

DNB LEIDRAAD WWFT EN SW

Voorkoming misbruik financiële stelsel voor
witwassen en financieren van terrorisme en
beheersing van integriteitrisico's



Versie 1.0 – april 2011

Inhoudsopgave

1. Inleiding	2
2. Doel en status van de DNB leidraad	2
3. Risicogeorïenteerde benadering	3
3.1 Customer due diligence	3
3.2 Integere bedrijfsvoering	4
3.3 Integere bedrijfscultuur	5
3.4 Risicoclassificatie	6
3.5 Onacceptabel risico	9
3.6 Periodieke actualisatie en review	10
3.7 Buitenlandse kantoren/bijkantoren	10
4. Cliëntenonderzoek	11
4.1 Identificatie en verificatie	11
4.2 Uiteindelijke belanghebbende	14
4.3 Doel en aard zakelijke relatie	15
4.4 Herkomst vermogen	16
4.5 Vereenvoudigd cliëntenonderzoek	16
4.6 Hoogrisico situaties	17
4.7 Niet fysiek aanwezig zijn van de cliënt	18
4.8 PEP's	18
4.9 Correspondentbankrelaties	20
4.10 Uitbesteding	21
4.11 Introduceren van cliënten door derden	21
5. Monitoren	23
5.1 Algemeen	23
5.2 Monitoring bij money transfers: transactieanalyses	23
5.3 Methoden van monitoring	24
5.4 Monitoring bij hoogrisico jurisdicties	25
5.5 Beoordeling en vastlegging	25
6. Bij elektronische geldovermakingen te voegen gegevens	25
7. Vastlegging en bewaarplicht	26
8. Melden ongebruikelijke transacties	27
8.1 Meldplicht	27
8.2 Vrijwaringen	28
8.3 Geheimhouding	29
9. Training en opleiding	29
10. Sanctieregelgeving	29

1. Inleiding

Integriteit is – naast soliditeit – een voorwaarde voor een gezond financieel stelsel. De Nederlandsche Bank (DNB) houdt integriteittoezicht op een breed scala aan (financiële) instellingen. Dit specifieke toezicht is gebaseerd op de Wet op het financieel toezicht (Wft), de Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) en de Sanctiewet 1977 (SW). Het doel van het integriteittoezicht is onder andere het voorkomen van het gebruik van het financiële stelsel voor witwassen en financieren van terrorisme. Het toezicht met betrekking tot de implementatie van de WWFT is toebedeeld aan DNB voor wat betreft de volgende soorten instellingen: kredietinstellingen, levensverzekeraars, betaaldienstverleners, geldtransactiekantoren, trustkantoren, leasemaatschappijen, en casino's (Holland Casino). Voor de SW vallen in aanvulling op deze instellingen ook pensioenfondsen en verzekeringsbedrijven onder het toezicht van DNB.

Het integriteittoezicht op trustkantoren is gebaseerd op de Wet toezicht trustkantoren (Wtt). De doelstelling van de Wtt ligt in lijn met die van de WWFT en de SW. De verplichtingen voor trustkantoren welke voortvloeien uit de Wtt met betrekking tot integriteitrisico's en customer due diligence (CDD) zijn gelijkwaardig te noemen¹.

DNB beoordeelt en handhaaft de toereikendheid en effectiviteit van de door de instellingen getroffen procedures en maatregelen, die zijn gericht op het tegengaan van witwassen en financieren van terrorisme. Handhaving vindt plaats conform het Handhavingsbeleid van de AFM en DNB aan de hand van de normen die zijn neergelegd in wet- en regelgeving².

2. Doel en status van de DNB leidraad

Deze DNB leidraad geldt voor de onder toezicht van DNB vallende instellingen en is in aanvulling op de "Algemene Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) en Sanctiewet (SW)" die het ministerie van Financiën in februari 2011 gepubliceerd heeft³. Beide leidraden verduidelijken de verschillende verplichtingen uit de WWFT en SW en bieden handvatten voor de implementatie van deze verplichtingen. De algemene leidraad en deze DNB leidraad dienen in samenhang gelezen te worden.

In deze DNB leidraad wordt verwezen naar internationale (niet bindende) guidance documenten van Financial Action Task Force on money laundering (FATF), Basel Committee on Banking Supervision (BCBS), International Association of Insurance Supervisors (IAIS) en de Wolfsberg Group⁴. Hoewel de guidance van deze organisaties veelal op bepaalde sectoren is gericht, is veel van de informatie in deze guidance documenten ook nuttig voor andere sectoren.

Deze leidraad is geen juridisch bindend document of beleidsregel van DNB als bedoeld in artikel 1:3 lid 4 Algemene Wet Bestuursrecht en heeft of beoogd geen rechtsgevolg. Deze leidraad komt niet in de plaats van wet- en regelgeving en beleids- of toezichthouderregelingen op dit gebied, zoals bijvoorbeeld de Regeling afgeschermdere rekeningen Wft of de Beleidsregel Integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten. De voorbeelden gegeven in deze leidraad zijn niet uitputtend en zullen niet altijd als voldoende zijn aan te merken. Zij zijn een handreiking voor de uitleg en toepassing van de wettelijke verplichtingen.

¹ In deze leidraad zal de Wtt niet in detail worden behandeld. Wel zal bij de behandeling van bepaalde onderwerpen (al dan niet in voetnoten) verwezen worden naar de Wtt of de Regeling integrale bedrijfsvoering Wtt (Rib).

² http://www.dnb.nl/openboek/extern/file/dnb_tcm40-184053.pdf

³ <http://www.rijksoverheid.nl/ministeries/fin/documenten-en-publicaties/richtlijnen/2011/02/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft-en-sanctiewet-sw.html>

⁴ De Wolfsberg Group is een groep van elf internationale banken, die tot doel heeft het ontwikkelen van standaarden voor de financiële sector op het gebied van 'Ken uw Cliënt' en de bestrijding van witwassen en terrorismefinanciering.

3. Risicogeorienteerde benadering

3.1 Customer due diligence

De WWFT en de Wft kennen een risicogeorienteerde benadering⁵. Dit houdt in dat instellingen wel alle maatregelen toepassen die de wet voorschrijft, maar de intensiteit daarvan afstemmen op de risico's die bepaalde cliënten, producten en diensten, alsmede de combinatie cliënt-product met zich meebrengen. Hoe hoger de risico's des te meer inspanningen de instelling verricht om die risico's te mitigeren.

De WWFT schrijft voor dat instellingen een cliëntenonderzoek verrichten alvorens een zakelijke relatie aan te gaan of een transactie uit te voeren. Ook op grond van de Wft dienen instellingen hun cliënten te kennen én relaties tegen te gaan met personen die het vertrouwen in de instelling kunnen schaden. De beheersing van integriteitsrisico's en CDD zijn hulpmiddelen om dit te bewerkstelligen. De gevolgen van het niet beheersen van deze risico's kunnen het vertrouwen van de consument in de instelling schaden. Belangrijke voorbeelden van integriteitsrisico's in dit kader zijn misbruik van de instelling voor witwassen en terrorismefinanciering. De CDD-normen zijn dus relevant voor de integere bedrijfsvoering van instellingen als geheel, maar ook specifiek voor het bestrijden van witwassen en terrorismefinanciering.

Een belangrijke aanzet voor CDD is gegeven in de door het BCBS opgestelde CDD standaarden in haar rapport 'Customer Due Diligence for banks' van oktober 2001 en de 'General guide to account opening and customer identification' van februari 2003 waarin wordt ingegaan op de gegevens die in dit kader moeten worden verzameld en beoordeeld.

