruikelijke transacties door het ontvangen van *instant alerts*.
- Het beperken van foutieve informatie of meldingen.

Zo bezien kunnen FinTech-oplossingen dus niet alleen een positieve bijdrage leveren aan de klantbeleving en kostenbesparing, maar kunnen zij ook daadwerkelijk de klantacceptatieprocessen verbeteren

Zorgvuldige afweging

Zo bezien kunnen FinTech-oplossingen dus niet alleen een positieve bijdrage leveren aan de klantbeleving en kostenbesparing, maar kunnen zij ook daadwerkelijk

---

[4] Op het moment van schrijven van dit artikel is het wetsvoorstel inmiddels aangenomen door de Tweede Kamer (op 6 maart 2018). Het wetsvoorstel ligt nu bij de Eerste Kamer.

[5] Het Uitvoeringsbesluit Wwft 2018 is ter consultatie aan de markt voorgelegd op 31 januari 2018. Marktpartijen konden reageren tot en met 28 februari 2018. Het is nu wachten op het definitieve besluit. Het concept Uitvoeringsbesluit Wwft 2018 dat ter consultatie is voorgelegd is te raadplegen via: https://www.internetconsultatie.nl/uitvoeringsbesluitwwft2018.

[6] Richtlijn 2005/60/EG.

[7] Na een snelle rondgang op Google komen partijen voorbij als IDology, Gemalto en Jumio.

de klantacceptatieprocessen verbeteren. Wwft-instellingen mogen wat de ESA's betreft echter niet over één nacht ijs gaan bij de keuze van een FinTech-oplossing en de integratie daarvan. Sterker nog, de ESA's verwachten dat marktpartijen zeer zorgvuldig afwegen, met het oog op de risico's van hun onderneming en de risico's bij individuele klantrelaties, of de implementatie van FinTech-oplossingen wel effectief is. Daarbij moet door de Wwft-instellingen met name gekeken worden naar:

— toezicht en controlemechanismen;
— de kwaliteit en effectiviteit van klantacceptatieprocessen;
— de betrouwbaarheid en afhankelijkheid van klantacceptatieprocessen;
— risico's vanwege het leveringskanaal; en
— geografische risico's.

Hieronder ga ik nader in op deze individuele factoren. Deze af te wegen factoren gelden overigens in aanvulling op de 'algemene' risicofactoren die marktpartijen al moeten afwegen uit hoofde van art. 8 AMLD4 en de zogenoemde *Risk Factor Guidelines*[8] en die verband houden met hun cliënten, landen of geografische gebieden, producten, diensten, transacties en leveringskanalen.

In algemene zin merken de ESA's op dat Wwft-instellingen die FinTech-oplossingen willen integreren, zich een volledig beeld moeten vormen van kenmerken van de oplossing om daarmee voldoende zekerheid te hebben dat de oplossing adequaat werkt en om voorbereid te zijn voor een moment waarop de oplossing (tijdelijk) niet werkt. Wwft-instellingen moeten voldoende in-house kennis en expertise hebben om effectieve integratie en gebruik ervan te waarborgen en om in geval van falen de continuïteit van de klantacceptatieprocedures te waarborgen. Uiteindelijk moet natuurlijk worden voorkomen dat – vanwege een falen van het systeem – klanten worden geaccepteerd die normaliter niet door het klantacceptatieproces zouden komen. Dit gaat vrij ver en betekent volgens de ESA's in ieder geval dat Wwft-instellingen zichzelf moeten afvragen:

— Of er voldoende technische kennis aanwezig is om de implementatie van de FinTech-oplossing te overzien, met name wanneer deze zijn ontwikkeld of worden uitgevoerd door derde partijen?
— Of de leiding en de compliance officer voldoende begrip hebben van de FinTech-oplossing?
— Of er een gedegen calamiteitenplan aanwezig is in geval van falen van de FinTech-oplossing?

