

# Van herstel naar balans

Een vooruitblik naar een meer risicogebaseerde aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering

DeNederlandscheBank

EUROSYSTEEM



# Inhoud

## 1 Witwassen en terrorismefinanciering: omvang en bestrijding

- 1.1 Witwassen en terrorismefinanciering in Nederland
- 1.2 Voorkomen en bestrijden van financieel-economische criminaliteit
- 1.3 Een risicogebaseerde aanpak

## 2 De rol van banken als poortwachter

- 2.1 Inspanningen van banken om witwassen en terrorismefinanciering tegen te gaan
- 2.2 Gevolgen van het aangescherpte beleid van banken
- 2.3 Versterking van de risicogebaseerde aanpak

## 3 Het toezicht op de poortwachtersrol door DNB

- 3.1 Toezicht richt zich op concrete risico's
- 3.2 Voorkomen van financieel-economische criminaliteit als speerpunt van toezicht
- 3.3 Prioriteiten voor het DNB toezicht in de komende jaren
- 3.4 Europese ontwikkelingen

## 4 Gebruik van data en inzet van technologie

- 4.1 Slimmere klantonderzoeken
- 4.2 Slimmere transactiemonitoring
- 4.3 Het inzetten van netwerkanalyses
- 4.4 Data-issues

## 5 Effectief door samenwerking

- 5.1 Samenwerking in Nederland
- 5.2 Kansen voor de toekomst

## Samenvatting en aanbevelingen

**De maatschappij moet erop kunnen vertrouwen dat financiële instellingen bijdragen aan het voorkomen en bestrijden van financieel-economische criminaliteit zonder dat de financiële dienstverlening in het geding komt.** De maatschappelijke urgentie om actief financieel-economische criminaliteit tegen te gaan is groot. Witwassen ondergraaft het vertrouwen van de burger in de financiële sector. Criminele en terroristische organisaties en personen gebruiken het witgewassen geld voor eigen gewin en om verdere activiteiten te financieren. Naar schatting wordt

jaarlijks in Nederland bijna 16 miljard aan crimineel geld verdiend. Uiteindelijk betaalt de 'gewone' burger hiervoor de prijs. Niet alleen via hogere belastingen, maar ook doordat de samenleving onveiliger wordt en de rechtsstaat wordt ondermijnd. Tegelijkertijd dient die bestrijding niet te leiden tot generieke beperkingen van de financiële dienstverlening, want ook die raken de burger.

**DNB ziet erop toe dat instellingen hun aanpak op orde hebben om financieel-economische criminaliteit te voorkomen en te bestrijden.** In dit rapport ligt de focus op de rol van banken in het tegengaan van witwassen en terrorismefinanciering, en het toezicht van DNB hierop. Banken vervullen een

spilfunctie in het financiële systeem. De wetgever heeft – in lijn met internationale verplichtingen – banken daarom als poortwachter een belangrijke rol toebedeeld in het voorkomen en bestrijden van witwassen en terrorismefinanciering. In de afgelopen jaren is door zowel DNB als het Openbaar Ministerie geconstateerd dat een deel van de bancaire sector de relevante wetgeving op dit gebied onvoldoende heeft nageleefd. Hiervoor heeft DNB ingrijpende handhavingsmaatregelen opgelegd. Met twee banken heeft het Openbaar Ministerie schikkingen getroffen. Mede als reactie hierop hebben banken hun inspanningen op dit vlak aanzienlijk vergroot, maar niet elke bank is hiermee even vergevorderd. Klantdossiers worden op orde gebracht. Banken hebben hun beleid met betrekking tot acceptatie en het afscheid nemen van klanten aangescherpt. Het aantal door banken gemelde ongebruikelijke transacties is sterk toegenomen. Het bestuursrechtelijk instrumentarium van DNB is in de loop der jaren versterkt. Dit ondersteunt de inzet van DNB die is gericht op het verstevigen van het fundament voor het bestrijden van financieel-economische criminaliteit. DNB zal haar gehele instrumentarium blijven inzetten om in de sector naleving van de Wwft te bereiken.

**Het tegengaan van financieel-economische criminaliteit kan efficiënter en effectiever door een meer risicogebaseerde aanpak.** Een effectievere aanpak betekent primair dat er minder criminele gelden door de financiële infrastructuur gaan. Dit zal tot uiting komen in het vaker weren van criminelen aan de poort. En waar crimineel geld toch het systeem in komt in betere detectie, meer veroordelingen en meer afgepakte gelden. Een efficiëntere manier om financieel-economische criminaliteit tegen te gaan betekent een beperktere belasting van banken én hun klanten. Effectiever en efficiënter: het kan. Door een meer risicogebaseerde aanpak van banken én toezichthouders. Door slimmere toepassing van datagedreven technologische innovaties. Door een meer gerichte samenwerking in de hele keten. Waarbij niet angst om het fout te doen de boventoon voert, maar het vertrouwen dat we in Nederland financieel-economische criminaliteit zoveel mogelijk tegengaan als we er met alle betrokkenen de schouders onder zetten.

← ↩

**Ons onderzoek laat zien dat banken in substantiële aantallen afscheid nemen van klanten, of niet overgaan tot dienstverlening.** Om meer zicht te krijgen op de vraag hoe vaak banken klanten uitsluiten van dienstverlening of die beperken, en op welke gronden dit gebeurt, heeft DNB een uitvraag gedaan bij de vier grootste (retail)banken. Hieruit blijkt dat deze vier banken in 2021 van 7.700 klanten afscheid hebben genomen vanwege risico's op witwassen of terrorismefinanciering. Van categorale uitsluiting lijkt geen sprake: deze klanten behoorden tot een groot aantal verschillende economische sectoren. Hoewel 7.700 absoluut gezien en in het licht van de repercussies voor de betrokken klanten een substantieel aantal vormt, betreft het tegelijkertijd slechts 0,02% van het aantal particuliere en 0,17% van het aantal zakelijke klanten van deze vier banken. Het aantal potentiële klanten dat om dezelfde reden niet is geaccepteerd, is op basis van de uitvraag niet volledig vast te stellen; een ruwe schatting komt uit op ongeveer 7.000.

**Zowel banken als de toezichthouder kunnen het voorkomen en bestrijden van witwassen en terrorismefinanciering meer risicogebaseerd aanpakken.**

De risicogebaseerde aanpak is vastgelegd in internationale en nationale kaders. Zowel voor de instellingen die als poortwachter fungeren als voor toezichthouders vormen die een belangrijke leidraad.

De uitdaging voor zowel de instellingen als toezichthouders is om de risicogebaseerde aanpak meer en effectiever in de praktijk te brengen, juist ook al in de herstelfase. Dit vergt in de eerste plaats een betere risico-identificatie. In de tweede plaats dienen genomen maatregelen beter in verhouding te staan tot de geïdentificeerde risico's. Bij grotere risico's zijn striktere maatregelen nodig. Bij kleinere risico's volstaan meer eenvoudige maatregelen. Zo kunnen schaarse middelen juist daar worden ingezet waar het meeste resultaat is te behalen.

**Banken kunnen hun klanten helpen door alleen informatie uit te vragen die gegeven het risico nodig is en door uit te leggen waarom die informatie wordt uitgevraagd.** Banken moeten bij hogere risico's meer informatie opvragen bij klanten om een beeld te hebben van het risico en om de meest passende beheersmaatregelen te kunnen nemen. Bij de klanten kan dat als vervelend en disproportioneel worden ervaren. Aangezien klanten er blij van geven bereid te zijn om een inspanning te leveren om witwassen en terrorismefinanciering tegen te gaan, is het van belang dat banken duidelijk uitleggen waarom gegevens worden opgevraagd. Brancheorganisaties en banken kunnen hierbij beter samenwerken. Deze samenwerking kan zich zowel richten op scherpere en specifiekere risicoanalyses, als op gerichte informatievoorziening. Het overleg hierover in het Maatschappelijk Overleg Betalingsverkeer biedt

hiervoor een kader. Met inachtneming van privacy-waARBorgen zou het helpen als banken meer wettelijke mogelijkheden krijgen om publieke registers (BRP, UBO) te gebruiken. Tevens zouden verschillende instellingen ook (mits de klant hier toestemming voor geeft) vaker gegevens moeten kunnen uitwisselen, zodat een klant die daarvoor kiest, niet meerdere keren dezelfde gegevens hoeft aan te leveren.

**DNB verwacht van de banken een meer risicogebaseerde aanpak, zowel in hun hersteloperaties als structureel.** Een meer risicogebaseerde aanpak kan ervoor zorgen dat banken klantrisico's op een adequatere en meer gebalanceerde manier inschatten. Banken dienen zich bij deze risico-beoordeling te baseren op het totaalbeeld van de klant. De juistheid van deze risico-inschatting door banken is van essentieel belang. Een verkeerde inschatting kan twee kanten op werken. Enerzijds kan een te lage inschatting van de risico's ertoe leiden dat een bank te weinig risicobeheersende maatregelen neemt. Anderzijds kan een te hoge inschatting van de risico's ertoe leiden dat een bank te veel en te intensieve maatregelen neemt. Dit kan ten onrechte de toegang tot bancaire dienstverlening beperken. En het zadelt de klant op met onnodig vergaande vragen om informatie en documentatie. Een meer risicogebaseerde aanpak kan eraan bijdragen een betere balans te vinden tussen risico's en maatregelen. En kan ook het aantal verkeerde inschattingen en onnodige de-risking

←  
↩

beperken. Waar mogelijk geeft DNB via beleidsuitingen banken vertrouwen dat zij hiermee binnen de wettelijke kaders blijven.

**Een risicogebaseerde aanpak vormt voor DNB de kern van haar toezicht op de poortwachtersfunctie ten aanzien van financieel-economische criminaliteit.** Hierbij houdt DNB het doel van de wet voor ogen: een schone en integere financiële sector. DNB beoogt de risicogebaseerde benadering in de komende periode naar een hoger niveau te brengen, zowel in haar toezicht als in de risicogebaseerde toepassingen van de relevante wetgeving door banken. DNB ziet een meer risicogebaseerde benadering van banken als belangrijk aandachtspunt in het toezicht, ook bij het toezien op de hersteloperaties van banken. Bij DNB zelf zorgt de risicogebaseerde aanpak ervoor dat de inzet van de toezichtscapaciteit groter is naarmate de risico's groter zijn, en minder waar deze beperkter zijn. Voor DNB als toezichthouder is de risicoanalyse daarom van essentieel belang.

**DNB zal in haar beleidsuitingen in toenemende mate werken met een risicogebaseerde benadering, en ruimte geven voor innovatieve toepassingen.** DNB ondersteunt instellingen in de vorm van *guidance* over wat DNB van ze verwacht. Waar mogelijk zal DNB samen met onder toezicht staande instellingen onderzoeken welke situaties tot een laag risico of tot een hoog risico leiden, en hoe vertrouwen kan worden


gegeven en verkregen dat de juiste maatregelen voor de geconstateerde risico's worden genomen. Daarbij is er ruimte om innovatieve oplossingen toe te passen, zeker waar die effectiever zijn dan een traditionele aanpak. Waar de wet toepassing van een innovatieve oplossing formeel niet toestaat, terwijl toepassing het doel van de wet ondersteunt, wil DNB de ruimte onderzoeken, bijvoorbeeld door ook in samenspraak met de wetgever te kijken of nodeloze hindernissen kunnen worden weggenomen. Waar mogelijk zal DNB in beleidsuitingen aandacht besteden aan situaties van laag risico en welke beheersing daarin proportioneel is.

**DNB geeft instellingen ruimte om te experimenteren met digitale innovaties in het bestrijden van financieel-economische criminaliteit, specifiek met machine learning en de digitale identiteit.** Inzet van technieken als kunstmatige intelligentie kunnen risico-inschattingen verbeteren, en daarmee de effectiviteit en efficiëntie van klantonderzoeken en transactiemonitoring vergroten. En een digitale identiteit kan de identificatie en verificatie van klanten bijvoorbeeld drastisch vergemakkelijken. Hierdoor kunnen de (administratieve) lasten voor instelling en klant omlaag. Voorwaarde voor verantwoorde innovatie is wel dat de onderliggende Wwft-compliance processen op orde zijn, dat de IT-infrastructuur betrouwbaar is en dat de kwaliteit en beschikbaarheid van data geborgd zijn. Daarbij moet discriminatie worden voorkomen. Ook moeten er

waarborgen zijn voor privacy en gegevensbescherming, en voor de uitlegbaarheid van gebruikte modellen.

**Een effectieve aanpak van witwassen en terrorismefinanciering is alleen mogelijk als betrokken partijen samenwerken.** Het robuuste systeem van nationale samenwerking en coördinatie, zowel beleidsmatig als operationeel, wordt door de FATF als sterk punt benoemd. Toch kan de effectiviteit van de samenwerking verder worden vergroot. Dit vergt dat elke ketenpartner opereert vanuit het gedeelde doel van het voorkomen en bestrijden van misbruik van het financiële stelsel voor witwassen of terrorismefinanciering. Van daaruit kunnen concrete en meetbare operationele doelstellingen en prioriteiten worden bepaald, zodat er specifieke onderwerpen en risico's gezamenlijk worden aangepakt. Daarvoor moeten dan ook de benodigde middelen en menskracht beschikbaar zijn. Het Financieel Expertise Centrum vervult hierin een coördinerende rol.

**De effectiviteit van de keten van het melden en onderzoeken van ongebruikelijke transacties kan worden verhoogd.** De wetgever zou er voor kunnen kiezen instellingen te vragen niet al te melden wanneer transacties 'ongebruikelijk' zijn, maar de focus bij het melden te leggen op 'verdachte' transacties, waarbij de instelling vermoedt dat de handelwijze van de klant verband houdt met witwassen of het financieren van terrorisme. Dit kan de kwaliteit van de meldingen



verhogen en het aantal meldingen doen afnemen. De FIU kan zich dan concentreren op een goede doorlevering aan opsporingsinstanties. Daarmee zou Nederland ook minder afwijken van de internationale usance om verdachte transacties te melden.

**Het samenbrengen van data kan, mits er (privacy) waarborgen zijn ingericht, helpen om verdachte transacties te detecteren en risico-inschattingen te verbeteren.** Zo werken vijf Nederlandse banken samen door in samenhang hun transacties te monitoren op signalen van witwassen en terrorismefinanciering, onder de naam Transactie Monitoring Nederland. Uitbreiding van de mogelijkheden tot samenwerking en gegevensuitwisseling tussen instellingen is wenselijk, in combinatie met adequate (privacy) waarborgen. Deze samenwerking kan ook de efficiëntie van de transactiemonitoring vergroten als het voor instellingen mogelijk wordt deze werkzaamheden uit te besteden (met behoud van de verantwoordelijkheid bij de uitbestedende bank). Artikel 10 Wwft staat dat nu in de weg; DNB is voorstander van aanpassing van dit artikel zoals voorzien in het Wetsvoorstel plan van aanpak witwassen.

**Uitgebreidere terugkoppeling van de FIU aan de banken zou het draagvlak voor transactiemeldingen vergroten en de meldingen ook effectiever maken.** Banken hebben hun poortwachtersrol aangescherpt. Dat is bijvoorbeeld zichtbaar in het toegenomen aantal

meldingen van ongebruikelijke transacties bij FIU-NL. Voor de effectiviteit van hun analyses zouden banken er bij gebaat zijn als de FIU aan hen teruggeeft op welke basis transacties door de FIU als verdacht zijn aangemerkt. Op die manier kunnen banken gerichter zoeken naar transacties die aan witwassen of terrorisme gerelateerd kunnen zijn. Dit komt de effectiviteit van de keten ten goede. Ook verder in de keten kunnen feedback-loops de effectiviteit vergroten.

# Inleiding

De Nederlandse maatschappij en burgers moeten erop kunnen vertrouwen dat financieel-economische criminaliteit – in het bijzonder witwassen en terrorismefinanciering – in de financiële sector wordt tegengegaan, zonder dat de dienstverlening aan diezelfde burger in het geding komt. De maatschappelijke urgentie om actief financieel-economische criminaliteit te voorkomen en te bestrijden is groot. Witwassen ondergraaft immers het vertrouwen van de burger in de financiële sector. Criminele en terroristische organisaties en personen gebruiken het witgewassen geld voor eigen gewin en om verdere activiteiten te financieren. Uiteindelijk betaalt de 'gewone' burger de prijs. Niet alleen via hogere belastingen, maar ook doordat de samenleving onveiliger wordt en de rechtsstaat wordt ondermijnd.