CDD leidt tot het beheersen van de integriteitsrisico's die dienstverlening aan cliënten met zich meebrengt. CDD kan als zodanig worden beschouwd als een essentieel element van risicomanagement. De bedreigingen die uit kunnen gaan van het zaken doen met een cliënt over wie men onvoldoende informatie heeft, werden veelal alleen in verband gebracht met kredietrisico, witwassen, financiële criminaliteit, terrorismefinanciering, corruptie en kapitaalvlucht. Het gaat bij integriteit echter ook om het bredere perspectief. Het rapport van het BCBS uit 2001 beziet de andere risico's in relatie tot de cliënt, zoals reputatie-, operationeel, juridisch en concentratierisico, die kunnen leiden tot aanzienlijke (materiële en immateriële) schade voor de instellingen:

- Reputatierisico: het risico dat door nadelige publiciteit kan ontstaan (kortweg: zou ik samen met deze cliënt in de krant willen staan?).
- Operationeel risico: het risico van schade als gevolg van het feit dat niet volgens procedures wordt gehandeld.
- Juridisch risico: het risico van rechtszaken, strafvervolgning, en de daarmee gepaard gaande boetes, schadevergoedingen en sancties die een bedreiging kunnen vormen voor de continuïteit van de bedrijfsvoering.
- Concentratierisico: het risico dat teveel zaken wordt gedaan met onderling verbonden partijen.

Het management van een instelling formuleert in het kader van de beheersing van integriteitsrisico's ingevolge de relevante toezichtwetgeving (Wft, Wtt), de WWFT en de SW beleid om te bepalen binnen welke kaders de instelling zal opereren. Ook wordt in het beleid aandacht besteed aan aspecten van risicomanagement, compliance, interne controle en opleidingen. Ook wordt een analyse van de integriteitsrisico's uitgevoerd. Teneinde de geïdentificeerde risico's te mitigeren treft de instelling beheersmaatregelen die procedures omvatten tot:

- de identificatie en verificatie van de identiteit van cliënten;
- de acceptatie van cliënten;
- de monitoring van cliënten, rekeningen en transacties.

⁵ Hierbij wordt ook verwezen het op de Wft gebaseerde Besluit Prudentiële Regels voor wat betreft de integere bedrijfsvoering

In dit kader wordt ook verwezen naar de brief van de minister van Financiën aan de Tweede Kamer van 15 oktober 2008 (Kamerstuk 31237, nr. 9) waarin wordt vermeld dat de maatregelen die gelden voor de Wft en de WWFT kunnen worden geïntegreerd en dat op eenzelfde wijze invulling kan worden gegeven aan de vereisten van de WWFT en de Wft.

In internationaal verband is er de volgende aanvullende informatie en guidance te vinden:

- Basel Committee on Banking Supervision, General guide to account opening and customer identification, februari 2003
- Basel Committee on Banking Supervision, Customer Due Diligence for Banks, oktober 2001
- Basel Committee on Banking Supervision, Consolidated KYC Risk Management, oktober 2004
- International Association of Insurance Supervisors, Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities, januari 2002.
- International Association of Insurance Supervisors, Guidance paper on AML and CFT, oktober 2004

3.2 Integere bedrijfsvoering

De Wft voorziet in een uitgebreid raamwerk inzake het beleid van instellingen met betrekking tot de integere bedrijfsvoering en de inrichting van de bedrijfsvoering gericht op een integere bedrijfsvoering. In de Wft is integriteit als een expliciete norm van het financiële toezicht opgenomen. De ratio hiervan is vertrouwen: voor het goed kunnen functioneren als instelling is vertrouwen van onder meer het publiek een randvoorwaarde. Integriteit vormt een van de pijlers van dat vertrouwen. Het wettelijk aangrijpingspunt van toezicht is de integere bedrijfsvoering. In de toezichtwetgeving, en met name in artikelen 3:10 en 3:17 Wft en de uitwerking hiervan in het Besluit Prudentiële Regels (BPR), staat de beheersing van integriteitrisico's centraal. Onder integriteitrisico's worden onder andere het risico op witwassen en het risico op financiering van terrorisme verstaan. De Wft en het BPR schrijven daarvoor in essentie een beheersingskader voor, gericht op het beheersen van integriteitrisico's. Het gaat er hierbij om dat instellingen voorkomen dat zij betrokken raken bij handelingen die tegen de wet ingaan en/of handelingen die maatschappelijk onbetamelijk zijn en dat zij een integere uitoefening van het bedrijf waarborgen⁶.

Componenten die, volgend uit het BPR, horen bij een integere bedrijfsvoering zijn de opzet van een strategie, een systematische analyse van integriteitrisico's, het vaststellen van een adequaat beleid gericht op risicobeheersing en integer handelen, het uitwerken en implementeren van de beleidsuitgangspunten in procedures en maatregelen en een systematische toetsing en beoordeling van de toereikendheid van de beheersomgeving.

De personen die het dagelijkse beleid van de instelling bepalen, geven sturing aan de bedrijfsactiviteiten door doelstellingen te formuleren, strategische keuzes te maken en vervolgens daaruit beleidsuitgangspunten af te leiden. Daarbij onderkent de hoogste leiding de integriteitrisico's en weegt deze in de uiteindelijke doelstellingen en strategieën mee. Documentatie en communicatie van strategie, beleid en procedures zijn belangrijk voor het daadwerkelijk ten uitvoer leggen ervan. Dit kan bijvoorbeeld door middel van 'mission statements', 'business principles' of strategische beschouwingen.

Deze personen geven ook sturing aan de opzet en uitvoering van en het toezicht op het integriteitbeheersingskader en zijn verantwoordelijk voor de daarbij te maken strategische keuzes en beslissingen bijvoorbeeld met betrekking tot:

- de criteria voor de acceptatie van hoogrisico cliënten;
- de criteria voor onacceptabele risico's en over het beëindigen van cliëntrelaties; en
- investeringen in een geautomatiseerd rekening- en transactiemonitoringsysteem.

⁶ Zie ook artikel 2, onderdeel c Wtt. Hier valt te lezen wat DNB verstaat onder 'integere bedrijfsvoering' bij trustkantoren.

Het management is, conform de beleidsregel deskundigheid 2011⁷, deskundig met betrekking tot de integere bedrijfsvoering. Het management kan daarbij waarborgen dat de instelling integriteitrisico's beheerst.

Verder is het management actief betrokken bij het analyseren en onderkennen van integriteitrisico's en treft zij adequate integriteitbeheersmaatregelen (bijvoorbeeld door het toekennen van voldoende resources aan het opzetten van een adequaat monitoringsysteem of opleiding). Hierbij zal het management zich laten ondersteunen door staffuncties die over de relevante kennis en ervaring beschikken (compliance functie, beveiligingsfunctie, risk management functie, commerciële functies, etc.). Ook ziet het management erop toe dat de instelling geen cliënten accepteert of producten en diensten verleent ten aanzien waarvan de instelling geen kennis of ervaring heeft, en ziet zij bij de ontwikkeling en vóór de introductie van nieuwe producten en diensten erop toe dat voldoende rekening is gehouden met de integriteitrisico's.

Hierbij is het van belang dat de leden van het management die bij de besluitvorming zijn betrokken beschikken over voldoende autoriteit en bevoegdheden om noodzakelijke beslissingen te kunnen nemen en door te (laten) voeren.

Integriteitbeleid, procedures en maatregelen kunnen worden gecommuniceerd door middel van handboeken, richtlijnen, organisatieschema's, procesbeschrijvingen, functie- en taakomschrijvingen, workshops of e-learning. Daarbij is het ook belangrijk dat werknemers worden getraind en gescreend om een adequaat niveau van kennis en integriteit te bewerkstelligen.

De beheersing van integriteitrisico's wordt geëvalueerd en gesignaleerde tekortkomingen en gebreken leiden tot tijdige en doeltreffende bijstelling van het integriteitbeheersingskader. De personen die het dagelijkse beleid bepalen vergewissen zich er van dat het integriteitbeheersingskader toereikend is opgezet en daadwerkelijk goed werkt. Dit oordeel kan mede worden gevormd op basis van de bevindingen van onafhankelijk intern toezicht, zoals de compliance functie, de risicobeheerfunctie en de interne auditfunctie. De controlewerkzaamheden die op grond van het intern toezicht worden uitgeoefend worden onafhankelijk van de uitvoering en op systematische wijze uitgevoerd. De reikwijdte van het intern toezicht omvat alle (buitenlandse) bedrijfsonderdelen en alle hiërarchische lagen van de instelling. De bevindingen die naar aanleiding van intern toezicht door de compliance functie, de risicobeheerfunctie en de interne auditfunctie aan het management zijn gerapporteerd, zijn van groot belang voor de evaluatie en bijstelling van doelstellingen, strategie en het integriteitbeheersingskader.