Dit is al meteen een zware verplichting voor Wwft-instellingen die FinTech-oplossingen willen integreren in hun klantacceptatieproces. Zeker voor kleinere marktpartijen, voor wie het omwille van kosten en compliance juist nuttig kan zijn FinTech-oplossingen te implementeren, zal het lastig zijn om aan deze eisen van de ESA's te voldoen. Dit zal alleen al zo zijn omdat de keuze voor de oplossing er juist in gelegen zal zijn dat men intern niet voldoende technische of personele middelen heeft. Hier ligt in ieder geval een uitdaging voor de directie van de Wwft-instelling; zij zal moeten vaststellen dat waar de instelling besluit tot implementatie van een FinTech-oplossing, de instelling ook in staat is om de impact daarvan te overzien. Ik kan me voorstellen dat de compliance officer betrokken wordt in deze afweging en daarin een belangrijke rol vervult.

Toezicht en controlemechanismen bij selectie van FinTech-oplossing

Wanneer Wwft-instellingen besluiten FinTech-oplossingen te integreren in hun klantacceptatieproces, moeten zij richting DNB of de AFM kunnen aantonen dat ze adequate governance en controlemechanismen hanteren omtrent besluitvorming voor een FinTech-oplossing in het klantacceptatieproces. DNB en de AFM moeten hierbij de volgende aspecten toetsen:

a. De Wwft-instelling moet de FinTech-oplossing eerst goed en grondig testen voor implementatie. De oplossing moet aansluiten bij het klantacceptatieproces van de Wwft-instelling en moet voldoen aan de relevante wet- en regelgeving. Wanneer de resultaten niet eenduidig zijn, moet de Wwft-instelling de FinTech-oplossing nog enige tijd draaien parallel aan het oude proces totdat de instelling ervan overtuigd is dat de FinTech-oplossing hetzelfde resultaat behaalt. De compliance en/of risk officer moeten worden betrokken bij de tests. Deze tests moeten aan de toezichthouder op verzoek kunnen worden overlegd.
b. De Wwft-instelling moet een schriftelijke overeenkomst aangaan met de aanbieder van de FinTech-oplossing en moet daarin afdwingen dat hij wordt geïnformeerd over alle wijzigingen met betrekking tot de oplossing en wijzigingen en ook voorafgaande goedkeuring verlangen.
c. De Wwft-instelling moet procedures hebben die voorzien in continue monitoren van de effectiviteit en werking van de FinTech-oplossing, door in ieder geval de processen te toetsen. Als er een fout wordt ontdekt, moet de Wwft-instelling: (i) alle geïnfecteerde klantrelaties beoordelen; (ii) een afweging maken of bepaalde geïnfecteerde klantrelaties of daarbij betrokken transacties moeten worden beëindigd met de kennis van nu; en (iii) een afweging maken of melding moet worden gedaan aan de Financial Intelligence Unit ('FIU') van een ongebruikelijke transactie. Het verdient aanbeveling om deze afwegingen te documenteren.
d. Wanneer een fout is ontdekt in de FinTech-oplossing, moet de Wwft-instelling – in aanvulling op de hierboven genoemde maatregelen – beoordelen of: (i) de oplossing nog wel voldoende betrouwbaar is voor de Wwft-instelling; (ii) bepaalde aanpassin-

[8] JC 2017 37, 26/06/2017. Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and firms should consider when assessing the money laundering and terrorist financing risk associated with individual business relationship and occasional transactions.

gen moeten worden gemaakt; en (iii) de oplossing kan worden voortgezet. Het verdient aanbeveling deze afwegingen te documenteren.