DNB ziet erop toe dat financiële instellingen hun aanpak op financieel-economische criminaliteit op orde hebben, en draagt zo bij aan een schone en integere financiële sector. Dit blijft onverminderd nodig. Zowel de samenleving als de politiek vragen om een stevige en effectieve aanpak van financieel-

economische criminaliteit. Het toezicht hierop is dan ook door DNB aangemerkt als één van haar drie speerpunten.

Dit rapport besteedt in het bijzonder aandacht aan het toezicht op banken, die een spilfunctie vervullen in het financiële systeem. Handhavingsacties en hersteltrajecten hebben de inspanning van banken om witwassen en terrorismefinanciering te voorkomen vergroot. Banken zijn strenger aan de poort geworden, en onderwerpen hun klanten tegenwoordig intensiever aan nader onderzoek. Hierdoor kunnen risico's beter worden beheerst. Het beïnvloedt echter ook de bancaire dienstverlening. DNB ontvangt signalen dat het voor bepaalde zakelijke partijen en consumenten moeilijk is geworden om toegang te krijgen tot bankdiensten of te behouden.

Tegen deze achtergrond houdt DNB in dit rapport haar toezicht en beleid ten aanzien van het voorkomen van financieel-economische criminaliteit door banken tegen het licht.<sup>1</sup> Naast *deskresearch* zijn met betrokken partijen interviews afgenomen.

Daarnaast is additionele informatie verzameld met behulp van een vragenlijst die is beantwoord door de vier grootste banken in Nederland en contact gezocht met klanten van banken die meldingen hebben gedaan bij DNB. Om de effectiviteit en efficiëntie van de voorkoming en bestrijding van financieel-economische criminaliteit te vergroten is het van belang te bezien hoe de inspanningen van de sector daadwerkelijk risicogebaseerd kunnen worden en hoe risicogebaseerd toezicht van DNB daaraan kan bijdragen. De bevindingen uit dit rapport wil DNB verder bespreken in de vorm van rondetafelgesprekken met de sector en andere stakeholders.

Na een inleidende schets van het probleemveld (hoofdstuk 1) wordt achtereenvolgens ingegaan op de rol van de banken in het voorkomen en bestrijden van witwassen en terrorismefinanciering en de mogelijke neveneffecten daarvan (hoofdstuk 2), het toezicht van DNB (hoofdstuk 3), het perspectief dat inzet van technologie biedt (hoofdstuk 4), en de noodzaak tot intensieve samenwerking van alle betrokken partijen (hoofdstuk 5).

<sup>1</sup> Dit rapport richt zich op voorkoming en bestrijding van witwassen en terrorismefinanciering door banken. Andere integriteitsrisico's, waaronder de naleving van de sanctiewetgeving, zijn buiten *scope* geplaatst. Ook de rol van niet-bancaire instellingen blijft in dit rapport buiten beeld.



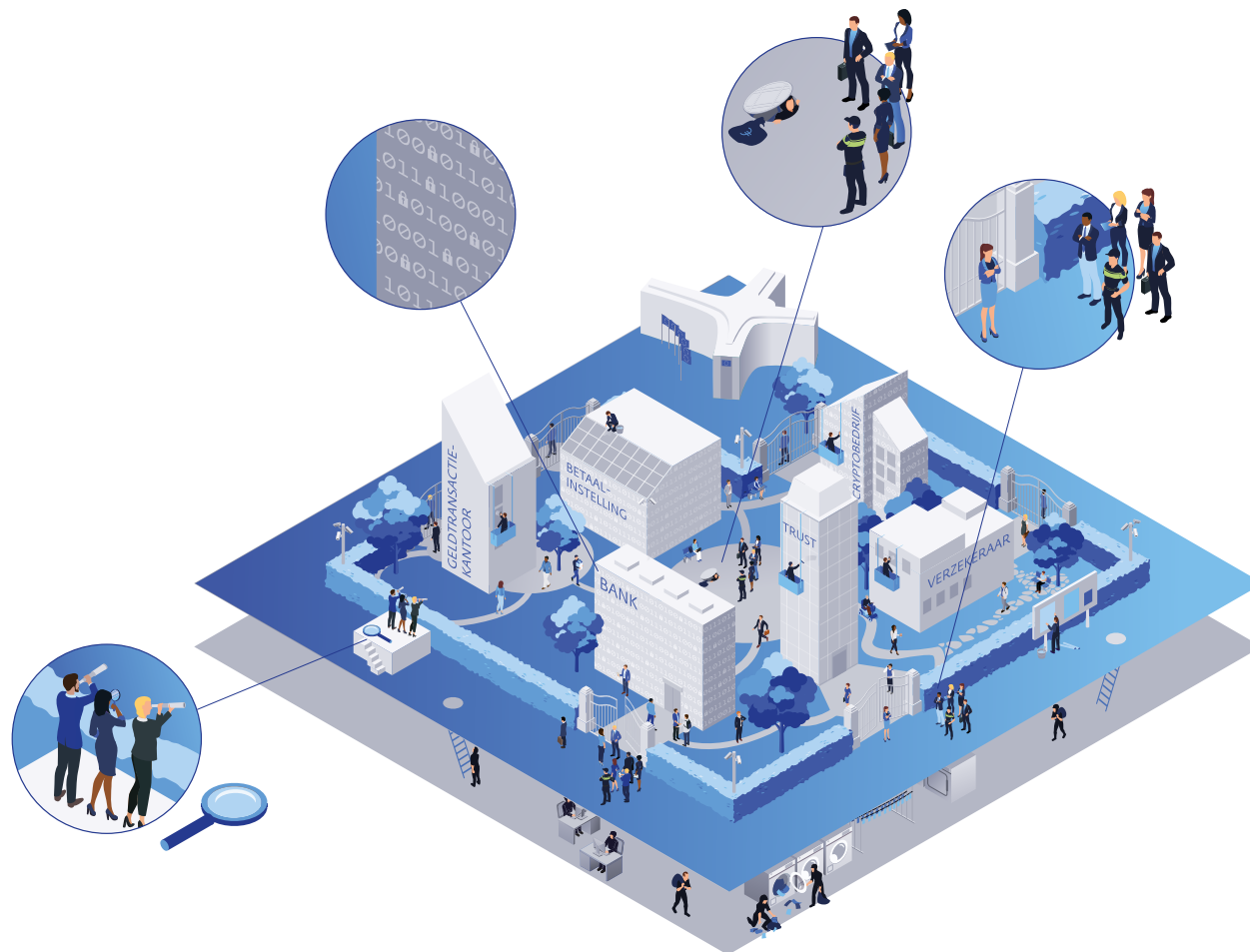
# 1 Witwassen en terrorismefinanciering: omvang en bestrijding

## 1.1 Witwassen en terrorismefinanciering in Nederland

**Criminele geldstromen vormen een maatschappelijk probleem.** Opbrengsten van criminele activiteiten worden witgewassen om ze te kunnen gebruiken in de legale economie. Witwassen is erop gericht om crimineel geld een ogenschijnlijk legale herkomst te geven. De ondermijnende invloed van de georganiseerde criminaliteit in Nederland is reden tot zorg. De onderliggende financiële stromen vormen hierin een belangrijk element. Een specifieke vorm van financieel-economische criminaliteit die van de financiële infrastructuur gebruikmaakt is terrorismefinanciering, wat een verzamelnaam is voor handelingen die het doel hebben om alle vormen van bijstand aan terroristische activiteiten mogelijk te maken.

### **Witgewassen geldstromen zijn omvangrijk.**

Naar zijn aard is de omvang van witwassen en terrorismefinanciering moeilijk in kaart te brengen. Schattingen wijzen uit dat tussen de 2 en 5 procent van het wereldwijde bruto binnenlands product op jaarbasis wordt witgewassen.<sup>2</sup> Een onderzoek schat dat in Nederland bijna EUR 16 miljard aan crimineel geld wordt verdiend.<sup>3</sup> Volgens dit onderzoek verdween ongeveer de helft van het geld naar het buitenland,



<sup>2</sup> M. Tiwari, A. Gepp & K. Kumar (2020), *A review of money laundering literature: the state of research in key areas*, Pacific Accounting Review, Vol. 32 No. 2, p. 271-303.

<sup>3</sup> Bijna € 13 mrd wordt er jaarlijks witgewassen in Nederland (fd.nl). Gebaseerd op data van de FIU over de periode 2009-2014. Zie ook B. Unger e.a. (2018), *Aard en omvang van criminele bestedingen 2018* (wodc.nl).



← ↩

maar kwam ook een bedrag van naar schatting bijna EUR 5 miljard crimineel geld uit het buitenland naar Nederland. De goede staat van de (digitale) infrastructuur en de kwaliteit van de juridische en financiële dienstensector in Nederland ondersteunen niet alleen de reguliere economie maar zijn ook aantrekkelijk om witwassen te faciliteren. Publicaties als de Panama Papers, de Paradise Papers en FinCEN Files laten zien dat witwassen in Nederland relatief veel voorkomt. Over de omvang van terrorismefinanciering is minder bekend. De Nederlandse National Risk Assessment Terrorismefinanciering 2019 beschrijft 12 veroordelingen voor het leveren van financiële ondersteuning aan vrienden of familieleden die naar strijdgebieden zijn gereisd waar terroristische activiteiten plaatsvinden. In 2020 registreerde de Financial Intelligence Unit Nederland (FIU-NL) 4412 verdachte transacties gerelateerd aan terrorisme, ruim 4% van het totaal aantal verdachte transacties.<sup>4</sup>

#### **Het voorkomen en bestrijden van witwassen en terrorismebestrijding kent een internationaal kader.**

De basis voor de aanpak zijn de aanbevelingen van de Financial Action Task Force (FATF), een invloedrijke internationale organisatie waar Nederland bij is aangesloten. Ook op Europees niveau wordt veel samengewerkt (zie verder hoofdstuk 3). Een internationale aanpak van financieel-economische

criminaliteit is essentieel omdat geldstromen ook tussen landen plaatsvinden, verhullende constructies grensoverschrijdend worden opgezet, en organisaties die criminele activiteiten ondernemen of zich bezighouden met terrorismefinanciering in veel gevallen internationaal

opereren. Om de consistentie en effectiviteit te bevorderen van het nationale beleid om witwassen en terrorismefinanciering tegen te gaan, worden periodiek internationale evaluaties uitgevoerd. Dat is in Nederland in 2021-2022 driemaal het geval (Box 1).

#### **Box 1 Internationale evaluaties Nederlands anti-witwassen/anti-terrorisme-financieringsbeleid**

De Financial Action Task Force (FATF) voerde in 2021-22 een evaluatie uit naar het Nederlandse beleid om witwassen en terrorismefinanciering tegen te gaan (FATF (2022), [The Netherlands - Mutual Evaluation Report](#)). De FATF is de intergouvernementele organisatie die de internationale standaarden opstelt, die omgezet worden in nationale (en Europese) regelgeving. In haar beoordeling constateert de FATF dat Nederland aanzienlijke verbeteringen in zijn raamwerk heeft aangebracht, en goed voldoet aan de FATF-standaarden.

Sterke punten zijn onder meer de mate van nationale samenwerking en coördinatie, zowel beleidsmatig als operationeel, en het gebruik van data en 'intelligence'. Als verbeterpunten worden onder meer de aanpak van misbruik van rechtspersonen en versterking van risicogebaseerd toezicht genoemd.

De Raad van Europa evalueert in opdracht van de Europese Commissie hoe EU-lidstaten de verplichtingen die voortvloeien uit de vierde anti-witwasrichtlijn uitvoeren in de praktijk. In 2022 zal een (geanonimiseerd) EU-breed rapport worden uitgebracht.

Samen met zes toezichthouders uit andere EU-landen is DNB in 2021 onderworpen aan een AML/CFT implementatie review door de Europese bankenautoriteit (EBA). De review richt zich op de doeltreffendheid van het AML/CFT toezicht op banken. In 2022 zal een (geanonimiseerd) samenvattend rapport over de betreffende zeven landen worden gepubliceerd.

DNB hecht groot belang aan deze evaluaties. Ze heeft intensief samengewerkt aan de voorbereiding, en zal de aanbevelingen in haar toezichtaanpak opnemen.

<sup>4</sup> [FIU-Nederland Jaaroverzicht 2020](#).

←

↩

**Ondanks het beleidsraamwerk met wereldwijde aanbevelingen voor regelgeving blijft een effectieve aanpak van financieel-economische criminaliteit uitdagend.** Geschat wordt dat autoriteiten wereldwijd 0,05% van de illegaal verkregen gelden afpakken.<sup>5</sup> In Nederland is in 2021 door middel van strafrechtelijke incasso door het Openbaar Ministerie (OM) EUR 291 miljoen (dus 1,8% van de eerdergenoemde 16 miljard) afgepakt.<sup>6</sup> Dit suggereert dat in Nederland naar verhouding meer geld wordt afgepakt dan wereldwijd. Tegelijkertijd is 1,8% nog steeds relatief weinig.

## 1.2 Voorkomen en bestrijden van financieel-economische criminaliteit

De Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) vormt de wettelijke basis. In de Wwft is de Europese Anti-Money Laundering Directive (AMLD) geïmplementeerd. De AMLD is een Europese richtlijn gericht op het voorkomen van misbruik van het financiële stelsel voor witwassen en financieren van terrorisme, die in lijn is met de aanbevelingen van de FATF. In de Wwft staat dat instellingen moeten voorkomen dat criminelen via hun diensten criminele gelden in het financieel systeem kunnen brengen. Dit voorkomen doen zij, kort gezegd, door:

- 1) onderzoek te doen naar hun (nieuwe) klanten;
- 2) transacties te monitoren; en 3) ongebruikelijke

transacties te melden bij de FIU-NL. Op deze manier fungeren instellingen als 'poortwachter': ze voorkomen dat vermogen met een criminele herkomst zich mengt in het financieel stelsel en helpen om financiële stromen te detecteren en te stoppen die ongewenst toch in dat stelsel terecht zijn gekomen.

**In het cliëntenonderzoek wordt vastgesteld wie de (potentiële) klanten zijn, waar het geld vandaan komt of naar toe gaat, en waarvoor het geld wordt gebruikt.** De instelling dient hiervoor gegevens te verzamelen over de klant. De Wwft geeft aan wat het resultaat van het cliëntenonderzoek moet zijn, de instelling bepaalt vervolgens zelf hoe dit bereikt wordt.

Geeft het cliëntenonderzoek onvoldoende duidelijkheid over de klant, de identiteit, en herkomst van gelden, of is het ingeschatte risico op criminele herkomst of crimineel gebruik te groot, dan mag de instelling geen werkzaamheden uitvoeren voor deze klant. Dit weert kwaadwillenden en criminelen dus bij de poorten van het financiële systeem.

Aan de hand van transactiemonitoring worden ongebruikelijke transacties gedetecteerd en gemeld: transacties die niet passen in het normale verloop van een rekening. Of een transactie ongebruikelijk is, bepaalt een instelling enerzijds door middel van een lijst met

objectieve indicatoren op basis waarvan meldingen worden gedaan. Deze indicatoren kunnen per categorie instelling verschillen. Vaak gaat het om karakteristieken zoals een transactie die boven een bepaalde drempelwaarde komt. Anderzijds wordt de ongebruikelijkheid van een transactie bepaald door de *expert opinion* van analisten bij instellingen: de transactie geeft wel of geen aanleiding om te veronderstellen dat deze verband kan houden met witwassen of financieren van terrorisme. Hier komen zogenaamde 'subjectieve meldingen' uit voort. In 2021 hebben Wwft-instellingen aan de FIU-NL 1,2 miljoen ongebruikelijke transacties gemeld (tabel 1).<sup>7</sup> Ruim 50% van de meldingen komt van betaalinstanties waaronder geldtransferbedrijven, 25% van crypto-dienstverleners en ruim 20% van banken. De overige meldingen zijn verdeeld over een divers aantal andere poortwachters, zoals wisseldiensten, cryptobeurzen, accountants, notarissen en autohandelaren.

<sup>5</sup> R. Pol (2020), *Anti-money laundering: The world's least effective policy experiment? Together, we can fix it* (tandfonline.com), Policy Design and Practice, 3:1, p. 73-94.

<sup>6</sup> Openbaar Ministerie jaarbericht 2021, Kerncijfers 2021, tabel Afpakken.

<sup>7</sup> FIU-Nederland Jaaroverzicht 2021.