3.3 Integere bedrijfscultuur

Een integere bedrijfscultuur en integer gedrag zijn essentieel voor de effectiviteit van de integriteitbeheersmaatregelen. In het document "De 7 Elementen van een Integere Cultuur. Beleidsvisie en aanpak gedrag en cultuur bij financiële ondernemingen 2010-2014" beschrijft DNB integer gedrag als een professionele, individuele verantwoordelijkheid waarbij iemand zich bewust is van en zorgvuldig rekening houdt met rechten, belangen en wensen van andere belanghebbenden, een open en transparante houding heeft, en bereid is om verantwoordelijkheid te nemen en verantwoording af te leggen over genomen beslissingen en acties.

Een integere cultuur doelt vervolgens op een sfeer en klimaat waarin een onderneming zich ook in ruimere zin gedraagt of handelt op een manier die uitlegbaar en te verantwoorden is. Een cultuur waarin deze professionele, individuele verantwoordelijkheid gestimuleerd en beloond wordt, en waarbij niet alleen de tekst van de wet wordt nageleefd, maar ook de geest van de wet. De 7 Elementen die hierbij leidend zijn, zijn: evenwichtig handelen, consistent handelen, bespreekbaarheid, voorbeeldgedrag, uitvoerbaarheid, handhaving en transparantie⁸.

⁷ Beleidsregel van De Nederlandsche Bank N.V. (DNB) en de Stichting Autoriteit Financiële Markten (AFM) inzake deskundigheid van beleidsbepalers bedoeld in de Wet op het financieel toezicht, de Pensioenwet, de Wet verplichte beroepspensioenregeling en de Wet toezicht trustkantoren (Beleidsregel deskundigheid 2011), Staatscourant 2010 nr. 20810 29 december 2010.

⁸ Zie "De 7 Elementen van een Integere Cultuur. Beleidsvisie en aanpak gedrag en cultuur bij financiële ondernemingen 2010-

Het management vervult een voorbeeldfunctie in de integere bedrijfscultuur. De houding, beslissingen en reacties van het management op ongewenst gedrag is van belang. Er wordt dan ook een cultuur gecreëerd waarin integer handelen wordt bevorderd, bijvoorbeeld door:

- het neerleggen van principiële keuzes en gewenst gedrag, zoals de omgang met cliënten, in interne gedragscodes;
- het bespreken van dilemma's, bijvoorbeeld met betrekking tot de acceptatie van cliënten, in specifieke gremia onder leiding van het management;
- het formuleren van richtlijnen in de taken en verantwoordelijkheden van het management bijvoorbeeld met betrekking tot het houden van toezicht op de naleving van gedragscodes, procedures en richtlijnen, het vertonen van voorbeeldgedrag en het adequaat reageren op ongewenst handelen door personeelsleden en het sanctioneren ervan;
- het bespreken van integriteitaspecten, gedrag en 'resultaten' in beoordeling- en functioneringsgesprekken van het management en personeel. Zo zou bijvoorbeeld het accepteren van cliënten, die weliswaar winstgevend zijn voor de instelling maar die een onacceptabel risico vormen voor de instelling, beloond kunnen worden, hetgeen niet wenselijk is.

3.4 Risicoclassificatie

Zoals gezegd is de aard en diepgang van de maatregelen afhankelijk van de aard en omvang van de integriteitrisico's. De aard en omvang van de risico's zijn sterk gerelateerd aan de kenmerken van de cliënt, van het product en van de dienst(en) die de instelling aanbiedt, alsmede de combinatie cliënt-product. Hoe hoger de risico's, des te meer inspanningen de instelling verricht om die risico's te mitigeren.

Het raamwerk van de WWFT (en van de Wft en de Wtt) schrijft voor dat instellingen, op basis van het onderscheid in aard en omvang van het risico, cliënten indelen in risicocategorieën. De risicocategorieën variëren van laag tot hoog risico en de indeling geschiedt op basis van objectieve en kenbare indicatoren. Toepassing van de risicogebaseerde benadering leidt er vervolgens toe dat de procedures van cliëntidentificatie, -verificatie en -acceptatie en de monitoring zijn gebaseerd op de risicocategorieën waarin de cliënten zijn ingedeeld. Gelijkwaardige risico's worden door gelijkwaardige integriteitbeheersmaatregelen beheerst.

Indeling van cliënten in risicocategorieën geschiedt daarbij aan de hand van geïdentificeerde indicatoren om de potentiële risico's te bepalen. Bij het opstellen van een risicoprofiel wordt een aantal kenmerken van de cliënt in aanmerking genomen. Te denken valt aan de achtergrond van de cliënt, ingezetenschap, of inkomstenbron. Ook de producten die een cliënt afneemt, kunnen ingedeeld worden naar risico. Bepaalde leaseproducten, levensverzekeringen met een lage jaarlijkse of lage eenmalige premie, consumentenkredieten of spaarproducten hebben een inherent lager risico vanwege de lange termijn waarop voordelen kunnen worden gerealiseerd⁹. Andere producten zoals back-to-back leningen, handelsfinanciering, transacties in vastgoed, en andere hoogwaardige, complexe producten kunnen vanwege de complexiteit of ondoorzichtigheid juist een hoger risico opleveren. Een aandachtspunt bij het opstellen van het risicoprofiel en het monitoren van de relatie is de combinatie van cliënt en product. Uiteindelijk heeft een instelling inzicht in de rationaliteit en realiteit van de transacties en producten voor die cliënt.

De in de praktijk meest gehanteerde risicocriteria zijn: land of geografisch risico, cliëntrisico en product/dienstrisico. Het gewicht dat aan elk van deze criteria wordt gegeven om het overall risico op witwassen en terrorismefinanciering te bepalen, kan per instelling verschillen. Instellingen maken dus ook eigen afwegingen met betrekking tot de weging van de risicocriteria, daar gelaten wettelijke bepalingen die grenzen of voorwaarden hieraan kunnen stellen.

2014'. http://www.dnb.nl/binaries/De%207%20Elementen%20van%20een%20Integere%20Cultuur_tcm46-233197.pdf

⁹ Zie ook overweging 9 van Uitvoeringsrichtlijn tot vaststelling van uitvoeringsmaatregelen voor Richtlijn 2005/60/EG van het Europees Parlement en de Raad wat betreft de definitie van politiek prominente personen en wat betreft de technische criteria voor vereenvoudigde klantenonderzoekprocedures en voor vrijstellingen op grond van occasionele of zeer beperkte financiële activiteiten (2006/70/EG).

- *Land of geografisch risico*

Er is geen wettelijke definitie die bepaalt wanneer een specifiek land of geografische regio een hoger integriteitsrisico vertegenwoordigt, maar factoren die kunnen bepalen dat een hoger risico aanwezig is, zijn:

- Landen of geografische gebieden die onderworpen zijn aan sancties, embargo's of soortgelijke maatregelen, vastgesteld door bijvoorbeeld de Verenigde Naties, de Europese Unie of de Verenigde Staten.
- Landen of geografische gebieden die door betrouwbare bronnen (bijvoorbeeld de FATF, het IMF of de Wereld Bank¹⁰) zijn geïdentificeerd als landen of gebieden die in onvoldoende mate een systeem ter voorkoming van witwassen en/of terrorismefinanciering hebben opgezet. Verwezen naar het zogenoemde ICRG-proces (International Co-operation Review Group) van de FATF. Na elke FATF vergadering (in februari, juni en oktober) worden door de FATF lijsten met landen gepubliceerd, waarover de FATF haar bezorgdheid uitspreekt voor wat betreft het hebben van een voldoende systeem ter bestrijding van witwassen en terrorismefinanciering. Deze lijsten worden op de website van de FATF gepubliceerd (<http://www.fatf-gafi.org>) en DNB geeft op haar website aandacht aan elke update van deze lijsten (<http://www.dnb.nl/openboek/extern/id/nl/all/40-197639.html>).
- Landen of geografische gebieden die door betrouwbare bronnen zijn geïdentificeerd als financiers van of anderszins ondersteunend voor terroristische activiteiten.
- Landen of geografische gebieden die door betrouwbare bronnen zijn geïdentificeerd als hebbende een hoog niveau van corruptie of andere criminele activiteiten.