e. De Wwft-instelling moet maatregelen (zoals periodieke tests) treffen die waarborgen dat de instelling alle relevante informatie en documentatie ingewonnen met de FinTech-oplossing kan opslaan en bewaren. De Wwft-instelling moet op verzoek van de toezichthouders alle relevante informatie direct kunnen verstrekken.
f. De Wwft-instelling moet maatregelen treffen die datalekken voorkomen, waarbij de Wwft-instelling moet kunnen aantonen hoge standaarden te hanteren voor data en IT veiligheid.
g. De Wwft-instelling moet waarborgen dat het gebruik van de FinTech-oplossing in het klantacceptatieproces niet leidt tot strijd met privacyregelgeving, met name wanneer klantdocumentatie extern is opgeslagen. De Wwft-instelling zou dit volgens de ESA's moeten kunnen 'bevestigen' aan de toezichthouders.
h. De Wwft-instelling moet maatregelen treffen die voorkomen dat haar werknemers samenspannen met criminelen, zoals screening van nieuwe medewerkers (*pre-employment screening*). Dit is breder dan alleen ten aanzien van FinTech-oplossingen.
i. De Wwft-instelling moet waarborgen dat haar medewerkers voldoende getraind zijn om de FinTech-oplossing te kunnen gebruiken. Hiertoe moeten Wwft-instellingen periodieke training verzorgen met specifieke focus op de praktische en technische toepassing van de FinTech-oplossing en het detecteren van ongebruikelijke transacties.
j. De Wwft-instelling moet alle mogelijke compliance- en operationele risico's afwegen die zijn gerelateerd aan het gebruik van de FinTech-oplossing, zoals bijvoorbeeld een faillissement of andere opstartproblemen van nieuwe FinTech initiatieven. Dit moet in aanvulling op de algemene risicobeoordeling als bedoeld in art. 8 AMLD4.
k. Wanneer de Wwft-instelling informatie uitwisselt met de aanbieder van de FinTech-oplossing, specifiek wanneer deze gevestigd is in een derde land, moet worden vastgesteld dat dit toegestaan is op grond van wet- en regelgeving.

De ESA's vereisen van Wwft-instellingen dus nogal vergaande maatregelen alvorens een Wwft-instelling überhaupt kan overgaan tot de keuze voor een bepaalde FinTech-oplossing. Het is naar mijn mening van belang het selectieproces voor een bepaalde FinTech-oplossing zorgvuldig te documenteren, zodat dit op een later moment desgewenst kan worden overgelegd aan de toezichthouder om aan te tonen dat de instelling alle relevante factoren heeft afgewogen. Het lijkt mij ook prudent dat de Wwft-instelling een selectie maakt van verschillende aanbieders van vergelijkbare producten, om daarin een bewuste keuze te maken voor de beste FinTech-oplossing gelet op het doel dat de Wwft-instelling ermee beoogt te bereiken.

De ESA's vereisen van Wwft-instellingen dus nogal vergaande maatregelen alvorens een Wwft-instelling überhaupt kan overgaan tot de keuze voor een bepaalde FinTech-oplossing

Kwaliteit en effectieve werking van de FinTech-oplossing

Wwft-instellingen zijn op grond van AMLD4 verplicht om aan de toezichthouder te kunnen aantonen dat hun klantacceptatieprocedures evenredig zijn aan de witwasrisico's die zij lopen. Dit betekent volgens de ESA's onder meer dat een Wwft-instelling die een FinTech-oplossing wil implementeren, moet kunnen aantonen dat die oplossing voldoende betrouwbaar is en ook evenredig is met het oog op de witwasrisico's die de Wwft-instelling loopt. Volgens de ESA's moeten de toezichthouders in ieder geval de volgende factoren afwegen:

a. De Wwft-instelling moet maatregelen treffen die waarborgen dat een klantrelatie pas tot stand komt nadat het volledige klantacceptatieproces is doorlopen. De uiteindelijke keuze voor het aangaan van een klantrelatie moet bij de Wwft-instelling liggen (en dus niet bij de FinTech-oplossing), waaronder de acceptatie van hoog risicoklanten en de goedkeuring voor een klantrelatie met een PEP. Dit speelt met name wanneer het klantacceptatieproces wordt doorlopen via een FinTech-oplossing van een externe aanbieder.
b. De Wwft-instelling moet controlemechanismen hebben om de kwaliteit van het klantacceptatieproces en de gegevens en informatie die worden ingewonnen te kunnen monitoren wanneer de Wwft-instelling gebruikmaakt van een (interne of externe) FinTech-oplossing. Denk hierbij aan regelmatige tests, voortdurende compliancemonitoring, beoordelingen door de *internal audit*-functie en *on-site visits* in geval van een externe dienstverlener.
c. Wanneer de FinTech-oplossing voorziet *in* monitoring van de klantrelatie en klanttransacties, dan moet de Wwft-instelling waarborgen dat de oplossing effectief en efficiënt werkt. De oplossing moet volledig aansluiten bij de processen van de Wwft-instelling en toegang hebben tot alle informatie. De Wwft-instelling moet weten welke data en informatie wordt meegewogen door de FinTech-oplossing en moet de betrouwbaarheid van die data en informatie op waarde kunnen schatten. De FinTech-oplossing moet in staat zijn een zorgvuldige afweging te maken van ongebruikelijke transacties en moet een totaalbeeld kunnen vormen van het klantprofiel, door alle relevante informatie aan elkaar te linken.
d. De Wwft-instelling moet waarborgen dat de documentatie, de gegevens en informatie ingewon-

nen door de FinTech-oplossing in het kader van de klantacceptatie actueel blijft.

De Wwft-instelling moet dus een goed begrip hebben van het specifieke product dat hij afneemt

De Wwft-instelling moet dus een goed begrip hebben van het specifieke product dat hij afneemt. Dit betekent wat mij betreft in de praktijk dat de aanbieder van de FinTech-oplossing het product en alle kenmerken uitgebreid presenteert aan de Wwft-instelling, dat daar alle bij het klantacceptatieproces betrokken medewerkers bij betrokken zijn en dat er verschillende oefensessies gepland worden om met het product te werken.

Betrouwbaarheid van gegevens ingewonnen met de FinTech-oplossing

Wwft-instellingen moeten extra aandacht besteden aan de geldigheid en authenticiteit van de documentatie, gegevens en informatie die worden ingewonnen via video conferences, mobiele apps, of andere digitale wegen. Hierbij moeten Wwft-instellingen in ieder geval de volgende factoren afwegen:

a. De Wwft-instelling moet het risico dat het beeld van de klant op het scherm wordt gemanipuleerd zoveel mogelijk beperken. Hiertoe kan de instelling verschillende maatregelen treffen:
   - Een live chat met een medewerker die getraind is ongebruikelijk gedrag te herkennen.
   - Een ingebouwde applicatie die automatisch biometrische gezichtsherkenning toepast op basis van een digitale foto of video conference.
   - Minimale verlichting van het scherm dat wordt gebruikt voor het maken van een foto of video conference, zodat de persoon duidelijk in beeld komt.
   - Een ingebouwde applicatie die afbeeldingen kan herkennen waarin gephotoshopt is.

b. De Wwft-instelling moet voorkomen dat het getoonde identiteitsbewijs van een ander persoon is die veel lijkt op de klant. Hiervoor moeten bepaalde waarborgen zijn ingebouwd in de FinTech-oplossing die dergelijke verschillen tussen personen kunnen herkennen.