Tabel 1 Aantal ongebruikelijke en verdacht verklaarde transacties

	2017	2018	2019	2020	2021
<b>Ongebruikelijke transacties</b>	361.015	394.743	541.236	722.239	1.230.411
waarvan gemeld door:					
banken	22.789	67.524	147.952	245.143	262.991
betaaldienstverleners	309.619	291.589	350.775	422.878	638.218
cryptodienstverleners				7.309	301.928
overig	28.607	35.630	42.509	54.218	27.274
gedeelte op grond van:					
subjectieve factoren	68%	69%	59%	57%	45%
objectieve factoren	32%	31%	41%	43%	55%
<b>Verdachte transacties</b>	40.546	57.950	39.544	103.947	96.676
waarvan gemeld door:					
banken	4.163	15.437	12.919	40.382	47.325
betaaldienstverleners	33.533	39.239	21.996	56.866	38.513
cryptodienstverleners				3	5.860
overig	2.850	3.274	4.629	6.699	4.978

Bron: FIU Nederland Jaaroverzichten 2019, 2020, 2021. Ongerekend 'wettelijke indicator objectief 02' (de lijst met daarop door de Europese Commissie aangewezen risicolanden).

**In de afgelopen jaren zijn betekenisvolle verbeteringen gerealiseerd in het tegengaan van witwassen en terrorismefinanciering.** De Algemene Rekenkamer oordeelt dat er op dit dossier duidelijk vooruitgang is geboekt.<sup>8</sup> Dit blijkt bijvoorbeeld uit de toegenomen activiteiten in de keten. In 2021 meldden instellingen drie-en-een-half keer zoveel ongebruikelijke transacties als in 2017; het aantal door de FIU als verdacht aangemerkte transacties nam in die periode met 138% toe. Ook de instroom van witwasmisdrijfzaken bij het OM (+155% tussen 2017 en 2021<sup>9</sup>) en het aantal veroordelingen bij de rechter (van +/- 600 veroordelingen in 2016 naar +/- 1100 veroordelingen in 2020<sup>10</sup>) zijn duidelijk gestegen.

**Toegenomen inspanning door banken heeft als effect gehad dat meldingen door banken aanzienlijk zijn toegenomen.** De afgelopen jaren hebben banken hier beduidend meer capaciteit op ingezet. Mede daardoor hebben banken in 2021 1054% meer meldingen van ongebruikelijke transacties gedaan bij de FIU dan in 2017. Ook het aantal door de FIU als verdacht aangemerkte transacties afkomstig van banken is in die periode toegenomen, met 1036%.

<sup>8</sup> Algemene Rekenkamer (2022), Bestrijden witwassen deel 3: stand van zaken 2021.  
<sup>9</sup> Openbaar Ministerie Jaarbericht 2021, Kerncijfers 2021, tabel Instroom misdrijfzaken.  
<sup>10</sup> Algemene Rekenkamer (2022), figuur 5.

← ↶

**Daarbij is toegang tot de bancaire sector moeilijker geworden.** De toegang tot de bancaire infrastructuur is een stuk strikter geworden. Banken hebben hun beleid met betrekking tot acceptatie en het afscheid nemen van klanten aangescherpt. Dit komt ook tot uiting in de toename van het aantal klachten en rechtszaken, waarin de beslissingen van banken worden aangevochten. Om meer zicht te krijgen op het aangescherpte beleid van banken met betrekking tot acceptatie en het afscheid nemen van klanten, heeft DNB ten behoeve van dit rapport een uitvraag gedaan bij banken (zie hiervoor hoofdstuk 2). Met deze *factfinding* wil DNB eraan bijdragen dat het debat over het voorkomen en bestrijden van witwassen en terrorismefinanciering meer op basis van kwantitatieve feiten en minder op basis van kwalitatieve anekdotische beelden wordt gevoerd.

**De wetenschappelijke literatuur laat voorzichtig positieve effecten van anti-witwasbeleid zien.** Zo laat onderzoek in Nederland zien hoe de invoering van de vierde anti-witwasrichtlijn (AMLD4) in 2015 het de witwasnetwerken moeilijker heeft gemaakt.<sup>11</sup> De gedachte is hier dat de Richtlijn witwassen bemoeilijkt, waardoor criminelen nieuwe methodes,

samenwerkingsverbanden en structuren moeten vinden om hun doelen te bereiken. Onderzoek toont tevens aan dat de AMLD4 een positief effect heeft op de beurswaardering van Europese banken.<sup>12</sup> Ook is aangetoond dat de toepassing van anti-witwasregelgeving een positief effect heeft op de ontwikkeling van de financiële sector.<sup>13</sup> Tevens laat een studie, uitgevoerd in bijna 100 landen, zien dat anti-witwasregelgeving aantoonbaar neerwaarts effect heeft op hoeveel gelden er worden witgewassen.<sup>14</sup>

**DNB is toezichthouder op de naleving van de Wwft door financiële instellingen zoals banken, verzekeraars, trustkantoren, aanbieders van cryptodiensten en betaalinstellingen.** De andere Wwft-toezichthouders zijn: de Autoriteit Financiële Markten (AFM), het Bureau Financieel Toezicht (BFT), het Bureau Toezicht Wwft (BTWwft), de Kansspelautoriteit (Ksa) en de deken van de Nederlandse Orde van Advocaten (NOvA). Deze toezichthouders vormen samen de bestuursrechterketen in de bestrijding van financieel-economische criminaliteit. Daarnaast zijn er relevante autoriteiten uit de strafrechterketen betrokken: de FIU-NL, de Fiscale Inlichtingen en Opsporingsdienst (FIOD), de politie en het Openbaar Ministerie (OM).

De FIU-NL analyseert de meldingen van de poortwachters. Van de 1,2 miljoen gemelde ongebruikelijke transacties in 2021 zijn er bijna 97.000 transacties als 'verdacht' aangemerkt. De FIU-NL classificeert transacties als verdacht op basis van eigen onderzoek en naar aanleiding van *hits* bij de politie, het OM en het CJIB. Deze verdachte transacties worden doorgegeven aan opsporingsinstanties zoals de FIOD en de politie, die onderzoeken of mogelijk sprake is van strafbare feiten. Het OM besluit uiteindelijk of vervolging wordt ingesteld. De deelnemers aan de bestuursrechterketen en de strafrechterketen worden samen de ketenpartners genoemd en streven naar een integrale aanpak van financieel-economische criminaliteit.



<sup>11</sup> P. Gerbrands, B. Unger, M. Getzner & J. Ferwerda (2022), *The effect of anti-money laundering policies: an empirical network analysis* (springeropen.com), EPJ Data Science, 11:15.

<sup>12</sup> A. Premti, M. Jafarinejad, & H. Balani (2021), *The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks* | Elsevier Enhanced Reader, Research in International Business and Finance, 57.

<sup>13</sup> I. Ofouda, J. Abor, J & E. Agbloyor (2020), *Anti-money laundering regulations and financial sector development*, International Journal of Finance & Economics.

<sup>14</sup> A. Chong & F. Lopez-De Silanes (2015), *Money Laundering and Its Regulation*, Economics & Politics, Vol. 27 Issue 1.

←

↶

**Het overtreden van de Wwft kan zowel bestuursrechtelijke als strafrechtelijke consequenties hebben.**

De toezichthouder kan bestuursrechtelijk ingrijpen, primair om herstel te bewerkstelligen zodat de instelling in kwestie voldoet aan de Wwft. Hiervoor heeft de toezichthouder ook formele (wettelijke) instrumenten tot haar beschikking, bijvoorbeeld de aanwijzing of de last onder dwangsom. Op grond van een van de laatste wijzigingen van de Wwft moet de toezichthouder een formele maatregel in beginsel publiceren. Dit geldt ook als er een boete wordt opgelegd. Een boete heeft daarbij een bestraffend karakter. Omdat overtreding van Wwft-bepalingen ook kan kwalificeren als economisch delict, zal in het geval van een mogelijke boete een keuze gemaakt moeten worden tussen een strafrechtelijke of een bestuursrechtelijke afdoening. De keuze voor het strafrecht dan wel het bestuursrecht kan afhangen van de zwaarte van het economische delict. Gevallen van opzet of grove schuld zullen (sneller) in het strafrecht behandeld worden. Het OM heeft hierbij het primaat.

Samenwerking tussen ketenpartners is van belang om witwassen en terrorismefinanciering te voorkomen en te bestrijden. Eén van de oudste samenwerkingsverbanden voor het bestrijden van financieel-

economische criminaliteit is het Financieel Expertise Centrum (FEC). In het FEC werken alle hierboven genoemde ketenpartners samen. In FEC-verband wordt informatie uitgewisseld, kennis overgedragen en worden gezamenlijke projecten uitgevoerd. Dat gebeurt al lange tijd door samenwerkende publieke partners en sinds een aantal jaren ook door samenwerking met enkele grote financiële instellingen. Een voorbeeld is de *Serious Crime Task Force* waarbinnen de politie, het OM, de FIU-NL en de FIOD samen met een aantal grote banken aan de gezamenlijke aanpak van ondermijnende criminaliteit werken.

### 1.3 Een risicogebaseerde aanpak

**Een risicogebaseerde aanpak vormt de kern van de internationale en nationale kaders voor het voorkomen en bestrijden van witwassen en terrorismefinanciering.** Gebaseerd op een analyse van de risico's dienen landen een risicogebaseerde aanpak te hanteren die waarborgt dat maatregelen om witwassen en terrorismefinanciering tegen te gaan evenredig zijn aan de geïdentificeerde risico's.<sup>15</sup> Waar grotere risico's worden geïdentificeerd moeten de landen deze in het regelgevend kader met bijbehorend strikte maatregelen adresseren. Waar risico's lager zijn, volstaan eenvoudiger maatregelen. Deze risico-gebaseerde benadering ligt ook ten grondslag aan de

Europese (AMLD) en Nederlandse (Wwft) regelgeving.<sup>16</sup> Zo bepaalt de Wwft dat op grond van een basisonderzoek (zie verder hoofdstuk 2) een instelling het cliëntenonderzoek aantoonbaar afstemt op de risicogevoeligheid voor witwassen of terrorismefinanciering bij elk type cliënt, zakelijke relatie, product of transactie. Ook voor de toezichthouders geldt dat ze hun taak op een op risicogebaseerde wijze uitvoeren (zie verder hoofdstuk 3).

<sup>15</sup> Zie onder meer de aanbevelingen van de FATF en de richtlijnen van de EBA.

<sup>16</sup> Zie onder meer de memorie van toelichting bij de wijziging van de Wwft, Kamerstukken II 2018/2019 35245, nr. 3.

← ↻

**Een risicogebaseerde aanpak is ook in bredere zin gebruikelijk bij toezichthouders.** Het centrale idee is dat er het meeste aandacht is voor de grootste risico's, en dat het toezicht effectiever wordt als de middelen van de toezichthouder juist op deze grote risico's worden ingezet. Toezichtsexpert Malcolm Sparrow omschrijft de kern als volgt: *"Pick important problems, fix them, and then tell everyone"*.<sup>17</sup> Dit zorgt voor meer maatschappelijke impact, met een effectievere inzet van de beperkte capaciteit van de toezichthouder. Of zoals de WRR stelt: *"Het idee achter risicogericht toezicht is dat de toezichthouder niet meer bij alle onder toezicht staande organisaties controleert, maar alleen kijkt naar een selectie daarvan op basis van risicoanalyse en risicoprofielen. Het toezicht wordt intensiever daar waar de risico's groter zijn."*<sup>18</sup>

De risicogebaseerde aanpak bestaat in grote lijnen uit drie stappen:

1. *Het identificeren van risico's:* in deze fase kijkt de toezichthouder welke risico's er te vinden zijn voor de te realiseren publieke doelen die voortvloeien uit haar (juridische) mandaat.
2. *Het classificeren van risico's:* na identificatie van risico's moet er een bepaalde ordening in de risico's gemaakt worden, om te bepalen aan welke risico's de toezichthouder zijn aandacht besteedt. Vaak

wordt hier zowel gekeken naar de impact die het risico kan hebben (hoeveel schade kan er aan de publieke doelen worden aangericht?), en de kans dat het risico zich voordoet (is het een *black swan* risico, of gaat het zich vrijwel zeker voordoen?).

3. *Het mitigeren van risico's:* als vervolgens de aan te pakken risico's bekend zijn gaat de toezichthouder kijken welk instrumentarium hij moet inzetten om de betrokken instelling deze risico's te laten beheersen. Dit betekent soms dat eerst gekeken wordt naar informele interventies, voordat 'zwaardere' handhavingstoezicht wordt ingezet. Maar er kan ook aanleiding zijn om meteen een zwaardere maatregel in te willen zetten.

DNB onderschrijft deze risicogebaseerde benadering, en gebruikt deze als uitgangspunt voor het toezicht op de naleving van Wft en Wwft (zie verder hoofdstuk 3).

<sup>17</sup> M. Sparrow (2000), *The Regulatory Craft: controlling risks, solving problems and managing compliance*. Brookings Institution.

<sup>18</sup> WRR (2013), *Toeziën op publieke belangen. Naar een verruimd perspectief op rijksstoezicht*.

## 2 De rol van banken als poortwachter

**Banken zijn een belangrijke poortwachter omdat ze toegang verschaffen tot essentiële financiële diensten en de spil zijn in het financiële transactie-verkeer.**

Banken zijn bij vrijwel elke financiële transactie in meer of mindere mate betrokken. De maatregelen die banken nemen om misbruik van de bancaire dienstverlening tegen te gaan, kunnen dan ook een grote bijdrage leveren aan het voorkomen en bestrijden van witwassen en terrorismefinanciering. Dit geeft een belangrijke verantwoordelijkheid. De invulling van de poortwachtersrol van de banken brengt met zich dat ook bonafide burgers en bedrijven te maken hebben met deze maatregelen. Streven is daarbij dat de dienstverlening aan burgers en bedrijven zo min mogelijk in het geding komt.

**Ten behoeve van deze analyse hebben banken en klanten gegevens verstrekt.** Om inzicht te krijgen in de vraag hoe banken hun rol als poortwachter inrichten, welke kosten daarmee gepaard gaan en wat daarvan de gevolgen voor de klanten zijn, is een enquête onder de vier grootste banken gehouden.<sup>19</sup> DNB heeft ook gesprekken gevoerd met deze banken en met enkele andere stakeholders. In het vervolg van het hoofdstuk wordt vooral geput uit de resultaten van deze enquête.

Voorts is gebruik gemaakt van informatie van klanten van banken die in het eerste halfjaar van 2022 contact hebben gezocht met de Infodesk van DNB over de maatregelen tegen witwassen en terrorisme. DNB heeft die klanten telefonisch om nadere informatie gevraagd over hun ervaringen.

### 2.1 Inspanningen van banken om witwassen en terrorismefinanciering tegen te gaan

**In de afgelopen jaren heeft DNB geconstateerd dat een deel van de bancaire sector in onvoldoende mate de Wwft heeft nageleefd.** DNB heeft dan ook herhaaldelijk handhavend moeten optreden, en enkele banken zijn ook strafrechtelijk vervolgd, met aanzienlijke schikkingsmaatregelen tot gevolg. Bij 28 banken - waaronder de grotere banken - lopen hersteltrajecten om de tekortkomingen in het verrichten van klantonderzoeken en in het monitoren en melden van transacties te verhelpen.<sup>20</sup>

**De banken hebben inmiddels hun inspanningen en investeringen op dit vlak aanzienlijk vergroot.**

Volgens bovengenoemde enquête bedroegen in 2021 de kosten voor het bestrijden van witwassen en terrorismefinanciering 8% van de totale administratieve

kosten van de vier grootste banken. Dit betrof ruim EUR 1,1 miljard, waarvan een kwart was toe te schrijven aan hersteltrajecten. Het overgrote deel van de kosten betreft loonkosten voor de ruim 10.000 FTE die zijn ingezet op het voorkomen van witwassen en terrorismefinanciering.<sup>21</sup>

**De toegenomen inspanningen worden ook zichtbaar in het aantal meldingen van ongebruikelijke transacties.**

Waar banken in 2017 nog bijna 23.000 ongebruikelijke transacties meldden bij FIU-NL, waren dit er in 2021 bijna 263.000 (zie tabel 1 in hoofdstuk 1). Banken ervaren hierbij tegelijkertijd dat de opvolging van deze meldingen achterblijft en dat de meldingen voor hen niet tot nauwelijks zichtbaar resulteren in strafrechtelijke trajecten. Ook geven banken aan dat de terugkoppeling vanuit FIU-NL onvoldoende toegevoegde waarde biedt voor het kunnen aanscherpen van beleid, procedures en maatregelen. Voor de effectiviteit van hun analyses zouden banken er bij gebaat zijn als de FIU aan ze terugmeldt op welke basis transacties door de FIU als verdacht zijn aangemerkt en, waar mogelijk, welke resultaten opsporing heeft behaald met behulp van de gemelde transacties.