- *Cliëntrisico*

Gebaseerd op eigen criteria zal een instelling vaststellen of een cliënt een hoger risico met zich meebrengt. Categorieën van cliënten die een hoger risico met zich kunnen meebrengen zijn:

- Cliënten die hun zakelijke relatie of transacties in ongebruikelijke omstandigheden (laten) uitvoeren, zoals een onverklaarbaar geografische afstand tussen de instelling en de locatie van de cliënt, frequente en onverklaarbare overstap naar een andere instelling en frequente en onverklaarbare schuiven met tegoeden tussen rekeningen in verschillende geografische locaties.
- Cliënten waarbij de structuur en kenmerken van de entiteit of relatie het moeilijk maakt om de daadwerkelijke eigenaar of controlerende belangen te identificeren.
- 'Cash intensive businesses', zoals geldtransactiekantoren, bureaux de change, gokhallen et cetera.
- Liefdadigheidsinstellingen en andere 'non-profit' instellingen (met name in grensoverschrijdende situaties), die niet onderworpen zijn aan een vorm van monitoring of toezicht.
- 'Gatekeepers' zoals accountants, advocaten of andere beroepsbeoefenaars die rekeningen aanhouden of handelen namens cliënten en waarbij de instelling vertrouwt op de 'gatekeeper'.
- Gebruik van tussenpersonen die niet (in voldoende mate) zijn onderworpen aan maatregelen ter voorkoming van witwassen en terrorismefinanciering of niet onder toezicht staan.
- Cliënten die zijn aan te merken als politiek prominente personen (Politically Exposed Persons, PEP's).

- *Product/dienstrisico*

Bij de bepaling van het product/dienstrisico kan aandacht worden besteed aan de volgende factoren:

- Diensten die door internationaal erkende en betrouwbare bronnen zijn genoemd als een hoger risico dienst, zoals internationale correspondent banking diensten en (internationale) private banking activiteiten.
- Diensten betreffende handel en levering van bankbiljetten en edelmetalen.
- Diensten die inherent anonimiteit bevorderen of zeer gemakkelijk grensoverschrijdend kunnen worden verleend, zoals online banking diensten, 'stored value cards', 'private investment companies' en trusts.

¹⁰ De bronnen kunnen overigens ook nationale organisaties of private 'non governmental organisations' zijn.

- Nieuwe of vernieuwende producten of diensten die niet direct door de instelling zelf worden aangeboden, maar via de kanalen van de instelling.

Op grond van een risicoanalyse en objectieve en kenbare indicatoren deelt de instelling het totale cliëntenbestand in risicocategorieën in. Dit wordt beïnvloed door diverse factoren die het risico doen toenemen, dan wel afnemen. Hierbij kan worden gedacht aan het doel van de te openen rekening of de relatie die wordt aangegaan, de hoeveelheid te deponeren tegoeden door een cliënt of de omvang of bestemming van de uit te voeren transacties, de mate waarin een cliënt op een bepaalde wijze onder toezicht staat van de autoriteiten (zoals een financiële instelling), de intensiteit en duur van de cliëntrelatie, bekendheid met achtergronden van de cliënt, zoals land van herkomst, en het gebruik van 'corporate vehicles' of andere structuren die geen aanwijsbaar (commercieel) doel hebben en onnodig de complexiteit of transparantie bemoeilijken.

De systematiek voor de indeling van cliënten in risicocategorieën wordt schriftelijk gedocumenteerd, bijvoorbeeld in het cliëntacceptatiebeleid of -procedures. Het aantal risicocategorieën dat wordt gehanteerd kan variëren, maar sluit wel goed aan op de aard, omvang en complexiteit van de cliënten, producten en diensten van de instelling.

Voorbeelden van risicogroepen en van de indeling van cliënten daarin kunnen zijn:

Risicocategorie	Voorbeelden
Laag risico	<ul style="list-style-type: none"> - standaarddiensten voor particulieren (spaarrekeningen, salarisrekening etc.) - standaarddiensten voor commerciële relaties van kleine omvang (rekening courant faciliteiten etc.) - levensverzekeringen met een laag bedrag aan jaarlijkse premie of een lage eenmalig premie¹¹ - pensioenverzekeringen¹²
Normaal risico	<ul style="list-style-type: none"> - rekeningen en routinematige internationale (documentaire) betalingen voor middelgrote en grote ondernemingen - routinematige en standaard producten en diensten met betrekking tot private banking - correspondentbankrekeningen voor banken onderhevig aan gelijkwaardige wetgeving als de WWFT
Hoog risico	<ul style="list-style-type: none"> - complex gestructureerde financieringstransacties of zekerhedenconstructies aan particulieren - PEP's of cliënten die transacties verrichten waar PEP's bij betrokken zijn - bankproducten en dienstverlening die naar hun aard vatbaar zijn voor onoorbaar gebruik (bijvoorbeeld back-to-back leningen, grote constante stortingen, zakelijke vastgoedactiviteiten) - cliënten met transacties van/naar gesanctioneerde landen (waaronder handelssancties), free trade zones, offshore centra, tax havens, landen waarvoor de FATF in het kader van het zogenoemde ICRG-proces waarschuwt - cliënten met frequente, niet routinematige, complexe treasury en private banking producten en diensten - niet-routinematig, grensoverschrijdend betalingsverkeer door niet-clianten - correspondentbankrekeningen met banken uit jurisdicties met zwakke wetgeving op het gebied van bestrijden van witwassen en terrorismefinanciering

Bepaalde typen cliënten, zoals coffeeshops of exploitanten van relaxbedrijven, kunnen een hoger witwasrisico geven vanwege de hoge mate van inkomend chartaal geld en het feit dat de herkomst van dit chartaal geld minder transparant is dan de herkomst van inkomend giraal geld. Het is echter niet de bedoeling van de WWFT om categoriaal dit type cliënten een eenvoudige betaalrekening te weigeren. Een instelling beoordeelt per cliënt hoe risicogevoelig die relatie is en welke waarborgen ter beheersing van het risico worden genomen. Bij deze waarborgen kan een

¹¹ Zie ook artikel 7, lid 1, onderdeel a WWFT.

¹² Zie ook artikel 7, lid 1, onderdeel b WWFT.

instelling bijvoorbeeld denken aan een limiet te stellen aan de contante transacties en in grote mate girale betalingen te verlangen. Artikel 3 van de WWFT ziet toe op het acceptatiebeleid van instellingen waarbij het gaat om het resultaat: de klant te kennen en weten waarvoor de zakelijke relatie gebruikt zal worden. Indien het cliëntenonderzoek echter niet tot dit bedoelde resultaat leidt, nemen instellingen ook artikel 5, lid 1 WWFT in acht en zal de instelling (bij de eerstvolgende mogelijkheid) de relatie verbreken. Indien de relatie wordt verbroken vanwege het vermoeden van witwassen of het financieren van terrorisme ligt het ook voor de hand dat er een melding op grond van artikel 16 WWFT wordt gedaan bij FIU-Nederland (FIU-NL). In een brief van de minister van Financiën van 18 januari 2010 aan de Tweede Kamer heeft de minister aangegeven welke afspraken er met de Nederlandse Vereniging van Banken zijn gemaakt ten aanzien van betaalfaciliteiten voor integriteitgevoelige sectoren (<https://zoek.officielebekendmakingen.nl/kst-27863-35.html>).