c. De Wwft-instelling moet controlemechanismen inbouwen die waarborgen dat het identiteitsbewijs niet is gewijzigd, nagemaakt of hergebruikt. Hiertoe kunnen Wwft-instellingen de volgende maatregelen treffen:
   - Ingebouwde *tools* die frauduleuze identiteitsbewijzen kunnen herkennen op basis van de (veiligheids)kenmerken van het identiteitsbewijs (watermerk, de foto, overige gegevens en de plek waar die gegevens zijn weergegeven op het document).
   - Vergelijken van de veiligheidskenmerken aan de hand van een template identiteitsbewijs.
   - Wanneer verificatie niet plaatsvindt op basis van door de overheid uitgegeven identiteitsdocumenten, een *tool* die het mogelijk maakt de van de klant verkregen informatie te controleren aan de hand van een combinatie van betrouwbare en onafhankelijke bronnen (waaronder de Kamer van Koophandel), aangevuld met analyses van *social media*, IP-adres, locatie en andere gegevens uit openbare bron.
   - Beperken van de identiteitsbewijzen die voor verificatie kunnen worden gebruikt tot bewijzen die:
     - Sterke veiligheidskenmerken hebben of biometrische gegevens zoals vingerafdrukken en een foto van het gezicht. Het lijkt mij sowieso zeer wenselijk dat het document in ieder geval een foto heeft.
     - Een gekwalificeerde elektronische handtekening gekoppeld hebben (als bedoeld in de zogenoemde eIDAS Verordening[9], waarover hierna meer). De gekwalificeerde elektronische handtekening voldoet aan bepaalde waarborgen. Er wordt een gekwalificeerd certificaat (een digitaal bestand) aan het oorspronkelijke document toegevoegd. Het certificaat is uitgegeven door een speciale instantie. Een gekwalificeerde elektronische handtekening biedt aldus extra waarborgen dat de persoon inderdaad is wie hij of zij beweert te zijn.
     - Via de FinTech-oplossing een koppeling maken met informatie uit betrouwbare en onafhankelijke bron, zoals de Kamer van Koophandel.
     - Via de FinTech-oplossing een koppeling maken met het door de overheid ingerichte stelsel voor elektronische identiteit (eID) als bedoeld in de eIDAS Verordening.

[9] Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Zie voor een nadere beschouwing van de juridische implicaties van de eIDAS Verordening: J.J. Linnemann, 'Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten', *IR* 2015, nr. 5/6, p. 176-181 en J.J. Linnemann, 'Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten: elektronische identificatie', *IR* 2016, nr. 4, p. 134-139.

Lidstaten moeten vanaf 29 september 2018 toestaan dat Europese burgers en bedrijven zich kunnen identificeren bij organisaties in de publieke sector met behulp van een eID, uitgegeven in iedere willekeurige lidstaat van de EU

Als korte toelichting: een eID is in feite een elektronische identiteit, die de persoon in kwestie in de gelegenheid stelt zich online te identificeren. Lidstaten moeten vanaf 29 september 2018 toestaan dat Europese burgers en bedrijven zich kunnen identificeren bij organisaties in de publieke sector met behulp van een eID, uitgegeven in iedere willekeurige lidstaat van de EU. Het is dan in feite een derde (namelijk de uitgever van het eID) die garandeert jegens de organisatie waar de persoon inlogt, dat de persoon is wie hij of zij beweert te zijn. Aan de opzet van een eID zitten bepaalde waarborgen vast, zoals dat de uitgever van het eID de identiteit van de persoon heeft vastgesteld. In Nederland zijn eHerkenning[10] (voor rechtspersonen) en Idensys[11] (voor natuurlijke personen) dergelijke eID's die door de Nederlandse overheid worden ondersteund teneinde bij organisaties in de publieke sector te kunnen inloggen. Ondernemingen kunnen er tevens voor kiezen hun klanten zich te laten identificeren door deze eID's, maar dat zijn ze – anders dan de overheid – niet verplicht. Vanuit de private sector is door een gezamenlijk initiatief van banken een eID ontwikkeld onder de naam iDIN.[12] Banken zijn immers al verplicht – op grond van de Wwft – al hun klanten te identificeren.[13]

d. De Wwft-instelling moet maatregelen treffen die waarborgen dat alle ongebruikelijke transacties of patronen worden herkend. De instelling moet de output van de FinTech-oplossingen kunnen controleren op kwaliteit en vergelijken met haar eigen output tot dusver.
e. Wanneer de FinTech-oplossing wordt gebruikt voor het monitoren van de zakelijke relatie, moet de Wwft-instelling kunnen waarborgen dat alle relevante informatie en data beschikbaar is voor de FinTech-oplossing en betrouwbaar is.