<sup>19</sup> Het gaat om de vier grootste banken afgemeten aan het aantal klanten. In 2016 is over hetzelfde onderwerp ook een uitvraag gedaan. De resultaten zijn beperkt vergelijkbaar, op een enkel punt vindt een vergelijking plaats.

<sup>20</sup> DNB brief aan de minister van Financiën over de casus ABN Amro Bank NV

<sup>21</sup> Voor de bancaire sector als geheel bedroegen de kosten in 2021 bijna EUR 1,4 miljard, en het aantal ingezette fte bijna 13.000.

**De klanten van de banken merken ook dat banken hun aanpak hebben aangescherpt.** Zo wordt er meer informatie bij hen opgevraagd en nemen banken afscheid van klanten die bijvoorbeeld de gevraagde informatie niet verschaffen of die buiten de *risk appetite* van de bank vallen. Het aantal klanten aan wie dienstverlening is beëindigd of aan wie wordt besloten geen diensten te verlenen is dan ook sinds 2016 toegenomen. Hierna wordt nader ingegaan op deze gevolgen.

## 2.2 Gevolgen van het aangescherpte beleid van banken

### 2.2.1 Gevolgen voor de klantacceptatie

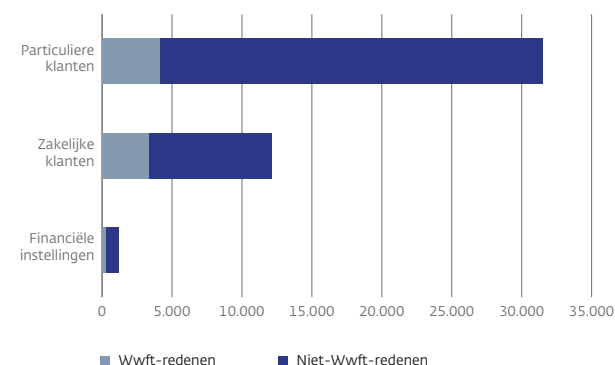
**In hun rol als poortwachter waren banken criminele geldstromen uit het financiële systeem.** Banken besluiten dan om klanten bij wie het risico té hoog is dat zij bij dergelijke geldstromen betrokken zijn, niet (langer) toe te laten tot het systeem of bepaalde diensten niet te verlenen. Dit past bij hun taak als poortwachter. Conform het gedachtegoed van de Wwft dient de bank zich daarbij te baseren op een risico-inschatting. De bank kan immers niet zelf volledig vaststellen of sprake is van een criminele geldstroom. De bank móet de risico-inschatting maken, en daarop handelen. Bij onderschatting van de risico's kan onbedoeld witwassen of terrorismefinanciering worden gefaciliteerd. Maar het kan ook gebeuren dat klanten onnodig worden geweerd. Deze onnodige *de-risking* is ongewenst omdat

bonafide klanten dan geen toegang meer hebben tot essentiële financiële diensten.

**Banken nemen vaak om andere redenen afscheid van klanten dan vanwege risico's op witwassen of terrorismefinanciering.** In 2021 hebben de vier banken tezamen met bijna 45.000 klanten de relatie beëindigd (figuur 1). In 17% van de gevallen, 7.700 klanten, was dit vanwege risico's op witwassen of terrorismefinanciering. Ten opzichte van 2016 is dit volgens een ruwe schatting ongeveer een verdubbeling; de toename betreft vooral het zakelijke segment. Voorbeelden van zulke 'Wwft-redenen' zijn dat een klant buiten de risicobereidheid van een bank valt of niet mee wil werken aan het cliëntenonderzoek. Dit betrof ruim 4.100 particulieren, 0,02% van het totaal aantal particuliere klanten aan het eind van 2020.<sup>22</sup> Met 3.600 zakelijke klanten (inclusief financiële instellingen), 0,17% van het totaal aan zakelijke klanten, is de relatie in 2021 om Wwft-redenen beëindigd. Naast de 'Wwft-redenen' zijn er ook andere redenen om de bankrelatie te beëindigen, zoals betrokkenheid bij fraude, en in het geval van zakelijke klanten ook het niet (meer) passen in het commerciële beleid van de bank of vanwege milieugerelateerde of maatschappelijke factoren. Onder dit laatste vallen bijvoorbeeld risico's op ernstige milieuschade of mensenrechtenschendingen.

**Figuur 1 Aantal klanten waar in 2021 afscheid is van genomen**

Uitgesplitst naar onderliggende reden



Toelichting: op basis van gegevens van de vier grootste banken. Wwft-redenen: klant past niet binnen integrity risk appetite m.b.t. naleving Wwft, klant non-coöperatief, bank kon niet voldoen aan wettelijke eisen m.b.t. cliëntenonderzoek, overig Wwft gerelateerd. Niet-Wwft-redenen o.a. fraude, reputatierisico bank, commerciële redenen, milieugerelateerde of maatschappelijke factoren.

**Bij het beëindigen van klantrelaties lijkt er weinig verband met de risicocategorie waarin die klant was ingedeeld, hetgeen kan duiden op een gebrekkige risicoclassificatie.** Banken schatten aan de hand van hun klantenonderzoek het risico in dat een klant betrokken raakt bij witwassen of terrorismefinanciering. Op basis daarvan worden ze ingedeeld in een risicocategorie: laag of verlaagd, midden of normaal, en hoog of verhoogd. Daarnaast is er de categorie 'onacceptabel', waarbij de klantrelatie zo snel mogelijk wordt beëindigd. Kijkend naar de verdeling

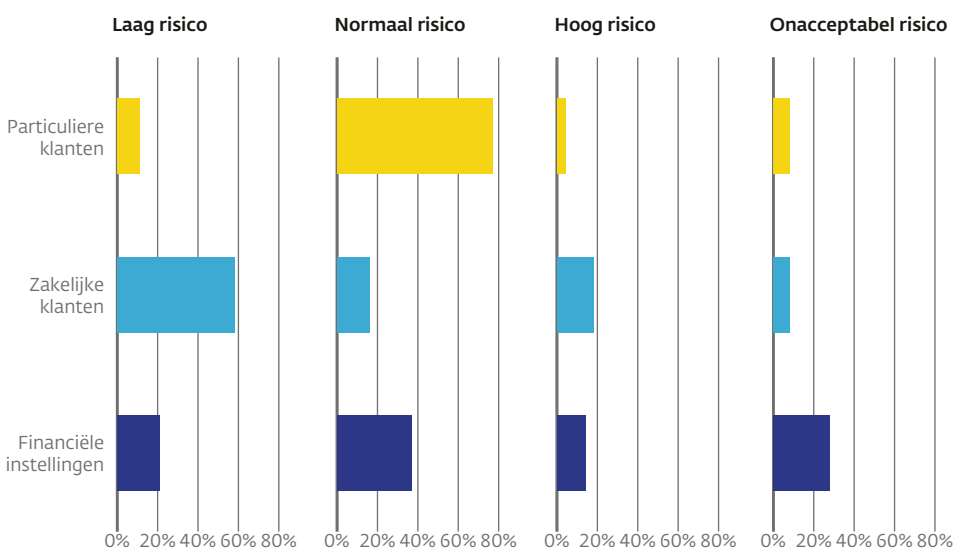
<sup>22</sup> Het zal voorkomen dat een persoon of bedrijf bij meerdere banken klant is. Deze klant komt dus bij meerdere banken voor als bestaande klant of als klant waarmee de relatie is beëindigd.



naar risicocategorie van bankklanten waar in 2021 vanwege Wwft-redenen afscheid van is genomen, is te zien dat veel van die klanten niet waren ingeschat als hoog risico, maar als laag of midden (figuur 2). Geconstateerde risico's op witwassen en terrorismefinanciering deden zich dus ook voor bij klanten die aanvankelijk als laag of normaal risico werden gezien.

**Figuur 2** Verdeling van klanten waar in 2021 om Wwft-redenen afscheid van is genomen per risicocategorie

In procenten van de klantengroepen

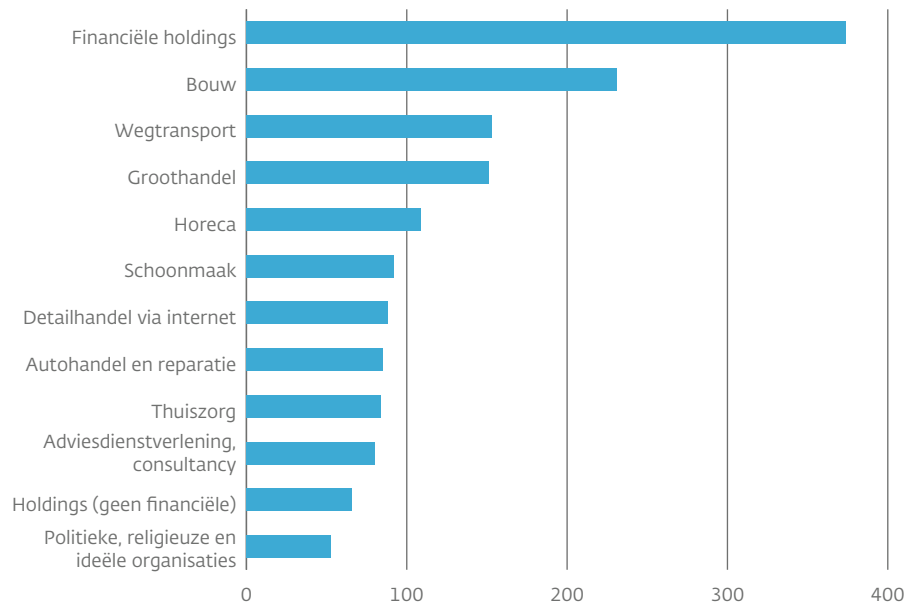


Toelichting: op basis van gegevens van de vier grootste banken. De totalen tellen per klantgroep op tot 100%..

**Met financiële holdings, bouwbedrijven, transport-bedrijven en groothandelaren is de relatie relatief vaak beëindigd vanwege risico's op witwassen en terrorismefinanciering (figuur 3).** Ten opzichte van het totaal aantal bankklanten in deze sectoren betreft het minder dan 0,5% van de gevallen. Terwijl het aantal beëindigingen beperkt is ten opzichte van het totale klantenbestand, is tussen sectoren variatie in het aantal

beëindigingen. De relatie met financiële holdings is het vaakst beëindigd met 374 gevallen, gevolgd door 231 gevallen in de bouw, 153 gevallen in de transportsector en 151 groothandelaren. Ten opzichte van het totaal aantal klantrelaties in de betreffende sector gaat het om 0,13% in de bouw en 0,42% in de transportsector.

**Figuur 3** Aantal zakelijke klanten waar in 2021 om Wwft-redenen afscheid van is genomen per sector



Toelichting: op basis van gegevens van de vier grootste banken. Betreft de 12 grootste sectoren qua aantal klanten waarvan afscheid is genomen. In enkele gevallen zijn kleinere sectoren geclusterd.

**De reden om over te gaan tot het beëindigen van dienstverlening verschilt per geval.** Klantkenmerken die hierbij veelvuldig naar voren komen zijn negatieve berichten over de klant uit de media of andere bronnen, of toegenomen risico's door complexe, ongebruikelijke of onverwacht grote transacties. Daarnaast is het opereren in sectoren met een verhoogd risico op witwassen of terrorismefinanciering een vaak genoemd klantkenmerk, net als relaties met landen die worden gezien als een verhoogd risico op witwassen/terrorismefinanciering. Tot slot betreft het in een aantal gevallen klanten die gevraagde informatie of documentatie niet aanleveren of onvoldoende duidelijke binding hebben met Nederland.

Hoewel de Wwft vereist dat in bepaalde gevallen de bank de relatie *moet* beëindigen, blijkt dit in de praktijk niet altijd haalbaar. De jurisprudentie op dit terrein ontwikkelt zich, maar banken zien dat klanten relatief vaak het beëindigen van de bankrelatie succesvol kunnen aanvechten bij de rechter: het feit dat banken een nutsfunctie hebben en klanten waarschijnlijk moeite zullen hebben elders een rekening te krijgen maakt dat rechters geregeld (maar zeker niet altijd) verbieden om afscheid te nemen van klanten. De 'lat' om de relatie te kunnen beëindigen ligt hoog, en dat maakt dat de 'controle aan de poort' sterker wordt.

Er is bij banken geen compleet beeld waar klanten heengaan als de klantrelatie is beëindigd; in elk geval

had een deel ook een bankrekening bij een andere bank en kon die relatie mogelijk voortzetten.

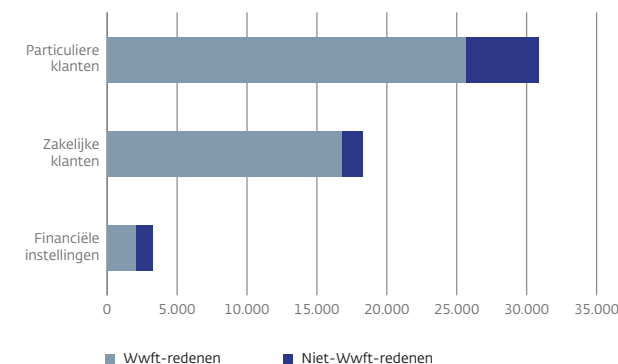
**Afscheid nemen van klanten is een relatief zwaar middel om Wwft-gerelateerde risico's te ondervangen, vandaar dat banken er ook wel voor kiezen de dienstverlening te beperken.** In totaal gaat het hier om ruim 52.000 klanten. De reden om de dienstverlening te beperken is in het merendeel van de gevallen (83% particulieren, 92% zakelijk en 62% financiële ondernemingen) Wwft-gerelateerd (figuur 4). Het gaat om bijna 26.000 particuliere en bijna 19.000 zakelijke klanten (inclusief financiële ondernemingen). Dit staat in contrast met de eerder aangehaalde redenen om de klantrelatie te beëindigen, waarbij het merendeel *niet*-Wwft gerelateerd is (figuur 1). Juist risico's op witwas- en terrorismefinanciering kunnen vaak ook verminderd worden door de dienstverlening aan te passen, bijvoorbeeld ten aanzien van het gebruik van contant geld. Waar klanten betrokken zijn bij fraude of werkzaam zijn in een sector waar een bank om ethische redenen niet meer actief wil zijn, is beperking van dienstverlening minder op zijn plaats.

Er is veel overlap tussen de sectoren waarbij dienstverlening is beperkt en waarbij dienstverlening is beëindigd om Wwft-redenen. De zeven sectoren waar de meeste beperkingen voorkomen, zijn ook de meest voorkomende sectoren bij de beëindiging van de dienstverlening. Horecabedrijven zijn na financiële

holdings in aantal het vaakst beperkt in dienstverlening (figuur 5). Mogelijk dat het instellen van een 'basisbankrekening' voor kleinzakelijke klanten een verdere manier is om klanten met een hoog risicoprofiel toch, onder beperkingen, diensten te kunnen verlenen. Voor particulieren bestaat al het recht op een basisbankrekening, aangevuld met het Convenant Basisbankrekening voor personen voor wie dat wettelijke recht niet geldt (bijvoorbeeld wegens begaan van een financieel delict).

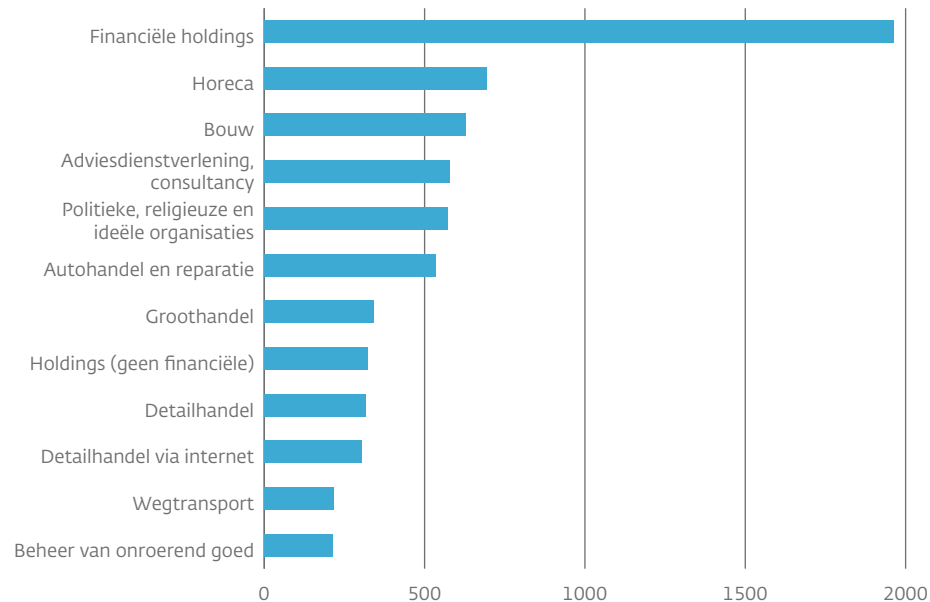
**Figuur 4 Aantal klanten waarbij in 2021 de dienstverlening is beperkt**

Uitgesplitst naar onderliggende redenen



Toelichting: op basis van gegevens van de vier grootste banken. Wwft-redenen: klant past niet binnen integrity risk appetite m.b.t. naleving Wwft, klant non-coöperatief, bank kon niet voldoen aan wettelijke eisen m.b.t. cliëntenonderzoek, overig Wwft gerelateerd. Niet-Wwft-redenen o.a. fraude, reputatierisico bank, commerciële redenen, milieugerelateerde of maatschappelijke factoren.