DNB beschouwt vastgoed als een van de speerpunten binnen het integriteittoezicht omdat een zakelijke vastgoedactiviteit naar haar aard een hoger risico op fraude en witwassen met zich meebrengt. Dit vanwege de relatief hoge waarde van vastgoedobjecten, de vaak ondoorzichtige prijsvorming en de complexiteit van transacties. DNB heeft in 2011 de beleidsregel 'Integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten' gepubliceerd¹³. Met deze beleidsregel geeft DNB aan dat instellingen in hun wettelijk vereiste integriteitbeleid en de daarop gebaseerde procedures en maatregelen (waaronder een gedegen uitvoering van CDD) rekening moeten houden met verhoogde integriteitrisico's die verbonden zijn aan zakelijke vastgoedactiviteiten. Daarnaast worden in deze beleidsregel handvatten gegeven om het integriteitbeleid op dit onderwerp in te vullen.

Aanvullende informatie:

- FATF, 'Money Laundering and Terrorist Financing through the real estate sector', 2007, <http://www.fatf-gafi.org/dataoecd/45/31/40705101.pdf>
- Financieel Expertise Centrum, 'Rapportage project vastgoed', 2008, http://www.fec-partners.nl/media_dirs/2/media_files_data/rapportage_project_vastgoed.pdf
- Financieel Expertise Centrum, 'Red flags Misbruik Vastgoed-actualisering 2010', http://www.fec-partners.nl/media_dirs/2/media_files_data/red_flags_misbruik_vastgoed_actualisering_2010.pdf

3.5 Onacceptabel risico

Op grond van de risicoanalyse en toepassing van de regelgeving kan en zal het voorkomen dat de instelling vaststelt dat de cliënt een onacceptabel risico met zich meebrengt. Dit kunnen omstandigheden of kenmerken zijn die blijken uit initiële onderzoeken tijdens de cliëntacceptatie of uit de periodieke review van het risicoprofiel van de cliënt. Indien er sprake is van onacceptabele risico's zal de instelling de cliënt niet accepteren dan wel de bestaande relatie beëindigen. Dit beleid is vastgelegd in beleid en procedures. In dit in de praktijk vaak genoemde 'cliënt-exit-beleid' geeft de instelling aan onder welke omstandigheden en volgens welke procedure de relatie met de cliënt wordt beëindigd.

Voorbeelden van mogelijk onacceptabele risico's:

- problemen bij het verifiëren van de identiteit van de cliënt;
- cliënten die anoniem wensen te blijven dan wel fictieve identiteitsgegevens verstrekken;
- shellbanks (banken die geen fysieke aanwezigheid hebben in het land waar ze gevestigd zijn en een vergunning hebben);
- naam van de cliënt komt overeen met een naam op freezelist van de EU;
- cliënten waarvan blijkt dat, op basis van nadere informatie uit bijvoorbeeld EVA, VIS of anderszins, dat de combinatie van cliënt met de producten die deze wil afnemen onacceptabele risico's met zich meebrengt;

¹³ Beleidsregel van De Nederlandsche Bank N.V. met betrekking tot integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten, Staatscourant nr 2641, 16 februari 2011.

- cliënten die geen of onvoldoende informatie willen verstrekken over (dan wel ontoereikende documentatie ter verificatie daarvan kunnen overleggen) de aard en achtergrond van de cliënt, in het bijzonder de herkomst van het vermogen;
- organisatiestructuur van de cliënt blijkt na onderzoek complex, niet transparant of ondoorzichtig, gelet op de activiteiten van de cliënt, zonder dat hier een logische, bedrijfseconomische verklaring aan ten grondslag ligt;
- professionele tegenpartijen die niet over de vereiste vergunningen beschikken, zogenaamde illegale financiële ondernemingen¹⁴.

3.6 Periodieke actualisatie en review

De indeling van cliënten in risicocategorieën is dynamisch, dat wil zeggen dat het risicoprofiel van cliënten in de loop der tijd kan wijzigen. Review is het doen van onderzoek naar de cliënt om vast te stellen of de cliënt nog steeds aan het vastgestelde risicoprofiel voldoet. De cliëntgegevens worden daartoe periodiek door de instelling geactualiseerd. Uitgangspunt is dat de frequentie en diepgang van de review afhankelijk is van het risico dat de cliënt met zich meebrengt.

Voor laagrisico cliënten vindt een review plaats bijvoorbeeld op het moment dat de cliënt een nieuwe dienst of product vraagt, dat mogelijk tot een verhoging van zijn risicoprofiel leidt, de cliëntkenmerken (bijvoorbeeld verhuizing naar een hoogrisico jurisdictie) wijzigen of op basis van signalen van incidenten.

Voor hoogrisico cliënten zal in de praktijk regelmatig (enkele malen per jaar) worden gekeken naar de specifieke risico's. Uitgangspunt is dat frequentie en diepgang van de review afhankelijk is van het risicoprofiel van de cliënt. Verder kan deze gevoed worden door eventuele signalen die duiden op een hoger risico, bijvoorbeeld vanwege het rekeninggebruik of specifieke transacties, een en ander bezien vanuit de geconsolideerde positie van de betreffende cliënt. In alle gevallen zijn de betrokken medewerkers op de hoogte van mogelijke risico's rondom dit soort hoogrisico cliënten.

Instellingen besteden in het beleid en procedures aandacht aan de frequentie en de wijze waarop cliëntgegevens periodiek worden geactualiseerd en waarop het risicoprofiel van de cliënt periodiek opnieuw wordt onderzocht.

Voor wat betreft de opzet van een risicogebaseerde benadering (risk-based approach, RBA) heeft FATF diverse guidance documenten opgesteld:

- RBA guidance for the Financial Sectors, juni 2007 (<http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf>)
- RBA guidance for Trust and Companies Service Providers, juni 2008 (<http://www.fatf-gafi.org/dataoecd/19/44/41092947.pdf>)
- RBA guidance for Casinos, oktober 2008 (<http://www.fatf-gafi.org/dataoecd/5/61/41584370.pdf>)
- RBA guidance for Money Service Businesses, juni 2009 (<http://www.fatf-gafi.org/dataoecd/45/1/43249256.pdf>)
- RBA guidance for the Life Insurance Sector, oktober 2009 (<http://www.fatf-gafi.org/dataoecd/0/15/43905397.pdf>)

3.7 Buitenlandse kantoren/bijkantoren

De lokale wet- en regelgeving met betrekking tot een integere bedrijfsvoering en ter mitigatie van integriteitsrisico's of meer in het bijzonder, ter voorkoming van witwassen en terrorismefinanciering, kan sterk verschillend zijn. Internationaal opererende instellingen definiëren op integrale wijze minimumnormen bij de implementatie van integriteitsbeleid en -procedures, die gelden voor de gehele groep. Dit betekent dat de opgezette integriteitsbeheersmaatregelen in ieder geval worden toegepast ten aanzien van de gehele bedrijfsvoering, alle functionele activiteiten, cliënten en producten wereldwijd. Het kan voorkomen dat een instelling opereert in jurisdicties waar de lokale wet- en regelgeving lagere integriteitsnormen stellen dan de integraal vastgestelde minimumnormen.

¹⁴ Zowel DNB als de AFM beschikken over openbare registers waarin de toegelaten financiële instellingen zijn opgenomen. Hierin kan worden nagegaan of een instelling over een vergunning of registratie beschikt.

Instellingen passen in die gevallen de hogere eisen van de groep binnen die kantoren en branches toe. Indien de lokale wet- en regelgeving hogere eisen stelt aan integriteitbeheersmaatregelen dan de minimumnormen, beoordeelt de instelling de minimumnormen opnieuw en past deze, waar nodig, aan.