Risico's vanwege het leveringskanaal (online of digitaal)

Juist in gevallen waar een onderneming een FinTech-oplossing wil integreren in het klantacceptatieproces, zal vaak geen fysiek contact plaatsvinden met de klant. Relevant in dit kader is dat AMLD4 – in tegenstelling tot de huidige Wwft en AMLD3 – niet langer voorschrijft dat in geval de cliënt niet fysiek aanwezig is voor verificatie van diens identiteit, dit per definitie kwalificeert als verhoogd risico en er altijd verscherpt cliëntonderzoek moet worden toegepast. In plaats daarvan volgt uit Annex III van AMLD4 dat het aangaan van een zakelijke relatie op afstand – zonder bepaalde waarborgen zoals een elektronische handtekening – een factor is voor een potentieel verhoogd risico. Het is dus aan de instelling zelf hier een afweging in te maken. De ESA's merken hierbij op dat Wwft-instellingen bij het onboarden van een klant via een FinTech-oplossing in ieder geval de volgende factoren moeten meenemen.

a. Bestaat er een risico dat de klant niet is wij hij of zij beweert te zijn (identiteitsfraude)? Om dit risico (dat in feite altijd aanwezig is) zoveel mogelijk te beperken, kunnen instellingen de volgende maatregelen treffen:
   - Verificatie aan de hand van een combinatie van gegevens, waaronder van het identiteitsbewijs, de informatie van de live chat en overheidsinformatie.
   - Ingebouwde *tool* aan de hand waarvan de moedertaal van een klant kan worden achterhaald op basis van schriftelijke communicatie met die klant.
   - Als voorwaarde stellen dat alle documentatie is afgegeven met een gekwalificeerde handtekening.
   - Verificatie van het adres door er een brief naartoe te sturen.
   - Verificatie van de identiteit aan de hand van een eID dat is afgegeven in overeenstemming met de eIDAS Verordening.[14]

   Dit laatste lijkt mij een zeer positieve ontwikkeling. Het effect van het gebruik van een eID is dat een onderneming kan vaststellen dat een persoon is wie hij of zij beweert te zijn.[15] Wat mij betreft mag daar dus (juist) ook in het kader van de Wwft veel waarde aan toegekend worden. Die koppeling werd tot nu toe echter nog niet gemaakt, dus wat dat betreft is het naar mijn idee positief dat de ESA's die koppeling nu wel maken.[16] Het kan ook

[10] www.eherkenning.nl.
[11] www.idensys.nl.
[12] www.idin.nl.
[13] Zie voor een nadere beschouwing van de juridische implicaties van het eID het in voetnoot 10 aangehaalde artikel van Linnemann.
[14] Zie voetnoot 9.
[15] Zie ook Overweging 16 eIDAS Verordening.
[16] Overigens is de koppeling ook gemaakt in het recente FinTech Action plan van de Europese Commissie, van 8 Maart 2018 (IP/18/1403. Hierin noemt de Europese Commissie (op pagina 4): '*Additionally, the cross border recognition of electronic means of identification provided by the eIDAS Regulation will provide safeguards and mitigate risks from emerging technologies, while making it easier to meet customer due diligence anti-money laundering requirements and strong authentication of parties in a digital environment.*' En later op pagina 10: '*(...) the Commission announced its intention to facilitate the cross-border acceptance of e-identification and remote know-your-customer processes. The aim is to enable banks to identify consumers digitally in compliance with anti-money laundering and data protection*

zijn dat de ESA's hier al vooruitlopen op een voorstel van de Europese Commissie tot wijziging van AMLD4 (het 'Voorstel' en ook wel 'AMLD5' genoemd).[17] In art. 13 lid 1, onder a) van het Voorstel is expliciet aangegeven dat een Wwft-instelling de identiteit van de cliënt kan verifiëren op basis van documenten, gegevens of informatie uit betrouwbare en onafhankelijke bron, *met inbegrip van, voor zover beschikbaar, een eID zoals vastgesteld in de eIDAS Verordening*. Dat zou er dus toe moeten leiden dat indien een klant inlogt met behulp van een eID en daarmee bepaalde gegevens verstrekt aan de Wwft-instelling, daarmee ook de identiteit van de klant door de Wwft-instelling is geverifieerd. Dat neemt niet weg dat er nog additionele maatregelen getroffen moeten worden, maar het zou in potentie een lastenverlichting kunnen betekenen voor veel Wwft-instellingen (met name waar het natuurlijke personen betreft, en geen UBO of wettelijke vertegenwoordiger hoeft te worden geïdentificeerd). Het is interessant om deze ontwikkelingen nauwgezet te volgen de komende tijd.

b. Bestaat er een risico dat de klant (door een ander) onder druk is gezet gedurende het klantacceptatieproces? Dit zou natuurlijk vrij ver gaan, maar de ESA's verwachten niettemin van Wwft-instellingen dat ze controlemechanismen hebben geïmplementeerd die dwang kunnen herkennen, bijvoorbeeld door werknemers die live chats voeren te trainen op het herkennen van dwang.