Figuur 5 Aantal klanten waarbij in 2021 om Wwft-redenen de dienstverlening beperkt is per sector



Toelichting: op basis van gegevens van de vier grootste banken. Betreft de 12 grootste sectoren, in enkele gevallen zijn kleinere sectoren geclusterd.

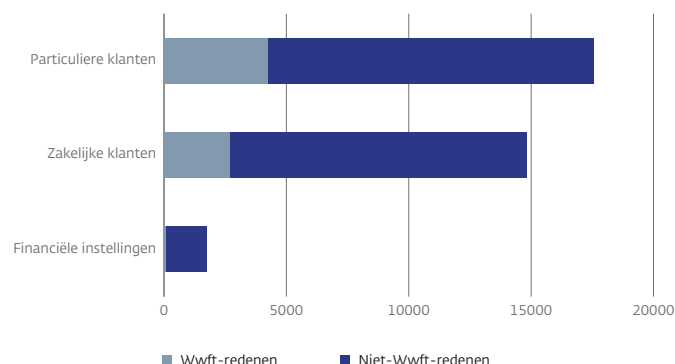
**Ongeveer 34.000 potentiële klanten zijn in 2021 niet als klant geaccepteerd door banken.** Naast klanten waaraan de dienstverlening is beëindigd, is er ook een groep die helemaal niet als klant is geaccepteerd. Deze groep bestaat naar schatting uit circa 18.000 particulieren, 15.000 zakelijke klanten en 1.750 financiële instellingen (figuur 6). Net als voor het afscheid nemen

van bestaande klanten liggen Wwft-redenen veelal niet ten grondslag aan de weigering: naar schatting slechts bij een kwart voor particulieren, 18% voor zakelijke klanten en 4% voor financiële ondernemingen. Als er wel sprake is van een Wwft-reden dan zijn veelvoorkomende kenmerken van klanten die zijn afgewezen onvolledige of foutieve documentatie, niet

willen meewerken aan informatieverzoeken, niet passen binnen de risicobereidheid van de bank of onvoldoende binding hebben met Nederland. Ook hier is sprake van een stijging ten opzichte van 2016. Een verdeling naar sectoren is op basis van de beschikbare gegevens niet goed te maken. Het is veelal onbekend of deze klanten bij een andere bank wel zijn aangenomen als klant. Uit anekdotische informatie blijkt wel dat klanten die bij een bank zijn afgewezen het proberen bij andere banken, het zogenoemde waterbedeffect. Er is geen data beschikbaar over de mate waarin klanten zijn ontmoedigd, waardoor het niet tot een vastgelegde 'afwijzing' is gekomen.

Figuur 6 Aantal potentiële klanten waarbij in 2021 de dienstverlening is afgewezen

Uitgesplitst naar onderliggende redenen



Toelichting: op basis van gegevens van de vier grootste banken. De gegevens zijn onvolledig en deels geschat. Wwft-redenen: klant past niet binnen integrity risk appetite mbt naleving Wwft, klant non-coöperatief, bank kon niet voldoen aan wettelijke eisen m.b.t. cliëntenonderzoek, overig Wwft gerelateerd. Niet-Wwft-redenen o.a. fraude, reputatierisico bank, commerciële redenen en milieugerelateerde of maatschappelijke factoren.

### 2.2.2 Lasten voor klanten

**Hoewel klanten van banken het belangrijk vinden om witwassen en terrorismefinanciering tegen te gaan, is er bij klanten ook ongenoegen over de vragen om informatie door de bank.** Dit blijkt onder meer uit de meldingen die de infodesk van DNB op dit vlak krijgt. Banken hebben informatie nodig om een

beeld van de klant te vormen en daarmee te bepalen in welke mate er sprake is van risico's op witwassen of financieren van terrorisme. Tegelijkertijd ervaren sommige klanten deze belasting als ongewenst, vinden ze de reikwijdte van de vragen te groot en krijgen ze in sommige gevallen het gevoel dat ze hun onschuld moeten bewijzen. Ook vinden ze het vervelend dezelfde informatie meer dan één keer te moeten aanleveren. Ze geven er de voorkeur aan dat instellingen op elkaars oordeel mogen vertrouwen, of willen volstaan met toestemming geven aan instellingen om gegevens te delen.

#### **Banken geven aan dat ze de gevraagde informatie nodig hebben om de Wwft goed na te kunnen leven.**

Daarbij stellen de banken rekening te houden met de risicogebaseerde insteek van de Wwft. Dit komt onder meer tot uiting in het feit dat de belasting van particuliere klanten in de regel minder omvangrijk is dan voor zakelijke klanten. Dit geldt met name voor particulieren waar geen aanleiding is om aanvullende informatie op te vragen. Zodra een klant een hoger risicoprofiel krijgt, nemen de informatieverzoeken en het detailniveau van de gevraagde informatie toe – in uitzonderlijke gevallen kan het aantal gevraagde documenten substantieel toenemen. Banken zouden graag meer gebruik willen maken van publieke registers (BRP, UBO) om minder aan de klant zelf te

hoeven vragen. Ook het gemakkelijker hergebruiken van informatie door meerdere instellingen zou zowel de klant als de instelling helpen.

**De klantbelasting verschilt per bank, met name voor zakelijke klanten.** Sommige banken vragen in eerste instantie een beperkte set aan documenten op, terwijl andere banken direct uitgebreider uitvragen. Afhankelijk van o.a. klantkenmerken en beschikbaarheid van documenten uit openbare bronnen wordt om additionele informatie gevraagd. Net als voor particuliere klanten geldt dat het aantal documenten substantieel toeneemt naarmate een potentiële klant meer risico's met zich brengt. Met name kleinzakelijke klanten ervaren dit als een hoge belasting.

**Banken worstelen ook met de risicogebaseerde aanpak.** Er zijn situaties waarin de bank de toegevoegde waarde van de gevraagde informatie moeilijk kan duiden, terwijl tegelijkertijd op grond van de Wwft de noodzaak wordt gevoeld om toch nadere, soms vergaande, uitvragen bij de klant te doen. De open norm wordt dan toch 'rule based' ingevuld, uit vrees om niet aan de wet te voldoen en daar door de toezichthouder op te worden aangesproken. Een voorbeeld hiervan zijn de uitvragen bij (de kinderen van) politici of andere gezagsdragers<sup>23</sup> terwijl dit in meerdere gevallen niet past bij het daadwerkelijke

23 Zogenaemde 'politiek prominente personen' (*politically exposed persons*, 'PEP').



risico. Een ander voorbeeld is het door de bank bij het aannemen van een klant moeten opstellen van een verwacht transactieprofiel op basis van door die klant gegeven informatie. Liever wil een bank eventuele afwijkende transactiepatronen op een andere manier identificeren, zoals met behulp van indeling in een groep vergelijkbare klanten ('peer group') met een bijbehorend standaardprofiel.

**In het reviewproces van bestaande klanten wordt minder informatie opgevraagd dan bij nieuwe klanten.** Banken maken in principe gebruik van zowel een periodieke *review* als een *review* op basis van signalen. In de periodieke *review* wordt meer informatie opgevraagd naarmate het risicoprofiel van de klant hoger is. Klanten met het laagste risicoprofiel worden vaak alleen opnieuw bezien als daar een concreet signaal voor is. Voorbeelden van signalen voor een *review* zijn afwijkingen in het transactiepatroon, verhoogde of hoge contante betalingen of stortingen of activiteiten die afwijken van te verwachten activiteiten binnen een bepaalde sector.

**Voor sommige sectoren is het reviewproces relatief belastend.** Dit betreft met name sectoren die in de regel door banken als hoog risico worden beschouwd, zoals bijvoorbeeld zakelijk vastgoed, schroot-handelaren, trustkantoren en stichtingen. De hoge

risicoclassificatie maakt dat zij veel vaker aan een periodieke review worden onderworpen, en dat de bijbehorende informatievragen diepgaander zijn. Dit laatste aspect geldt ook voor de acceptatiefase.

**Uit informatie van meldingen bij DNB blijkt dat meerdere klanten vinden dat de bank onnodige informatie opvraagt of informatie waarvan klanten het onprettig vinden om die te delen.**<sup>24</sup> Bij verschillende meldingen wordt aangegeven dat het onduidelijk is waarom de bank gegevens opvraagt, zowel bij initieel cliëntenonderzoek als bij review. Het gaat dan bijvoorbeeld om belastingaangiftes, saldi bij andere banken en informatie uit een ver verleden. Klanten worden verrast door informatieverzoeken terwijl ze al lang klant zijn en ze verwachten dat de bank de informatie al in het bezit heeft of via een andere instantie kan krijgen. Nagenoeg alle melders onderschrijven het belang van het voorkomen van witwassen en de financiering van terrorisme en zijn ook bereid daaraan hun bijdrage te leveren, maar ze ervaren de aanpak als rigide en dwingend. Tot slot uiten ze zorgen over privacy en dat gevoelige informatie in verkeerde handen terechtkomt.

## 2.3 Versterking van de risicogebaseerde aanpak

**De Wwft is risicogebaseerd: de intensiteit van de maatregelen ter voorkoming van witwassen en financieren van terrorisme dient te worden afgestemd op de concrete risico's die een cliënt meebrengt.** Bij een verhoogd risico is meer aandacht nodig, bij een geringer risico kan worden volstaan met een minder intensieve controle.

**Het uitgangspunt voor de beheersing is en blijft de risicoanalyse.** Als een bank goed inzicht heeft in de integriteitsrisico's die zij loopt, zowel op het niveau van de eigen organisatie als op het niveau van de klant, kan zij haar aanpak daarop enten. Een (inadequate) risicoanalyse kan verschillende gevolgen hebben, die zijn samengevat in figuur 7. Een bank kan in dit proces twee typen verkeerde inschattingen maken. Enerzijds kan een te lage inschatting van de risico's ertoe leiden dat een bank te weinig risicobeheersende maatregelen neemt (het rode vlak). Anderzijds kan een te hoge inschatting van de risico's ertoe leiden dat banken te veel en te intensieve maatregelen nemen (het oranje vlak).

<sup>24</sup> Gebaseerd op een telefonische enquête onder 31 personen die zich in de eerste helft van 2022 hebben gemeld bij de Infodesk van DNB.



Figuur 7 Werkelijke risico en ingeschat risico

		Ingeschat risico	
		Laag	Hoog
Werkelijk risico	Laag	Maatregelen ter beheersing van het risico terecht beperkt	Maatregelen ter beheersing van het risico onterecht uitgebreid en intensief
	Hoog	Maatregelen ter beheersing van het risico onterecht beperkt	Maatregelen ter beheersing van het risico terecht uitgebreid en intensief

Als er te veel klanten onterecht “laag” of “hoog” worden ingeschat, dan is dat een indicatie dat het beoordelings-systeem van de bank tekortkomingen kent. Met het oog op de poortwachtersfunctie is er vanuit het toezicht veel aandacht voor het rode vlak. Deze aandacht blijft nodig, omdat juist daar een potentiële bron ligt voor misbruik van het financiële systeem.

Daarnaast vraagt een risicogebaseerde benadering ook om aandacht voor het oranje vlak.

De toezichthouder heeft ook een rol te spelen bij het tegengaan van ‘overcompliance’.

**Banken ervaren niet de ruimte om beheersmaatregelen te beperken, ook al is de toepassing ervan in het licht van het concrete geval niet proportioneel.** Dit is met name aan de orde waar een hoog risico factor in het geding is (bijvoorbeeld een PEP of een stichting), maar waar misschien in het concrete geval de mogelijke hoge risico’s zich niet voordoen. Dit is een potentiële oorzaak van onnodige *de-risking* en disproportionele klantbelasting. Een te strikte interpretatie van de Wwft kan ook bij lage risico’s leiden tot maatregelen van banken en een belasting van klanten die disproportioneel zijn. Dit leidt potentieel tot verlies van effectiviteit van en draagvlak voor de naleving van de Wwft en voor het toezicht. Een beperktere inzet in geval van lage risico’s schept de ruimte om capaciteit en aandacht te richten op hogere risico’s. Een dergelijke meer risicogebaseerde aanpak kan bijdragen aan de effectiviteit van de beheersing van de risico’s op financieel-economische criminaliteit.

**Het gebruik van contant geld levert een bijzonder spanningsveld op.** Contant geld is een wettig betaalmiddel, waarvan het legitiem gebruik niet gehinderd moet worden. Maar het gebruik van contant geld kan onder omstandigheden een sterke indicator zijn van witwassen of terrorismefinanciering. Op initiatief van DNB hebben organisaties die nauw betrokken zijn bij het Nederlandse betalingsverkeer in

april 2022 een nieuw Convenant Contant Geld afgesloten.<sup>25</sup> Hiervoor is door DNB een aantal overwegingen opgesteld bij het treffen van maatregelen tegen witwassen en terrorisme-financiering. Indicatoren die nadere aandacht vragen zijn het gebruik van ongebruikelijk grote bedragen, opmerkelijke patronen in betaalgedrag, het gebruik van grote coupures, frequente transacties die kunnen duiden op het zogenoemde ‘smurfen’ (grote transacties verdoezelen door ze op te splitsen), en transacties die niet passen bij het profiel van de klant. Banken zullen maatregelen die ze noodzakelijk achten om witwassen of financieren van terrorisme te voorkomen, baseren op een onderbouwde, klantspecifieke of klantgroep-specifieke risicobeoordeling. DNB zal hier tijdig over worden geïnformeerd, zodat DNB gelegenheid heeft daarover met de bank in gesprek te gaan.

**In het verder brengen van de risicogebaseerde benadering wil DNB, naast de blijvende aandacht voor hoge risico’s, juist ook de lage risico’s nader verkennen.** Een aanpak hiervoor zou kunnen zijn dat DNB en sector samen, op basis van concrete input, komen tot concrete leidraden op dit gebied. Dit vanuit de gedachte dat banken in een effectievere aanpak meer maatregelen toepassen waar het moet en minder waar het kan. Zo zouden banken bij een review mogelijk bepaalde informatie niet op hoeven vragen als

<sup>25</sup> [Afspraken over goed functioneren van contant geld in nieuw Convenant \(dnb.nl\)](#)



uit het transactiegedrag geen verhoogd risico blijkt. Ook zou het opvragen van aanvullende informatie bij cliëntacceptatie achterwege kunnen blijven als er – ondanks de aanwezigheid van een hoogrisicofactor – duidelijk sprake is van een laagrisicosituatie. Een daadwerkelijk risicogebaseerde benadering draagt ook bij aan het voorkomen van onnodige *de-risking*.

**Goede uitleg aan de klant waarom de bank (veel) informatie opvraagt en hoe de bank omgaat met die informatie, kan bijdragen aan het begrip van de klant.** De versterkte risicogebaseerde aanpak brengt altijd nog met zich dat banken bij hogere risico's meer informatie moeten opvragen bij klanten om een beeld te hebben van het risico en om de meest passende beheersmaatregelen te kunnen nemen. Bij de klanten kan dat als vervelend en disproportioneel worden ervaren. Aangezien klanten bereid zijn om een inspanning te leveren om witwassen en terrorismefinanciering tegen te gaan, is het van belang dat banken duidelijk uitleggen waarom gegevens worden opgevraagd. De uitleg dat het een wettelijke verplichting betreft op grond van de Wwft of dat het is opgelegd door de toezichthouder is onvoldoende, de klant heeft behoefte aan een inhoudelijke toelichting. Daarbij kunnen brancheorganisaties en banken nog meer, en meer structureel, samenwerken aan scherpere en specifiekere risicoanalyses om tot

gerichtere risicomitigatie te kunnen komen. Het overleg hierover in MOB-verband biedt hiervoor een kader. Voorts is het raadzaam om de zorgen met betrekking tot het delen van gevoelige gegevens serieus te nemen. Zo is het belangrijk dat de manier waarop gegevens worden aangeleverd, beveiligd is en dat in het benaderen van klanten de angst voor *phishing* wordt weggenomen. Bovendien willen klanten graag weten wat er met hun gegevens gebeurt. Inzicht in dat proces, waarbij de bank ook duidelijk maakt dat informatie niet voor andere doelen zal worden gebruikt, kan helpen zorgen weg te nemen.<sup>26</sup>

---

<sup>26</sup> De AVG vereist ook transparantie bij de verwerking van persoonsgegevens.