4. Cliëntenonderzoek

De kern van de WWFT is dat er cliëntenonderzoek moet worden verricht en dat een instelling het cliëntenonderzoek kan afstemmen op de risicogevoeligheid voor witwassen of financiering van terrorisme van het type cliënt, zakelijke relatie, product of transactie. Dit wordt aangeduid als cliëntenonderzoek op basis van een risicogeoriënteerde benadering. Deze risicogeoriënteerde benadering geeft instellingen de mogelijkheid om de intensiteit van het cliëntenonderzoek af te stemmen op de risico's die bepaalde typen cliënten, producten of transacties met zich meebrengen. Instellingen treffen daarbij extra maatregelen in gevallen waarin er hoger risico bestaat op witwassen of financiering van terrorisme. Dit alles stelt de eigen verantwoordelijkheid van de instelling voorop. Dit betekent dat de instelling op de hoogte is van technieken van witwassen en financieren van terrorisme, actuele ontwikkelingen, risico-indicatoren en deze verwerkt in beleid en op risicogebaseerde procedures en maatregelen.

Het cliëntenonderzoek stelt de instelling in staat om de cliënt te identificeren, zijn identiteit te verifiëren, de uiteindelijk belanghebbende van een transactie of relatie te identificeren en zich te vergewissen van de structuur van de groep waartoe een cliënt behoort, het doel en de beoogde aard van de zakelijke relatie vast te stellen en de herkomst van het vermogen vast te stellen. Ook controleert de instelling de activiteiten van de cliënt gedurende de relatie en toetst periodiek of de cliënt nog voldoet aan het risicoprofiel, zoals dat is opgesteld bij aanvang van de dienstverlening. De instelling heeft op het moment van het aangaan van de relatie voldoende informatie verzameld teneinde de cliënt op juiste gronden te kunnen accepteren. Hieronder zal worden ingegaan op de verschillende aspecten van het cliëntenonderzoek.

4.1 Identificatie en verificatie

Algemeen

Het begrip 'cliënt' is ruim gedefinieerd in de WWFT. Het betreft de natuurlijke persoon of rechtspersoon met wie een zakelijke relatie wordt aangegaan, hetgeen niet alleen de persoon is die voor zichzelf een transactie uitvoert, maar ook de persoon die zich bij een transactie laat vertegenwoordigen door een derde. Ook deze derde wordt als cliënt beschouwd.

In het algemeen wordt cliëntacceptatie en identificatie en verificatie als volgt omschreven:

- Cliëntidentificatie: is het proces waarin gegevens en informatie van de cliënt worden verzameld met het doel om de cliënt te 'kennen'. De gegevens maken een adequate en onderbouwde risicobeoordeling van de cliënt mogelijk.
- Verificatie: is het controleren van de juistheid van de door de cliënt aangedragen en overige gegevens, bijvoorbeeld aan de hand van originele, geldige identiteitsdocumenten en eventueel ondersteund door nader onderzoek.
- Cliëntacceptatie: is het proces waarin op basis van de identificatie, verificatie en de kennis over de aard en achtergrond van de cliënt een besluit wordt genomen over het al dan niet aangaan van een relatie met de cliënt.

Bij het identificeren verstrekt de cliënt gegevens over zijn identiteit. Bij het verifiëren van de identiteit gaat het om het vaststellen dat de opgegeven identiteit overeenkomt met de werkelijke identiteit. Aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron controleert de instelling de juistheid van de door de cliënt opgegeven identiteit. In de Uitvoeringsregeling WWFT wordt een aantal documenten genoemd die hiervoor gebruikt kunnen worden¹⁵.

¹⁵ Artikel 4 van de Uitvoeringsregeling wijst voor natuurlijke personen de volgende documenten aan: een geldig paspoort; een geldige Nederlandse identiteitskaart; een geldige identiteitskaart die is afgegeven door het daartoe bevoegde gezag in een andere lidstaat en is voorzien van een pasfoto en de naam van de houder; een

Er kunnen ook andere documenten, inlichtingen of gegevens worden geaccepteerd ten behoeve van de verificatie van de identiteit van een natuurlijk persoon mits deze afkomstig zijn uit een betrouwbare en onafhankelijke bron. Als voorbeeld kan worden genoemd de verificatie van de identiteit van een natuurlijke persoon uit een staat die geen EU-lidstaat is en die niet in het bezit is van een paspoort. Rekeningen op naam van de betreffende persoon (mogelijk) in combinatie met andere gegevens over de persoon, kunnen in bepaalde gevallen worden geaccepteerd. Dit laatste wordt overgelaten aan de risicobeoordeling van de instelling die de betreffende persoon als cliënt wil accepteren. Instellingen zijn goed in staat om dergelijke afwegingen te maken aangezien zij in het kader van het afdekken van het bedrijfsrisico zelf ook zal willen weten wie de cliënt is.

Voor buitenlandse rechtspersonen geschiedt de verificatie ook aan de hand van documenten of gegevens of inlichtingen uit betrouwbare en onafhankelijke bron. Hiertoe kunnen vergelijkbare documenten worden opgevraagd als voor de verificatie van Nederlandse rechtspersonen zoals beschreven in artikel 4, lid 3 van de Uitvoeringsregeling WWFT.

Indien het documenten betreft die niet afkomstig zijn van overheidsinstanties of rechterlijke instanties, dan zal de instelling zich afvragen of de documenten voldoende betrouwbaar zijn. Dergelijke documenten zullen op zichzelf veelal onvoldoende zijn om de identiteit op een adequate wijze te verifiëren. Documenten waarvan niet vaststaat dat daaraan een adequate identificatie en verificatie vooraf is gegaan, zoals studentenpassen en werknemerspassen, volstaan over het algemeen niet om de identiteit te verifiëren.

Wanneer identificatie en verificatie

De gevallen waarin cliëntenonderzoek dient plaats te vinden staan vermeld in artikel 3 WWFT¹⁶. Dit betreft de gevallen waarin een instelling een zakelijke relatie aangaat dan wel een (samenstel van) transacties verricht boven een bepaald grensbedrag.

Artikel 3, lid 3, onderdeel b WWFT stelt dat een instelling bij twee of meer transacties waartussen een verband bestaat met een gezamenlijke waarde van ten minste 15.000 euro een cliëntenonderzoek verricht. De instelling beoordeelt dit aan de hand van het soort transactie en de bedragen waar het om gaat. Vooropgesteld staat dat het gaat om incidentele transacties, hetgeen betekent dat er geen zakelijke relatie aanwezig is. Ook is het logisch dat het gaat om gelijksoortige transacties. Te denken valt aan een persoon die in meerdere transacties per dag of binnen een paar dagen contante gelden stort op een rekening waarvan hij of zij niet de rekeninghouder is (en ook niet handelt voor de rekeninghouder) waarbij die bedragen in totaal uitkomen boven 15.000 euro. Daarentegen, op een bedrijf dat elk dag de contante opbrengsten afkomstig uit de reguliere bedrijfsvoering afstort op eigen rekening is deze bepaling niet van toepassing omdat deze stortingen binnen de zakelijke relatie vallen.

Een instelling die money transfers verricht zal niet in alle gevallen een zakelijke relatie aangaan met een cliënt, zoals in de WWFT gedefinieerd. Uit de wetgeschiedenis kan echter worden opgemaakt dat bij money transfers een zakelijke relatie mag worden verondersteld. Het

geldig Nederlands rijbewijs; een geldig rijbewijs dat is afgegeven door het daartoe bevoegde gezag in een andere lidstaat en is voorzien van een pasfoto en de naam van de houder; reisdocumenten voor vluchtelingen en vreemdelingen; vreemdelingendocumenten, afgegeven op grond van de Vreemdelingenwet 2000.