Geografische risico's

Tot slot wijzen de ESA's op geografische risico's die Wwft-instellingen moeten afwegen bij digitale klantacceptatie. Wwft-instellingen moeten kunnen controleren vanuit welk land of regio de klant het klantacceptatieproces doorloopt (zoals aan de hand van GPS). Daarnaast moeten Wwft-instellingen beoordelen waarom een klant woonachtig of gevestigd in een ander land of regio juist de diensten wil gebruiken van de instelling.

Dankzij de Opinie de weg in ieder geval open ligt voor marktpartijen om FinTech-oplossingen te implementeren in hun klantacceptatieproces en transactiemonitoring

Indruk van de Opinie

In de Opinie schetsen de ESA's zeer gedetailleerde maatregelen die Wwft-instellingen moeten afwegen bij het gebruik van FinTech-oplossingen. Het voelt bijna alsof een team van knappe koppen van EBA bij elkaar is gaan zitten en alle mogelijke maatregelen heeft bedacht die men maar kan bedenken. Het positieve hieraan is dat dankzij de Opinie de weg in ieder geval open ligt voor marktpartijen om FinTech-oplossingen te implementeren in hun klantacceptatieproces en transactiemonitoring. Tot nu toe was onder omstandigheden gissen of de toezichthouders (DNB en de AFM) zich in dergelijke initiatieven konden vinden voor naleving van de Wwft. De ESA's dragen de toezichthouders nu expliciet op om deze ontwikkelen te ondersteunen, met name wanneer FinTech-oplossingen de effectiviteit en efficiëntie van naleving met de Wwft verbeteren.[18] Daarbij moeten de risico's natuurlijk ook zorgvuldig worden afgewogen. Wwft-instellingen moeten kunnen aantonen dat ze alle relevante risico's hebben geïdentificeerd, afgewogen en gemitigeerd voordat de keuze voor een FinTech-oplossing wordt gemaakt. Hier ligt dan ook een concrete uitdaging voor de Wwft-instelling. Wanneer de instelling overweegt een FinTech-oplossing te integreren in haar klantacceptatieproces, doet zij er goed aan de Opinie als checklist te hanteren, daar ook goed onderzoek naar te doen en niet blind te varen op beloftes van de makers van de FinTech-oplossing. Het proces voor de selectie van een FinTech-oplossing zou naar mijn mening goed moeten worden gedocumenteerd. Compliance officers zullen moeten waarborgen dat aan alle genoemde voorwaarden is voldaan.

Opvallend is verder dat een aantal van de door de ESA's gesuggereerde maatregelen breder toepasbaar is dan alleen maar met betrekking tot FinTech-oplossingen. Op bepaalde plekken geven de ESA's dit ook expliciet mee. Wat dat betreft biedt de Opinie dus een interessante inkijk in de maatregelen die Wwft-instellingen wat de ESA's betreft zouden moeten treffen voor naleving van de Wwft. Die gaan op het eerste gezicht nog weer verder dan de door DNB en de AFM aan de markt opgelegde maatregelen. Een voordeel is dat de ESA's vrij concrete handvatten bieden hoe marktpartijen invulling moeten geven aan hun verplichtingen op grond van AMLD4 (en daarmee de Wwft). Gelet op het risicogebaseerde karakter van de Wwft en de vele open normen, lijkt mij dat op zichzelf een positieve ontwikkeling, waarbij ik er overigens voor zou willen pleiten dat de lijst van maatregelen niet dwingend zou moeten zijn. Wwft-instellingen moeten de maatregelen treffen die zij nodig achten gelet op de specifieke risico's. Met andere woorden: als een risico zich niet of zeer beperkt voordoet, hoeft daarvoor ook geen maatregel getroffen te worden, of kan deze een lichtere invulling krijgen.