### 3 Het toezicht op de poortwachtersrol door DNB



**3.1 Toezicht richt zich op concrete risico's**  
**DNB zet in op risicogebaseerd toezicht.** Daarbij past een proportionele inzet van de toezichtcapaciteit: hoger en intensiever naarmate de omvang, impact en complexiteit van de risico's die een instelling loopt hoger zijn, en minder intensief waar deze lager zijn. Voor DNB is daarmee de risicoanalyse, net als bij de instellingen, een belangrijke basis voor de invulling van haar toezicht. Deze benadering ligt ook ten grondslag aan de toezichtmethodologie van DNB.<sup>27</sup>

#### **Risicogebaseerd toezicht heeft meerdere dimensies.**

Allereerst verschillen de risico's per sector: het risicoprofiel van de ene sector verschilt van die van een andere sector. Vervolgens verschillen de risicoprofielen van onder toezicht staande instellingen. De ene bank heeft een ander risicoprofiel dan een andere bank – bijvoorbeeld door de producten die een bank aanbiedt, de marktsegmenten die de bank bedient en de landen waarin de bank actief is. En bij een instelling zelf is de ene klant weer risicovoller dan de andere. DNB houdt rekening met deze verschillen bij de inzet van per definitie schaarse toezichtcapaciteit. DNB beoordeelt de beheersing die de instelling toepast in het concrete geval dus in het licht van het concrete risico.

**Om instellingen te helpen met het begrijpen van risico's en het implementeren van hun verplichtingen brengt DNB geregeld *guidance* uit, die waar nodig wordt geëvalueerd en aangepast.** De Wwft kent een flink aantal open normen. Die zijn soms uitdagend om na te leven voor instellingen. DNB biedt handvatten om deze normen te kunnen naleven. Deze informatiefunctie heeft een belangrijke plaats in het toezicht van DNB. Naast verduidelijkende documenten

van internationale organisaties als FATF en EBA, geeft DNB in leidraden, *good practices*, Q&A's en nieuwsberichten toelichting en verduidelijking. In de 'Leidraad Wwft en Sw' worden onder meer de risicogebaseerde aanpak, het cliëntenonderzoek, de transactiemonitoring en het melden van ongebruikelijke transacties toegelicht. Naast deze algemene toelichting bestaat er een aantal specifieke beleidsdocumenten, zoals over het cliëntenonderzoek bij stichtingen, *post-event* transactiemonitoring, de systematische integriteitsrisicoanalyse (SIRA) en over zakelijke vastgoedactiviteiten.

#### **3.2 Voorkomen van financieel-economische criminaliteit als speerpunt van toezicht**

**Voor DNB is het voorkomen en bestrijden van financieel-economische criminaliteit door de instellingen een speerpunt in het toezicht.** DNB heeft dit bevestigd in de 'Visie op Toezicht 2021-2024' en ook in eerdere documenten inzake haar toezichtstrategie.<sup>28</sup>

<sup>27</sup> DNB, ATM, *de vernieuwde toezichtaanpak*

<sup>28</sup> DNB, *Visie op toezicht 2021-2024* en *Visie-op-toezicht 2018-2022*



**Het bestuursrechtelijke mandaat van DNB ontwikkelt zich.** Het bestuursrechtelijk instrumentarium is in de loop der jaren versterkt. Zo zijn de maximumboetes voor overtreding van de Wwft sterk verhoogd en moeten formele maatregelen worden gepubliceerd. Dit ondersteunt de inzet van DNB die is gericht op het versterken van het fundament voor het voorkomen en bestrijden van financieel-economisch criminaliteit en het noodzakelijke herstel van tekortkomingen. DNB zal haar gehele instrumentarium blijven inzetten om in de sector naleving van de Wwft te bereiken. Daarnaast heeft de gerichte aanpak van het OM effecten gehad. De transacties van het OM met een aantal grootbanken hebben een duidelijk strafrechtelijk signaal afgegeven dat banken hun basis op orde moeten krijgen. In de toekomstige bestrijding van financieel-economische criminaliteit is het belangrijk om te kijken wanneer het strafrecht en wanneer het bestuursrecht ingezet kan worden, waarbij het primaat bij het OM ligt. Tegen die achtergrond blijft het bestuursrechtelijke mandaat van DNB, en in het verlengde daarvan DNB's bevoegdheden en toezichtinstrumenten, zich ontwikkelen. DNB zal haar gehele instrumentarium blijven inzetten met het oog op de effectieve invulling van de poortwachtersfunctie.

**Het handhaven van de Wwft-normen is een kerntaak van toezicht.** Handhaving is daarbij gericht op het doel van de Wwft, namelijk voorkomen dat banken en andere instellingen betrokken raken bij witwassen en financieren van terrorisme. De zwaarte van de ingreep hangt onder meer af van de ernst en duur van de overtreding, de mate van verwijtbaarheid en de mate waarin de instelling gericht is op het voldoen aan de normen.<sup>29</sup> Dit bepaalt bijvoorbeeld of DNB al dan niet een formele maatregel inzet. Sinds 2018 kan DNB voor overtredingen van de Wwft hogere boetes opleggen die in bepaalde gevallen op kunnen lopen tot 20% van de netto omzet. Ook publiceert DNB bestuurlijke sancties zoals een last onder dwangsom of een bestuurlijke boete. DNB vindt publicatie belangrijk, omdat dit de effectiviteit van deze instrumenten vergroot, doordat er een sterkere preventieve werking van uitgaat.

### 3.3 Prioriteiten voor het DNB toezicht in de komende jaren

**DNB beoogt de risicogebaseerde benadering naar een volgend niveau te brengen, zowel in haar toezicht als in de risicogebaseerde toepassingen van de Wwft door banken en andere instellingen.** In het integriteitstoezicht van DNB is de afgelopen jaren met name veel aandacht geweest voor de randvoorwaarden voor het beheersen van risico's op financieel economische criminaliteit. Kort gezegd:

de basis voor het voorkomen van betrokkenheid bij witwassen en financieren van terrorisme moest allereerst op orde worden gebracht. Dit heeft geleid tot – soms omvangrijke – herstelprogramma's.

**DNB blijft de komende jaren toezien op de implementatie van met banken gemaakte afspraken over herstel van tekortkomingen.** Daarbij beoogt DNB de intensiteit van toezicht, de beoordeling van de situatie en de handhaving risicogebaseerd in te vullen. Niet iedere overtreding zal automatisch tot een boete leiden, maar tekortkomingen dienen wel altijd te worden opgelost. Dit legt de basis voor de verdere invulling van de poortwachtersfunctie.

**DNB ziet de sterkere toepassing door banken van de risicogebaseerde benadering als volgende belangrijke aandachtspunt in het toezicht.** In dat kader is niet alleen van belang dat banken bij hogere risico's meer maatregelen nemen, maar past het ook dat instellingen de ruimte benutten voor een minder zware inzet bij lage risico's. Dit vraagt zowel van banken in de toepassing als van DNB in het toezicht een ontwikkeling. Het vraagt ook acceptatie dat een weloverwogen risico-afweging ook kan leiden tot een keuze die achteraf gezien toch niet de juiste blijkt te zijn. Dat wil dan niet per definitie zeggen dat de bedrijfsvoering gefaald heeft.

<sup>29</sup> Zie uitgebreider: AFM en DNB, [Handhavingsbeleid van de Autoriteit Financiële Markten en De Nederlandsche Bank](#).

Daarbij dienen instellingen hun risicobeoordeling te baseren op het totaalbeeld van de individuele klant, waarbij zowel risicoverhogende als -verlagende factoren meegewogen worden.<sup>30</sup> Dat bepaalde

risicofactoren van toepassing zijn, betekent niet dat een klant noodzakelijkerwijze in bijvoorbeeld een hogere risicocategorie moet worden ingedeeld. Zo is de sector waarin een klant opereert slechts één van de factoren die de instelling mee dient te wegen in de bepaling van de klantrisicoclassificatie.<sup>31</sup> De bank dient risicoverhogende, -verlagende en mitigerende factoren mee te wegen bij het verrichten van het cliënten-onderzoek naar de individuele klant, ook gebruikmakend van de in de loop van de klantrelatie verkregen informatie. Daarbij is ruimte voor differentiatie in het toepassen van maatregelen ter beheersing van specifieke risico's, afhankelijk van het totale risicobeeld van de klant.

**DNB zal in haar beleidsuitingen in toenemende mate werken met een risicogebaseerde benadering, en ruimte geven voor innovatieve toepassingen.** Als gezegd ondersteunt DNB instellingen in de vorm van guidance over wat DNB van ze verwacht. Waar mogelijk zal DNB samen met onder toezicht staande instellingen onderzoeken welke situaties tot een laag risico of tot een hoog risico leiden, en hoe vertrouwen

kan worden gegeven en verkregen dat de juiste maatregelen voor de geconstateerde risico's worden genomen. Daarbij is er ruimte om innovatieve oplossingen toe te passen, zeker waar die effectiever zijn dan een traditionele aanpak (zie verder hoofdstuk 4). Waar banken zorgen hebben of iets wel is toegestaan, gaat DNB graag het gesprek aan. Waar de wet toepassing van een innovatieve oplossing formeel niet toestaat, terwijl toepassing het doel van de wet ondersteunt, wil DNB de ruimte onderzoeken, bijvoorbeeld door ook in samenspraak met de wetgever te kijken of nodeloze hindernissen kunnen worden weggenomen. Het uiteindelijke doel is immers op een efficiënte en effectieve manier witwassen en terrorismefinanciering tegen te gaan.

**Waar mogelijk zal DNB in beleidsuitingen naast het bespreken van situaties met verhoogd risico aandacht besteden aan situaties van laag risico en welke beheersing daarin proportioneel is.** Dit vormt onderdeel van een evaluatiecyclus om na te gaan wat het effect is van de beleidsuitingen en op welke punten deze aangevuld of bijgesteld dienen te worden. Voorbeelden van mogelijk met de sector uit te werken situaties van potentieel laag risico zijn:

- PEPs die een product afnemen met een laag risico.
- Stichtingen met een beperkte jaarlijkse omzet.
- Een eenvoudige rekening-courantrelatie met een particulier.
- Consumentenkrediet en kleine leningen.
- Particuliere spaarrekeningen zonder mogelijkheid tot cash stortingen.

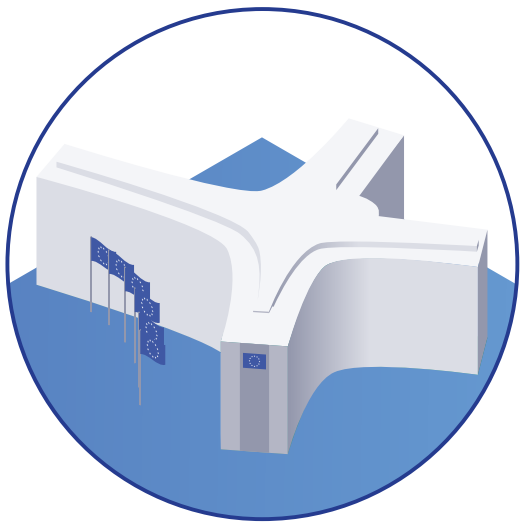
**Technologie en data spelen in het toezicht een steeds grotere rol.**

In de *Visie op Toezicht 2021-2024*<sup>32</sup> stelt DNB dat ze data beschouwt als een cruciaal middel voor effectief en efficiënt toezicht. Datagedreven toezicht vormt daarom het uitgangspunt voor DNB. Het doel is om een completer risicobeeld van instellingen te krijgen. DNB wil de komende jaren ook zelf in haar toezicht in toenemende mate gebruik maken van slimme algoritmes en kunstmatige intelligentie. Uiteraard geldt dit ook voor het integriteittoezicht van DNB. Zo heeft de *data science hub* van DNB recentelijk een transactie-monitoringsmodel ontwikkeld, om modellen van banken uit te dagen.

<sup>30</sup> EBA richtsnoeren ML/TF-*risicofactoren*, Richtsnoer 3.

<sup>31</sup> Zie: *Nadere duiding hoogrisicosectoren in de integriteitsrisico-uitvraag* (dnb.nl)

<sup>32</sup> DNB, *Visie op toezicht 2021-2024*



### 3.4 Europese ontwikkelingen

#### **Er komt een nieuw Europees kader voor de aanpak van witwassen en financieren van terrorisme.**

Hoewel de internationale invloed op het Nederlandse toezichtrechtelijk kader groot is, en er ook veel internationaal wordt samengewerkt, is het toezicht nog wel een nationale aangelegenheid. Dit gaat in de toekomst veranderen als het AML/CFT-pakket van de Europese Commissie wordt doorgevoerd. Onder meer met de oprichting van een nieuwe Europese toezichthouder, de Anti-Money Laundering Authority (AMLA), zal het toezicht op het voorkomen van witwassen en terrorismefinanciering in sterkere mate een Europees karakter krijgen (zie Box 2).

#### **Box 2 Een nieuw Europees kader voor AML/CFT toezicht**

Op 20 juli 2021 publiceerde de Europese Commissie een pakket voorstellen om de gezamenlijke Europese aanpak van witwassen en terrorismefinanciering te versterken. Het pakket bevat onder meer de volgende maatregelen:

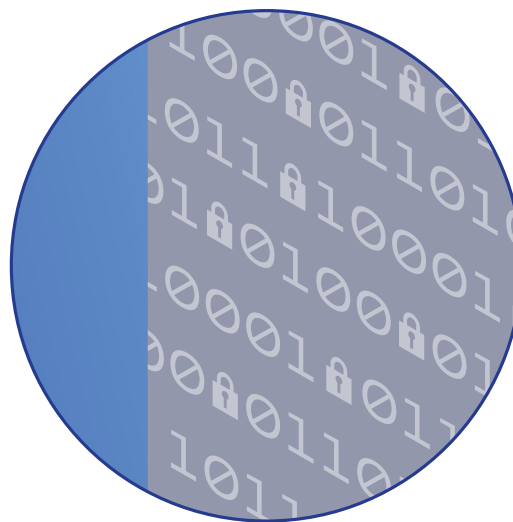
- De oprichting van een Europese autoriteit voor de bestrijding van witwassen en terrorismefinanciering (AMLA). Deze toezichthouder zal vanaf 2026 rechtstreeks toezicht uitoefenen op een aantal geselecteerde instellingen waar Europese witwasrisico's hoog zijn. Ook gaat de autoriteit nadere regelgeving opstellen, en zal ze een vehikel voor nauwere samenwerking tussen de lidstaten vormen.
- Een anti-witwasverordening (AMLR), die eveneens in 2026 in werking moet treden. De verordening uniformeert de regels waar instellingen zich aan moeten houden om het gebruik van het financiële stelsel voor witwassen en terrorismefinanciering te voorkomen, en heeft directe werking in alle lidstaten. De Europese regels zullen op dit vlak de Nederlandse Wwft vervangen.
- Een nieuwe antiwitwasrichtlijn (AMLD6), waarin onder meer de bevoegdheden van de nationale toezichthouders worden geregeld.

## 4 Gebruik van data en inzet van technologie

**Technologie kan het bestrijden van financieel-economische criminaliteit effectiever en efficiënter maken.**<sup>33</sup> Aangezien de Nederlandse samenleving en economie reeds in sterke mate zijn gedigitaliseerd, bestaat er al een uitstekende digitale infrastructuur voor toepassing van dergelijke technologie. Een optimale mens-machine samenwerking zal financiële instellingen in staat stellen witwassen en financieren van terrorisme effectiever en efficiënter te voorkomen, en daarnaast de (administratieve) belasting van de klant te verminderen. DNB ziet instellingen al experimenteren met digitale ontwikkelingen in klantonderzoeken en transactiemonitoring en is hier, mits de juiste waarborgen zijn ingericht, voorstander van.

**Voor succesvolle digitale innovatie is het belangrijk dat instellingen de basis op orde hebben.** Het gaat dan met name over goed ingerichte Wwft compliance processen, de kwaliteit en betrouwbaarheid van de IT-infrastructuur, datakwaliteit en de beschikbaarheid van (basis)gegevens.