Voor Nederlandse rechtspersonen zijn de volgende documenten aangewezen: een uittreksel uit het handelsregister; een akte of verklaring, opgemaakt onderscheidenlijk afgegeven door een in Nederland of in een andere lidstaat gevestigde advocaat, notaris, kandidaatnotaris of een hiermee vergelijkbare, onafhankelijke beoefenaar van een juridisch beroep; een document waaruit blijkt dat een kerkgenootschap of lichaam waarin zij is verenigd, is aangesloten bij het Interkerkelijk Contact in Overheidszaken dan wel dat het kerkgenootschap of lichaam is aangemerkt als een instelling als bedoeld in artikel 6.33, eerste lid, onderdeel b, van de Wet inkomstenbelasting 2001; een document waaruit blijkt dat een zelfstandig onderdeel van een kerkgenootschap deel uitmaakt van dat kerkgenootschap en het kerkgenootschap voldoet aan het bepaalde in onderdeel c.

¹⁶ Op grond van artikel 3, lid 5 WWFT gelden het eerste tot en met het vierde lid van dit artikel niet voor trustkantoren. Ook het vereenvoudigde cliëntenonderzoek uit artikel 6 WWFT en het verscherpte cliëntenonderzoek uit artikel 8 WWFT gelden (naast enkele andere artikelen uit de WWFT) daarom niet voor trustkantoren. De verplichtingen voor trustkantoren ten aanzien van cliëntenonderzoek zijn neergelegd in de Wtt en de Rib.

uitgangspunt is dat, gezien de onverminderd hoge kwetsbaarheid, instellingen die money transfers verrichten, cliënten identificeren bij elke transactie.

Verder geldt dat bij alle cliënten, met name bestaande cliënten, cliëntenonderzoek plaatsvindt indien:

- er indicaties zijn dat de cliënt betrokken is bij witwassen of financieren van terrorisme;
- de instelling twijfelt aan de betrouwbaarheid van eerder verkregen gegevens van de cliënt;
- het risico van betrokkenheid van een bestaande cliënt bij witwassen of financieren van terrorisme daartoe aanleiding geeft.

Uitgangspunt is dat de identificatie en verificatie zijn afgerond voordat de zakelijke relatie ontstaat en de dienstverlening aanvangt. Er bestaat echter uitzonderingen in die gevallen waar de dienstverlening, zoals het adviseren van cliënten, niet verstoord zou mogen worden¹⁷. Bij deze uitzonderingen wordt wel het doel van de wet in de gaten gehouden, namelijk het voorkomen dat de dienstverlening wordt gebruikt voor witwassen of terrorismefinanciering. Voorwaarden zijn dat er een laag witwas- of terrorismefinancieringsrisico is en dat de verificatie van de identiteit zo spoedig mogelijk plaatsvindt na het eerste contact met de cliënt.

Voor kredietinstellingen geldt tevens dat een rekening geopend kan worden maar dat de verificatie later kan plaatsvinden, zolang de instelling er in die tussentijd voor zorgt dat de rekening niet gebruikt kan worden¹⁸. Dit geldt ook voor creditcards die door kredietinstellingen uitgegeven worden. Zolang de creditcard geblokkeerd is (te vergelijken met een rekening die nog niet gebruikt kan worden) kan de kredietinstelling nog de verificatie uitvoeren, maar als de creditcard gedeblokkeerd is en de kaart gebruikt kan worden (ongeacht of hij daadwerkelijk gebruikt wordt) moet de identificatie en de verificatie afgerond zijn.

Ook bij het afsluiten van levensverzekeringen is het toegestaan de begunstigde van een polis te identificeren en de identiteit te verifiëren nadat de zakelijke relatie is aangegaan. In dat geval vindt het identificeren en het verifiëren van de identiteit plaats op of voor het tijdstip van uitbetaling, dan wel op of voor het tijdstip waarop de begunstigde zijn rechten krachtens de polis wil uitoefenen. De uitbetaling aan een begunstigde van een levensverzekering is geen incidentele transactie, maar vloeit voort uit de zakelijke relatie die de instelling met de verzekeringnemer is aangegaan. Indien de begunstigde een juridische entiteit is, zal ook de uiteindelijke belanghebbende worden geïdentificeerd en - op basis van op risicogebaseerde en adequate maatregelen - zijn of haar identiteit worden geverifieerd.

Indien er vanuit de polis een langdurige relatie met de begunstigde ontstaat (bijvoorbeeld bij annuïtaire betalingen), heeft een voortdurende controle op de uitbetalingen geen toegevoegde waarde aangezien deze betalingen door de instelling zelf worden gedaan.

De WWFT kent een overgangsregeling op grond waarvan het verrichten van cliëntenonderzoek (artikel 3, lid 1 WWFT) niet van toepassing is ten aanzien van cliënten die reeds op grond van de Wet Identificatie Dienstverlening zijn geïdentificeerd of ten aanzien van wie geen verplichting tot identificatie op grond van die wet was vereist¹⁹. Op het moment dat een cliënt volgens het binnen de instelling vastgelegde reviewproces voor een review in aanmerking komt zal het dossier op orde worden gesteld, waaronder de identificatie en verificatie van de uiteindelijk belanghebbende.

Verbod aangaan zakelijke relatie

Op grond van artikel 5 WWFT is het verboden een zakelijke relatie aan te gaan of een transactie uit te voeren indien er geen cliëntenonderzoek is verricht of indien het cliëntenonderzoek, inclusief het onderzoek naar de uiteindelijk belanghebbende, niet heeft geleid tot het bedoelde resultaat. Er is een wettelijke verplichting om de zakelijke relatie te beëindigen wanneer niet voldaan kan worden aan de wettelijke verplichtingen. Een instelling overweegt in deze gevallen een melding te doen bij FIU-NL.

¹⁷ Artikel 4, lid 2 WWFT.

¹⁸ Artikel 4, lid 4 WWFT.

¹⁹ Artikel 38 WWFT.

Indien de instelling de zakelijke relatie niet kan beëindigen, neemt de instelling (verdere) adequate maatregelen om alsnog het cliëntenonderzoek te verrichten. Bij bestaande hoogrisico cliënten vinden de vereisten van artikel 3 WWFT zo snel mogelijk plaats. Bij bestaande laagrisico cliënten zal dit met name aan de orde komen wanneer zich incidenten voordoen dan wel wanneer deze nieuwe diensten of producten afnemen die tot een wijziging van het risico leiden, dan wel op het moment dat de cliënt volgens vastgelegde reviewproces voor een review in aanmerking komt.

Bij levensverzekeringen waar het veelal juridisch niet mogelijk is om een bestaande relatie te beëindigen, worden de tegoeden bevroren totdat het onderzoek wel heeft geleid tot het bedoelde resultaat.

In de WWFT is ook een verbod opgenomen om een correspondentbankrelatie aan te gaan met een shellbank²⁰. Het is verder niet toegestaan om correspondentbankrelaties aan te gaan of voort te zetten met een kredietinstelling waarvan bekend is dat deze een shellbank toestaat van haar rekeningen gebruik te maken. Shellbanken brengen vanwege de aard van hun organisaties risico's met zich mee. Zij bieden dienstverlening aan in een land zonder dat zij daar over een fysieke vestiging beschikken, dat wil zeggen de aanwezigheid van bestuur en management. Gedragingen van dergelijke instellingen zijn voor toezichthouders moeilijk te controleren.

Afgeschermdde rekeningen

De internationale standaarden op het gebied van CDD en de bestrijding van witwassen en terrorismefinanciering stellen dat instellingen geen relaties mogen onderhouden met personen die anoniem blijven of personen die een fictieve naam opgeven. Omdat het in een aantal beperkte gevallen – het beschermen van de privacy en veiligheid van betrokken cliënten en het voorkomen van vormen van gebruik van voorwetenschap – nuttig kan zijn de identiteit van een cliënt intern af te schermen, voorziet de Regeling afgeschermdde rekeningen Wft in een procedure volgens welke de identiteit van de cliënt bij transactieverwerkingen niet zichtbaar of anderszins afgeschermd is. De cliënt is dan wel bekend bij de instelling, alleen is het niet voor alle medewerkers duidelijk om wie het gaat.