Het zou naar mijn mening ook in het belang van de markt zijn wanneer de AFM en DNB zouden uitspreken de Opinie waar relevant en waar mogelijk te volgen in hun toezicht op Wwft-instellingen. In dat

requirements, making full use of the electronic identification and authentication tools provided under eIDAS.'

[17] 2016/0208 (COD). Over het Voorstel van de Europese Commissie bereikten het Europees Parlement en de Raad een politiek akkoord over het Voorstel. Het Europees Parlement stemt 16 april 2018 over het Voorstel.

[18] Zie paragraaf 23 van de Opinie.

verband is nog relevant te noemen dat de AFM in haar agenda van 2018 heeft aangegeven te streven naar convergentie in het toezicht, om zo toezichtarbitrage te voorkomen.[19] De AFM geeft daarbij aan dat zij waar mogelijk en wenselijk zal pleiten voor meer Europese bevoegdheden voor een van de ESA's. Dit lijkt mij een zeer wenselijke ontwikkeling. Binnen deze visie past naar mijn mening zonder enige twijfel dan ook dat de AFM de Opinie van de ESA's zal volgen. Dat zou wat mij betreft ook voor DNB moeten gelden.

Slotwoord

De AFM en DNB richten zich in hun doorlopend toezicht steeds meer op naleving van integriteitswetgeving. De Wwft vraagt met haar risicogebaseerde benadering en open normen, en de steeds uitgebreidere en verdergaande uitleg daarvan door de toezichthouders (AFM, DNB en de ESA's) van Wwft-instellingen inmiddels veel meer dan alleen het opvragen van een kopie paspoort. Wwft-instellingen moeten heel zorgvuldig nadenken over hoe zij hun processen ter naleving van de Wwft inrichten. Dat blijkt eens te meer op basis van de Opinie. Niet zelden leidt dit tot hoge compliance en administratiekosten.

Er is hoop dat bepaalde FinTech-oplossingen de compliance burden wat kunnen verlichten. De Opinie doet alvast een gooi naar de mogelijkheden in dit opzicht. Dat biedt perspectief, want hierin ligt besloten dat het zeker mogelijk moet zijn om FinTech-oplossingen te implementeren voor naleving van de Wwft. Bovendien is het naar mijn mening bemoedigend dat in AMLD5 wordt voorgesteld dat de verificatie van de identiteit van de klant kan plaatsvinden aan de hand van documenten, gegevens of informatie ingewonnen door identificatie met een eID afgegeven in overeenstemming met de eIDAS Verordening. Dit past bij de huidige ontwikkelingen van meer grensoverschrijdende en digitale dienstverlening.

De ESA's leggen in de Opinie echter ook zeer nadrukkelijk de verantwoordelijkheid om naleving van de Wwft zorgvuldig te waarborgen neer bij de Wwft-instellingen, ongeacht het gebruik van een FinTech-oplossing. Instellingen mogen niet over één nacht ijs gaan bij de selectie van een FinTech-oplossing en moeten verschillende maatregelen implementeren en factoren afwegen. Dat schept dan toch weer wat onzekerheid, want *hoe* moet dat dan op een manier die de toets van de toezichthouders doorstaat? Wwft-instellingen doen er dus goed aan zorgvuldig af te wegen op welke manier zij FinTech-oplossingen kunnen implementeren in het klantacceptatieproces en de transactie monitoring en wat hun afwegingen daarbij zijn. Het is van belang het selectieproces goed te documenteren, om zo nodig later aan de toezichthouder aan te kunnen tonen waarom voor een bepaalde oplossing is gekozen. ■

[19] AFM Agenda 2018, p. 21, te raadplegen via: https://www.afm.nl/nl-nl/nieuws/2018/jan/agenda-2018.