Als deze basis niet op orde is, heeft digitaliseren van processen vaak geen zin. Het is daarom van belang dat banken de huidige herstelfase goed afronden, teneinde innovatieve technologie succesvol te kunnen inzetten.



**Het inzetten van technologie voor het bestrijden van financieel-economische criminaliteit kan spanning met privacywaarborgen voor klanten opleveren (Box 3).**<sup>34</sup> Klantonderzoeken en

transactiemonitoring raken immers per definitie aan de privacy van klanten. De aanwezigheid van persoonsgegevens in de data brengt voor instellingen verschillende verantwoordelijkheden rondom privacybescherming mee. Aan de andere kant zijn veel van deze gegevens wel nodig voor instellingen om te voldoen aan de verplichtingen en verwachtingen die voortvloeien uit de Wwft. Bij het inzetten van digitale technologieën kan het dus zo zijn dat het voldoen aan de eisen van de Wwft extra inspanning kan vergen doordat ook aan de eisen van de AVG moet worden voldaan. De 'traditionele' criminaliteitsbestrijding laat zien dat juridische onderbouwing en adequate verantwoording kunnen zorgen dat er aan deze spanning recht wordt gedaan.

<sup>33</sup> M.V. Achim, S.N. Borlea & V.L. Vaidean (2021), Does technology matter for combating economic and financial crime? A panel data study, Technological and Economic Development of Economy, 27, 1, p. 223-261.

<sup>34</sup> FATF (2017), FATF Guidance - Private Sector Information Sharing.

### Box 3 Adviezen over privacywaarborgen

De Autoriteit Persoonsgegevens (AP) stelt in haar advies van november 2021 over het gewijzigd voorstel voor de Wet gegevensverwerking door samenwerkingsverbanden (WGS): *“...het voorkomen en bestrijden van ernstige en ondermijnende criminaliteit is dermate belangrijk dat ook voor de AP vaststaat dat hiervoor ingrijpende inbreuken op het grondrecht op bescherming van persoonsgegevens noodzakelijk kunnen zijn.”* Ze acht verdere aanpassingen van het wetsvoorstel echter noodzakelijk om uitholling van door de AP in haar beoordeling gehanteerde beginselen, zoals de onschuldpresumptie en het beginsel van dataminimalisatie, te voorkomen. Het wetsvoorstel gaat in de ogen van de AP verder dan strikt noodzakelijk, bevat onvoldoende duidelijke en nauwkeurige regels en onvoldoende procedurele en materiële waarborgen. Daarmee voldoet het wetsvoorstel in de ogen van de AP niet aan de evenredigheidstoets. Noodzakelijke aanpassingen die de AP aangeeft zijn onder meer het beter motiveren van de noodzaak van bepaalde samenwerkingsverbanden, het schrappen van secundaire doelstellingen van de wet, het preciseren van risico's, en het opnemen van duidelijke regels over wanneer samenwerkingsverbanden in actie mogen komen en over de uitzonderingen op de rechten van betrokkenen die de wet mogelijk maakt.

In een reactie op onder meer dit advies heeft de minister van Justitie en Veiligheid in december 2021 gesteld dat hij is gesterkt in zijn opvatting dat het wetsvoorstel op een verantwoorde wijze de gezamenlijke gegevensverwerking door samenwerkingsverbanden in goede en rechtmatige banen kan leiden. Wel moet nog een aantal zorgpunten worden weggenomen, door aanpassing van de wet zodra die is aangenomen, en een nadere regeling van een aantal onderwerpen in een algemene maatregel van bestuur.

Vergelijkbare adviezen zijn uitgebracht over de Wet Plan van aanpak witwassen. In een advies over dit wetsvoorstel, daterend van januari 2021, signaleert de Raad van State dat informatie-uitwisseling bij gezamenlijke monitoring van banktransacties en bij klantonderzoeken kan leiden tot vergaande inbreuken op grondrechten. De Raad onderschrijft in dit advies wel het belang van de aanpak van witwassen en onderkent het belang van de poortwachtersrol van financiële instellingen.

Vanwege de bezwaren heeft de Raad geadviseerd om het wetsvoorstel in zijn huidige vorm niet in te dienen bij de Tweede Kamer. De AP heeft over deze wet in maart 2020 langs dezelfde lijn geadviseerd.

### 4.1 Slimmere klantonderzoeken

**Verdere digitalisering kan de effectiviteit en efficiëntie van *know your customer* (KYC)-processen vergroten.** Klantonderzoeken zijn tijdrovend en arbeidsintensief voor zowel instellingen als klanten. Digitalisering kan hier uitkomst bieden. Om de KYC-processen succesvol te digitaliseren, is het noodzakelijk te beschikken over kwalitatief goede en complete data en over goede modellen die risico-inschattingen van klanten kunnen maken op basis van deze data. Hieronder wordt op beide punten nader ingegaan aan de hand van een specifieke technologische innovatie.

#### 4.1.1 Toegang tot data: de digitale identiteit en wallet (eID)

**Een digitale identiteit kan de identificatie en verificatie in klantonderzoeken drastisch vergemakkelijken, waardoor de (administratieve) belasting voor instelling en klant afneemt.** Een centraal onderdeel van het klantonderzoek is de identificatie<sup>35</sup> van de klant en de verificatie daarvan.

Op dit moment wordt de data die nodig is voor deze identificatie vaak nog los opgevraagd bij de klant. Een digitale identiteit kan deze processen vergemakkelijken. In juni 2021 heeft de Europese Commissie een voorstel gedaan over de revisie van de Europese eIDAS-verordening,<sup>36</sup> waarmee een digitale identiteit voor EU-burgers wordt geïntroduceerd. De verwachting is dat deze na 2022 in werking zal treden. De Commissie

<sup>35</sup> Voor een identificatie is nodig: juridische naam, adres, BSN nummer, en geboortedatum.

<sup>36</sup> A trusted and secure European e-ID - Regulation | Shaping Europe's digital future (europa.eu). Zie ook Electronic Identities And Trust Services, [Alles wat u moet weten over eIDAS](#) | [Inloggen bij organisaties in de Europese Economische Ruimte \(eIDAS\)](#) | [Rijksoverheid.nl](#)



streeft er naar dat in 2030 80% van de EU burgers gebruik maken van deze innovatie.<sup>37</sup> Deze eID krijgt de vorm van een *wallet*, waarin ook andere data geverifieerd en gedeeld kunnen worden, zoals diploma's, adresgegevens, medische gegevens en machtigingen (van rechtspersonen) (figuur 8). Deze zaken worden alleen in de *wallet* opgenomen als ze afkomstig zijn van een betrouwbare en onafhankelijke bron – bijvoorbeeld de universiteit in het geval van een diploma. Met deze eID *wallet* kunnen personen zich identificeren en kiezen welke persoonlijke gegevens ze willen delen, zowel *online* als *offline*. Dit is een simpele en veilige manier die instellingen kunnen gebruiken om informatie van klanten op te vragen – en voor klanten om de informatie te delen. In potentie verhoogt dit dus de betrouwbaarheid van de identificatie en verificatie en verlaagt dit de administratieve belasting voor klant en bank. Een klant moet uiteraard wel toestemming geven voor het delen van (een selectie van) deze data.

Figuur 8 Europese eID Wallet



**4.1.2 Inzetten van kunstmatige intelligentie bij risicoanalyses van klanten**  
**Data-analyse met behulp van kunstmatige intelligentie kan, mits adequate waarborgen zijn ingericht, de risicoanalyse van klanten op een hoger plan brengen.** Onderzoek van McKinsey uit 2019 bij verschillende financiële instellingen laat zien dat de risicoclassificatie van klanten vaak onbetrouwbaar is: laag risico klanten worden vaak geclassificeerd als

hoog risico (vals positieven).<sup>38</sup> Dit brengt onnodige belasting voor instelling en klant met zich mee, aangezien er 'onterecht' extra onderzoek moet worden gedaan. Een nauwkeurigere analyse zou dus aanzienlijk kunnen schelen in de (administratieve) belasting van instelling en klant. Ook is het mogelijk dat klanten als laag risico worden geclassificeerd, terwijl ze in feite een hoog risico met zich brengen (vals negatief). Dit is met name problematisch omdat laag risico klanten niet of

relatief beperkt opnieuw bekeken worden, waardoor (mogelijk) criminele praktijken soms lang onder de radar kunnen blijven. Beter functionerende modellen, op basis van kunstmatige intelligentie (KI) hebben daarom volgens de European Banking Authority (EBA)<sup>39</sup> de potentie beter in staat te zijn om verdachte actoren en activiteiten te identificeren, door middel van het benutten van *machine learning*. *Machine learning* is een vorm van kunstmatige intelligentie die zelflerende

<sup>37</sup> European Parliamentary Research Service (2022), *Revision of the eIDAS Regulation: Findings on its implementation and application*.  
<sup>38</sup> McKinsey & Company (2019), *Transforming approaches to AML and financial crime*.  
<sup>39</sup> EBA (2020), *Report on Big Data and Advanced Analytics*, p.20.



componenten introduceert in modellen. De uitkomsten van het model worden getoetst aan het geprogrammeerde doel, waardoor er een feedbackloop ontstaat van de mate waarin de uitkomst het doel realiseert. Dit betekent dat de uitkomsten van het model dus niet expliciet geprogrammeerd zijn, maar dat het model zelf geleerd heeft om tot deze uitkomsten te komen. Dit zorgt voor nauwkeurige analyse waardoor er minder vals positieve en vals negatieve uitkomsten zullen zijn. Voorwaarde is wel dat de kwaliteit van de data goed is en dat data compleet is. Ook is nodig dat de modellen kunnen leren van wel of juist niet succesvolle uitkomsten. Terugkoppeling van de kant van de FIU en opsporingsinstanties over gemelde ongebruikelijke transacties kan bijvoorbeeld helpen bij dit leren.

**Voor verdere inzet van KI zijn adequate waarborgen onontbeerlijk.**<sup>5</sup> Om te voorkomen dat KI als een soort *black box* functioneert waarvan de uitkomsten niet goed zijn te herleiden, is het belangrijk om menselijke betrokkenheid te behouden.<sup>40</sup> Ook zal er aandacht moeten zijn voor onbewuste discriminatie in de modellen<sup>41</sup> en de mate waarin uitlegbaar is waarom een klant een bepaald risicoprofiel heeft gekregen.<sup>42</sup> Dat is belangrijk omdat het al dan niet toegang krijgen

- en houden - tot financiële dienstverlening van grote invloed is op klanten.

Ook voor de toezichthouder is het van belang dat het KI proces en de analyses die hieruit voortvloeien, inzichtelijk zijn. Het is dan ook belangrijk dat de KI-governance op een adequate manier is ingericht bij instellingen, bijvoorbeeld door de verantwoordelijkheden voor het inzetten van verantwoorde KI te beleggen binnen de gebruikelijke *three lines of defence*.

## 4.2 Slimmere transactiemonitoring

### Machine learning kan ook de transactiemonitoring verbeteren.

Banken zetten voor de detectie van afwijkende transacties op grote schaal transactiemonitoringssystemen in.<sup>43</sup> Hoewel er wel wordt geëxperimenteerd met meer geavanceerde modellen, zijn dit momenteel nog voornamelijk (relatief statische) regelgebaseerde systemen. De voorspellende waarde van deze systemen is relatief beperkt, waardoor er ook hier sprake kan zijn van veel vals positieven en vals negatieven voorspellingen. In regelgebaseerde systemen worden bepaalde criteria met drempelwaardes geformuleerd, waardoor overschrijding van deze drempelwaardes (bijvoorbeeld

een hoeveelheid kasstortingen) automatisch als afwijkend wordt geïdentificeerd door het systeem. Ook hier zou volgens de EBA<sup>44</sup> het inzetten van *machine learning* tot betere analyse van transacties leiden, en dus ook de effectiviteit van de transactiemonitoring verhogen en de belasting voor klant en instelling verlagen. Bovendien kunnen deze modellen beter omgaan met een meer dynamische omgeving, waarin zich continu nieuwe ontwikkelingen en dreigingen in het financiële systeem voordoen. Door middel van de zelflerende componenten kunnen de transactiemonitoringssystemen zo continu geactualiseerd worden.

### 4.2.1 Ex ante transactiemonitoring

**Betere voorspellingen door transactie-monitoringssystemen maken het mogelijk dat instellingen transacties ook meer kunnen stoppen, voordat ze uitgevoerd worden.** Uiteindelijk is voorkomen beter dan genezen. Transacties worden zo beoordeeld door een model voordat ze uitgevoerd worden. Indien ze een te hoge mate van ongebruikelijkheid hebben, kan er dan voor gekozen worden om de transactie eerst op te schorten, zodat een analist de transactie nader kan onderzoeken. Ongebruikelijke en verdachte transacties kunnen dan

<sup>40</sup> WRR (2021), *Opgave AI. De nieuwe systeemtechnologie*.

<sup>41</sup> J. Yong & J. Prelio (2021), *Humans keeping AI in check – emerging regulatory expectations in the financial sector*, FSI Insights No 35.

<sup>42</sup> EBA (2020), *Report on Big Data and Advanced Analytics*.

<sup>43</sup> E. Bosma (2022), *Banks as Security Actors: Countering Terrorist Financing at the Human-Technology Interface*.

<sup>44</sup> EBA 2020, *Report on Big Data and Advanced Analytics*, p. 23.







in een vroeg stadium gestopt worden. Instellingen maken, bijvoorbeeld bij uitvoering van sancties, al gebruik van ex ante transactiemonitoring om bepaalde transacties te stoppen. De regelgebaseerde methodes zijn echter waarschijnlijk niet nauwkeurig genoeg om dit op grotere schaal te kunnen doen. De inzet van *machine learning* kan hier meer mogelijkheden bieden. Wel is het belangrijk dat goede afspraken worden gemaakt over twee zaken: 1) welke grenzen overschreden moeten worden voordat transacties gestopt mogen worden door instellingen; 2) dat er altijd menselijke interventie moet zijn, en ongebruikelijke transacties dus niet volautomatisch definitief gestopt worden.

#### 4.2.2 Uitlegbare KI in transactiemonitoring

**Een uitdaging van het inzetten van *machine learning* modellen is dat ze moeilijk uitlegbaar kunnen zijn.**

Dit kan effect hebben op de mate waarin de resultaten van deze modellen gebruikt kunnen worden. Als er immers een onderzoek wordt uitgevoerd bij een klant en eventueel melding wordt gedaan bij de FIU op basis van een detectie van een *machine learning* algoritme, moet een instelling het model kunnen uitleggen en kunnen verantwoorden waarom de betreffende transactie ongebruikelijk is. Als reden geven dat het systeem dit nu eenmaal aangeeft (*computer says yes/no*),

vormt geen sluitende aanleiding om onderzoek te doen. Dit betekent echter niet dat instellingen deze complexere vormen van KI niet in kunnen zetten. Daarom is een essentiële voorwaarde dat er geen sprake is van automatische besluitvorming door de systemen. De modellen zouden dan meer als ondersteuning ingezet kunnen worden voor analisten. Daarnaast kunnen complexe systemen ingezet worden in combinatie met complementaire uitlegbaarheidstools, die inzichten geven over het functioneren van het model.<sup>45</sup>

#### 4.3 Het inzetten van netwerkanalyses

**Netwerkanalyses onderzoeken de connecties tussen entiteiten om beter zicht te krijgen op hun relaties.**

Netwerkanalyses complementeren bestaande *machine learning* toepassingen. Netwerkanalyses van elke individuele klant kunnen gebruikt worden als een input om de accuraatheid van de transactiemonitoring modellen te vergroten. In plaats van het analyseren van een individu wordt een (subcomponent van een) netwerk onderzocht op bekende methodes van witwassen en ander atypisch consumentengedrag. Netwerken worden gevormd door relaties tussen klanten en gerelateerde activiteiten. Deze links kunnen bestaan uit interne data, zoals overboekingen of gedeeld eigenschap, of op basis van externe data, zoals

gedeelde adressen of gebruik van dezelfde pinautomaat. Banken zijn met deze methode onlangs in staat geweest om een ondergronds bankennetwerk op te rollen, bestaande uit zoo verdachte klanten. Vervolgens zijn de risico-indicatoren voor ondergronds bankieren uit deze ontdekking verwerkt in nieuwe modellen, waardoor de voorspellende waarde van de modellen aanzienlijk werd verhoogd.

#### 4.4 Data-issues

**Digitale innovatie valt of staat bij kwalitatief goede en volledige data.** Bij het inzetten van *machine learning* geldt het adagium: *garbage in, garbage out*. Als de data van slechte kwaliteit is, zijn de uitkomsten dat ook, hoe goed de gehanteerde modellen zelf ook zijn.<sup>46</sup>

Automatische klantscreening tegen terrorismelijsten (*list matching*) is bijvoorbeeld weinig zinvol als namen niet correct of niet consistent gespeld zijn. Data zijn van slechte kwaliteit als deze inconsistent, onvolledig of gedupliceerd zijn. Dataverzamelmethodes, de manier waarop de database is gebouwd en de 'opschoning' van de data zijn allemaal belangrijke onderdelen om de datakwaliteit te waarborgen.

**Een centraal element in het bestrijden van financieel-economische criminaliteit is dat relevante data tussen verschillende partijen gedeeld kan**

<sup>45</sup> EIOPA (2021), *Artificial Intelligence governance principles: towards ethical and trustworthy Artificial Intelligence in the European insurance sector*.

<sup>46</sup> Bain & Company (2018), *How Banks Can Excel in Financial Crimes Compliance*.





**worden.** Het analyseren van data uit verschillende bronnen heeft veel voordelen, aangezien het combineren van datasets leidt tot nieuwe inzichten, en tevens komt tot betere besluitvorming, gedegener onderzoek en sterkere producten en diensten. Tegelijkertijd kunnen datasets van verschillende partijen, met name door bepalingen in de AVG, niet zomaar gecombineerd worden.

Er zijn echter verschillende technologische mogelijkheden, waarmee toch samengewerkt kan worden met data door verschillende instellingen, zonder dat gevoelige informatie daadwerkelijk gedeeld wordt. Zo noemt TNO de mogelijkheid tot Secure Multi-Party Computation (Box 4). Banken hebben, in samenwerking met TNO, deze methode reeds met succes ingezet om gezamenlijk op een effectieve manier fraude te detecteren.<sup>47</sup>

**Voor datadeling tussen partijen zijn passende juridische grondslagen noodzakelijk.** Een voorbeeld hiervan is het *Wetsvoorstel Gegevensverwerking door samenwerkingsverbanden (WGS)*<sup>46</sup>. Dit voorziet in een juridische grondslag om persoonsgegevens systematisch te delen en te verwerken voor zwaarwegende algemene belangen. In deze samenwerkingsverbanden kunnen zowel bestuursorganen als private partijen deelnemen.

Het voorstel is eind 2020 door de Tweede Kamer aangenomen, en ligt thans voor in de Eerste Kamer. In het coalitieakkoord hebben de coalitiepartijen aangegeven ervoor te willen zorgen dat de grondslagen voor gegevensuitwisseling met de juiste waarborgen zijn verankerd in de wet.

#### Box 4 Secure Multi-Party Computation (MPC)

Secure MPC is een innovatieve oplossing om de functionaliteit van een gezamenlijke database te genereren, waarin verschillende partijen data aanleveren, zonder dat data zichtbaar is voor andere partijen. MPC is een verzameling van cryptografische technieken die het mogelijk maken dat meerdere partijen gezamenlijk aan data kunnen rekenen. Doordat de data door cryptografie wordt beschermd, kunnen deze geanalyseerd worden zonder dat de partijen andermans data ooit kunnen inzien.

<sup>47</sup> A. Sangers e.a. (2019), *Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection*, in: Financial Cryptography and Data Security, p. 605-623.

## 5 Effectief door samenwerking

### 5.1 Samenwerking in Nederland

**Een effectieve aanpak van witwassen en terrorismefinanciering is alleen mogelijk als partijen samenwerken.**<sup>48</sup> Een groot aantal partijen is betrokken bij het voorkomen en het bestrijden van witwassen en terrorismefinanciering (zie ook hoofdstuk 1), elk met hun eigen mandaat en verantwoordelijkheid. De FATF ziet de samenwerking als sterk punt van het Nederlandse antiwitwas en -terrorismefinancieringsbeleid. Optimale samenwerking vergt gedeelde doelstellingen en prioriteiten. Dit doet niets af aan de eigen verantwoordelijkheid van alle partijen. De samenwerking tussen partners is geen vervanging van rollen en verantwoordelijkheden. Het is een versterking van ieders rol en verantwoordelijkheid om bij te dragen aan het gedeelde doel van het voorkomen en bestrijden van misbruik van het financiële stelsel voor witwassen of terrorismefinanciering. Elke partij houdt bij het uitoefenen van haar taak in de keten altijd het effect op het uiteindelijke doel voor ogen.

**De maatschappelijke urgentie om actief financieel-economische criminaliteit te voorkomen en te bestrijden is groot.** In het coalitieakkoord is afgesproken de jacht op crimineel geld te intensiveren en om prioriteit te geven aan financiële opsporing en 'intelligence' om ongewenste geldstromen te verstoren. In toenemende mate wordt dit gedaan door de samenwerking tussen publieke partijen, in publiek-

privaat verband en tussen private partijen onderling. Aangezien witwassen en terrorismefinanciering bij uitstek internationale fenomenen zijn, is ook versterking van internationale samenwerking van groot belang.

#### Publieke samenwerking

**Binnen het Financieel Expertise Centrum (FEC) wordt samenwerking binnen de publieke sector vormgegeven.** Het FEC is een samenwerkingsverband tussen autoriteiten met een toezicht-, controle-, vervolgings- of opsporingstaak gericht op de financiële sector en is opgericht om de integriteit van deze sector te versterken. In het FEC worden inzichten, kennis en vaardigheden uitgewisseld met als doel om via een betere informatiepositie en gezamenlijke aanpak het mogelijk te maken om scherper probleemgericht op te treden en criminele geldstromen terug te dringen. Een voorbeeld van publiek-publieke samenwerking zijn de gezamenlijke activiteiten van de FEC-partners bij de bestrijding van terrorismefinanciering. Daarbij wordt onder andere de buitenlandse financiering van non-profitorganisaties onderzocht op mogelijke verbanden met terrorisme of de financiering daarvan.



<sup>48</sup> Zie ook het [Plan van aanpak witwassen](#) van de minister van Financiën en de minister van Justitie en Veiligheid, 30 juni 2019, en de aanbevelingen in: Stichting Maatschappij en Veiligheid (2022), [Poortwachters tegen witwassen](#)

### Publiek-private samenwerking

**Naast samenwerking in het publieke domein is ook de publiek-private samenwerking (PPS) een belangrijk onderdeel van het FEC.** Deze samenwerking wordt vormgegeven door de vaste publieke partners, de vier grootbanken en de Nederlandse Vereniging van Banken. Ook bij het FEC PPS staan goede informatie-uitwisseling, het delen van kennis en het samen uitvoeren van projecten centraal. Een voorbeeld van een effectief publiek-privaat samenwerkingsinitiatief is de *Serious Crime Task Force* waarbinnen de politie, het OM, de FIU-NL en de FIOD samen met een aantal grote banken aan de gezamenlijke aanpak van ondermijning werken. Daarnaast wordt in de *Fintell Alliance* kennis uitgewisseld tussen de FIU-NL en de banken, om de kwaliteit van de analyse van banken te verbeteren waardoor tot betere meldingen kan worden gekomen.

**DNB ziet duidelijk meerwaarde in publiek-private samenwerking.** DNB staat dan ook positief tegenover haar deelname aan publiek-private initiatieven.<sup>49</sup> DNB streeft daarbij naar een aanjagende, adviserende of stimulerende rol. DNB staat ook welwillend tegenover verdergaande bijdragen door deel te nemen aan specifieke samenwerkingsprojecten, mits passend bij haar toezichtstaak. Daarbij overweegt DNB of deelname bijdraagt aan het toezichtdoel om financieel-

economische criminaliteit te voorkomen. Deelname aan een samenwerkingsproject moet passen bij de bevoegdheden en verplichtingen van DNB als toezichthouder, en er moet capaciteit beschikbaar zijn om aan een project deel te nemen.

### Samenwerking tussen private partijen

**Een initiatief op het vlak van privaat-private samenwerking is de samenwerking tussen vijf Nederlandse banken onder de naam Transactie Monitoring Nederland (TMNL).** In samenhang worden de betalingstransacties van de banken gemonitord op signalen die kunnen duiden op witwassen en terrorismefinanciering. DNB is geen partner in dit project, maar steunt het wel en draagt waar mogelijk bij in de vorm van het delen van kennis. De meerwaarde van deze samenwerking is dat door de combinatie van transactiegegevens van verschillende banken er verbanden gelegd worden die een afzonderlijke bank niet kan leggen. TMNL kan daarmee een vehikel worden waarbinnen de 'slimmere transactiemonitoring' (zie paragraaf 5.2) vorm krijgt. Hiervoor moeten wel goede privacy-waarborgen worden opgenomen: afdoende waarborgen om persoonsgegevens te verwerken binnen het kader van de AVG. Ook zou het voor instellingen mogelijk moeten worden om, met behoud van de verantwoordelijkheid, de werkzaamheden voor de transactiemonitoring uit te

besteden. Artikel 10 Wwft staat dat nu in de weg. Wijziging van deze bepaling maakt deel uit van het Plan van aanpak witwassen. In potentie kan TMNL verder uitgebreid worden met andere banken of niet-bancaire partners. Een verdere versterking kan voorts komen uit het opzetten van een 'feedback loop' met de FIU, waarbij de FIU terugkoppelt in hoeverre de resultaten van de analyses van TMNL tot succesvolle opsporing hebben geleid.

### Internationale samenwerking

**DNB verwelkomt nauwere Europese samenwerking.** Zoals in hoofdstuk 3 aan de orde is gekomen zal het toezicht op het voorkomen van witwassen en terrorismefinanciering meer Europees worden. DNB vindt doorvoering van de voorstellen van de Europese Commissie van groot belang om een meer gecoördineerde en uniforme aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering te bereiken. DNB ziet ruimte voor een gefaseerd groeimodel voor de nieuwe Europese autoriteit (AMLA), waarbij geleidelijk meer instellingen onder direct Europees AML/CFT toezicht zouden kunnen komen. Verder zou DNB in vergelijking tot het voorstel van de Europese Commissie de betrokkenheid van nationale toezichthouders onder andere ten aanzien van de Europese besluitvorming willen versterken.

<sup>49</sup> DNB (2020), DNB als partner in publiek-private samenwerking tegen financieel-economische criminaliteit

## 5.2 Kansen voor de toekomst

**Verregaande samenwerking tussen publieke en private partijen maakt het voorkomen en het bestrijden van financieel-economische criminaliteit effectiever.** Immers, het kennisniveau wordt hiermee vergroot en er is beter zicht op risico's, trends, typologieën en indicatoren gerelateerd aan financieel-economische criminaliteit. Daarnaast kunnen in de keten data en signalen worden gedeeld met als doel om criminaliteit tegen te gaan en te zorgen voor effectief toezicht en effectieve opsporing en vervolging. Daarbij is er nog ruimte om de publiek-private samenwerking te versterken, bijvoorbeeld ten aanzien van de coördinatie van de aanpak van financieel-economische criminaliteit in Nederland. Daarbij is het van belang om onderwerpen te prioriteren om deze vervolgens gezamenlijk aan te pakken, om voldoende middelen en menskracht te hebben en wettelijke mogelijkheden om informatie uit te wisselen.

**Sterkere coördinatie om financieel-economische criminaliteit in de financiële sector aan te pakken heeft baat bij centrale sturing en doorzettingsmacht om witwassen en terrorismefinanciering effectiever en efficiënter aan te pakken.** Het FEC kan een belangrijke rol spelen in deze coördinatie. In die hoedanigheid kan het FEC het doel van de Wwft en het doel van samenwerking in de keten scherp voor ogen

houden. Van daaruit kunnen concrete en meetbare operationele doelstellingen worden bepaald, en projecten worden opgezet. De volgende randvoorwaarden die hieronder worden toegelicht zijn daarbij van belang: scherpe prioritering, toereikende capaciteit en informatie-uitwisseling.

**Scherpe prioritering is nodig om daarmee onderwerpen te selecteren die gezamenlijk aangepakt kunnen worden.** Witwassen en terrorismefinanciering kunnen op heel veel deelterreinen samen worden aangepakt. Het is goed om samen keuzes te maken. Met een focus op een aantal prioritaire onderwerpen wordt de effectiviteit van de publiek-private samenwerking verder vergroot. De *National Risk Assessments* (NRA) voor witwassen en terrorismefinanciering kunnen als leidraden gebruikt worden om onderwerpen te prioriteren en vervolgens gezamenlijk aan te pakken.

**Effectieve samenwerking vergt toereikende capaciteit.** Het is van belang dat iedere schakel in de keten voldoende capaciteit heeft. De schakel met de minste capaciteit zal immers een 'bottleneck' vormen voor de gehele keten. In Nederland hielden in 2021 alleen al bij de vier grote banken 10.000 fte aan menskracht zich bezig met het voorkomen van witwassen en terrorismefinanciering (zie hoofdstuk 2).

Die capaciteit is de afgelopen jaren sterk gegroeid, o.a. door diverse hersteltrajecten bij banken. Voldoende capaciteit is ook voor de publieke partners in de keten van belang. De FIU, FIOD en OM hebben extra financiële middelen gekregen uit de zogenaamde 'ondermijningsgelden' van het ministerie van Justitie en Veiligheid. In het Plan van Aanpak witwassen stelt de minister van Financiën dat de capaciteit van de toezichthouders op de Wwft een aandachtspunt blijft omdat het belangrijk is dat zij op een hoogwaardige manier risicogebaseerd toezicht moeten uitoefenen.

**De effectiviteit van de keten van het melden en onderzoeken van ongebruikelijke transacties kan worden verhoogd.** De wetgever zou er voor kunnen kiezen instellingen te vragen niet al te melden wanneer transacties 'ongebruikelijk' zijn, maar de focus bij het melden te leggen op 'verdachte' transacties waarbij de instelling vermoedt dat de handelwijze van de klant verband houdt met witwassen of het financieren van terrorisme.<sup>50</sup> Hiermee kunnen in potentie transactie-monitoringsystemen scherper afgesteld worden, kan de kwaliteit van de meldingen worden verhoogd, en zal het aantal meldingen afnemen. De FIU kan hierdoor met een gerichtere dataset aan de slag, hetgeen de kans op een effectievere opvolging in de keten vergroot. Hiermee zou Nederland ook minder afwijken van de internationale usance om verdachte transacties

<sup>50</sup> Dit laat onverlet de verplichting zich te onthouden van het uitvoeren van transacties waarvan men weet of vermoedt dat deze verband houden met de opbrengsten van criminele activiteiten of met terrorismefinanciering.



te melden. Zoals in hoofdstuk 4 aan de orde kwam kan de inzet van '*machine learning*' hieraan bijdragen. Meer mogelijkheden tot datadelen binnen de meldingsketen en eerder genoemde 'feedback loops' zullen ook de effectiviteit vergroten.

**Informatie-uitwisseling is belangrijk voor zowel de publieke als private rol in het voorkomen en bestrijden van financieel economische criminaliteit.**

Voor de publieke partijen in de keten geldt 'twee weten meer dan één'. Door over specifieke casuïstiek of fenomenen informatie met elkaar te delen kan ieder van hen de eigen publieke taak beter en beter geïnformeerd uitoefenen. Dat moet uiteraard zorgvuldig en met aandacht voor vertrouwelijkheid en privacy plaatsvinden. Het op die wijze delen van informatie komt het voorkomen en bestrijden van financieel-economische criminaliteit ten goede. Private partijen hebben op hun beurt een informatiepositie die waardevol is voor de invulling van hun eigen rol en verantwoordelijkheid. Daarnaast zijn private partijen in staat om afwijkend gedrag te detecteren waardoor vroegtijdig ingrijpen in criminele processen mogelijk is. Private partijen beschikken daarmee over informatie die voor publieke partijen nuttig is. Maar het omgekeerde is ook het geval. Het is dus van belang dat publieke en private partijen informatie over en weer goed delen. De effectiviteit van de keten van melden en onderzoeken van ongebruikelijke transacties kan zo

worden verhoogd. In het Plan van Aanpak Witwassen wordt benoemd dat de ministers van Financiën en van Justitie en Veiligheid het belang zien van informatie-uitwisseling ten behoeve van het effectief invullen van de taken van de publieke ketenpartners en van de poortwachtersrol. Dit heeft vorm gekregen in het wetsvoorstel Plan van aanpak witwassen en het voorstel voor de Wet gegevensverwerking door samenwerkingsverbanden (zie hoofdstuk 4).



Auteurs: Hans Brits, Frans van Bruggen, Charlotte Dijkstra, Richard Hoff,  
David Keijzer, Joris van Toor, Lisanne Veldhuis.

Met dank aan de vele externe en interne partijen die hebben bijgedragen aan  
de totstandkoming van dit rapport.