De Regeling staat een kredietinstelling of een bijkantoor van een kredietinstelling toe restrictief gebruik te maken van afgeschermdde rekeningen. In deze regeling is beschreven op welke wijze kredietinstellingen en bijkantoren van kredietinstellingen een centraal register bijhouden waarbij de gegevens omtrent de identiteit van een cliënt bij transactieverwerkingen niet zichtbaar of anderszins afgeschermd zijn, terwijl deze wel elders bij de instelling bekend zijn. In het centrale register worden de gegevens opgenomen die op grond van artikel 33 WWFT worden vastgelegd. Het centrale register is zodanig ingericht dat op naam en nummer- of codesleutel kan worden geraadpleegd. Daarnaast wordt een beheerder van het centrale register aangewezen.

De Regeling ziet dus alleen op het afschermen van de identiteit bij de transactieverwerking. De eisen van WWFT omtrent het cliëntenonderzoek zijn onverminderd van toepassing, alsmede de Verordening van het Europees Parlement en de Raad van 15 november 2006 (EG nr. 1781/2006) betreffende bij geldovermakingen te voegen informatie over de betaler.

4.2 Uiteindelijke belanghebbende

In het geval dat de cliënt een juridische entiteit, zoals een rechtspersoon, stichting of trust is, identificeert de instelling de uiteindelijke belanghebbende (ultimate beneficial owner, UBO). Het cliëntenonderzoek naar de UBO is een wettelijke eis omdat criminelen vaak gebruik maken van constructies waarin (buitenlandse) rechtspersonen een rol spelen als een middel om de criminele herkomst van gelden te verbergen. Hieraan kan voldaan worden door de cliënt opgave te laten doen van wie de uiteindelijke belanghebbende is. Daarnaast neemt de instelling op risicogebaseerde en adequate maatregelen om de identiteit te verifiëren²¹. Deze

²⁰ Shellbank is gedefinieerd in artikel 1, lid 1 onderdeel j WWFT.

²¹ De verplichting voor trustkantoren om de uiteindelijke belanghebbende te identificeren, is opgenomen in artikel 10 Wtt juncto artikel 12 Rib. Op dit moment hanteren de Wtt en de WWFT nog verschillende definities ten aanzien van het begrip 'uiteindelijke belanghebbende'. Zie daarvoor artikel 1, onderdeel c Wtt.

verificatiemaatregelen stelt de instelling in staat om voldoende informatie te verkrijgen om de identiteit te verifiëren en overtuigd te zijn dat de instelling weet wie de uiteindelijke belanghebbende is. Dit betekent niet dat de instelling een keuze heeft in het al dan niet verifiëren van de identiteit van de UBO, afhankelijk van het risico. De identiteit wordt geverifieerd maar de wijze waarop dat gebeurt, is risicogebaseerd.

De identiteit van de UBO wordt geverifieerd aan de hand van onafhankelijke, betrouwbare documenten. Instellingen kunnen daartoe gebruik maken van openbare registers en andere openbare bronnen; de cliënt om relevante gegevens of documenten vragen; of deze informatie op andere wijze te verzamelen. Hierbij kan men rekening houden met het feit dat de omvang van dergelijke maatregelen gerelateerd is aan het risico op het witwassen van geld en de financiering van terrorisme, hetgeen weer afhankelijk is van het soort cliënt, product of transactie. Bij cliënten en transacties die een laag risico vormen, is vragen naar de identiteit van de uiteindelijke belanghebbende en het laten ondertekenen van een verklaring (door de UBO) daaromtrent voldoende. De instelling kan in overweging nemen om te controleren of de UBO een PEP is.

Ook beschikt de instelling over op risicogebaseerde en adequate maatregelen om in het geval van rechtspersonen, stichtingen of trusts en andere juridische constructies inzicht te verkrijgen in de eigendoms- en zeggenschapstructuur van de cliënt. Uitgangspunt is dat de instelling deze structuur kent, en ook begrijpt. Dit betekent dat bij ingewikkelde structuren van vele ondernemingen de instelling meer inspanningen verricht om de (internationale) beheersstructuur van de onderneming te begrijpen dan voor een Nederlandse BV met een directeur-groootaandeelhouder.

4.3 Doel en aard zakelijke relatie

Het inwinnen van informatie over het doel en de beoogde aard van de zakelijke relatie stelt een instelling in staat om eventuele risico's die de dienstverlening aan de cliënt oplevert, in te schatten. Een deel van de benodigde informatie zal doorgaans reeds naar voren komen tijdens het contact voorafgaand aan de zakelijke relatie. Ook uit de door de cliënt afgenomen diensten of producten zal blijken wat het doel van de relatie is. Aanvullende vragen van de instelling kunnen zich richten op het verkrijgen van helderheid over de gebruiker van het product of de afnemer van de dienst.

Bij de beoordeling van de achtergrond, de (bedrijfs)activiteiten en de branche van de (potentiële) cliënt kunnen één of (eerder) meer van de volgende –niet limitatieve– aspecten worden betrokken:

- de reden waarom de cliënt de zakelijke relatie wil aangaan
- de aard van de relatie tussen eventuele gemachtigde(n) en de cliënt. Indien er geen logische relatie bestaat (zoals bij familie van een natuurlijk persoon of een werknemer bij een rechtspersoon) is dit wellicht te definiëren als een hoger risico
- de aard van de (bedrijfs)activiteiten
- het met elkaar overeenstemmen van postadres met woon- of vestigingsadres
- de achtergrond van personen die invloed kunnen uitoefenen in de vennootschap of op het management
- de structuur van de organisatie waarvan de cliënt deel uitmaakt
- duidelijkheid over de herkomst van het vermogen van de cliënt en/of de gelden die via de rekening van de cliënt lopen
- de wijze waarop de cliënt financiële producten gebruikt of zal gaan gebruiken
- een beoordeling van hetgeen de cliënt aankondigt ten aanzien van het gebruik van financiële producten en of deze producten passen bij de aard van de bedrijfsactiviteiten en de branche waarin de cliënt opereert
- de mogelijkheid dat een eerdere relatie eenzijdig is opgezegd door een andere instelling
- de keuze van het filiaal van de instelling in een bepaalde gemeente of deel van het land, afgezet tegen de aard van het bedrijf en eventueel de vestigingsplaats van de cliënt
- redenen om te veronderstellen dat de cliënt pogingen doet zijn identiteit te verhullen door zich achter anderen te verschuilen
- transacties naar, via, of vanuit het buitenland, waaronder landen die op een FATF lijst staan
- hetgeen door de cliënt wordt voorgesteld is niet plausibel of 'te mooi om waar te zijn'
- de reputatie van de cliënt of mogelijke negatieve publiciteit over de cliënt
- het zich voordoen van ongebruikelijke/verdachte transacties op de risicogebieden, zoals witwassen, fiscaliteit, terrorismefinanciering, benadeling van derden.

4.4 Herkomst vermogen

Bij het aangaan van een relatie met een cliënt, is het uitgangspunt is dat de instelling de herkomst van het vermogen kent. De instelling stelt hierover vragen en legt verklaringen en bewijsstukken in het cliëntendossier vast²². Het feit dat de gelden afkomstig zijn van een gereguleerde instelling betekent niet dat de instelling zelf geen onderzoek hoeft uit te voeren. Om de plausibiliteit van de legale herkomst van het vermogen vast te stellen, heeft de instelling bepaalde indicatoren geïdentificeerd op basis waarvan de diepgang van het onderzoek wordt bepaald. Zeker bij hoog risico ligt het in de rede door middel van onafhankelijke, betrouwbare bronnen de plausibiliteit van het vermogen vast te stellen en vast te leggen. Bij levensverzekeringen gaat het dan bijvoorbeeld om zeer hoge premiebetalingen. De instelling draagt zorg voor vastlegging van het uitgevoerde onderzoek naar de herkomst van het vermogen.

4.5 Vereenvoudigd cliëntenonderzoek

Voor bepaalde cliënten kan worden volstaan met een vereenvoudigd cliëntenonderzoek. In artikel 6, lid 1 WWFT zijn typen cliënten aangegeven die een lager risico op witwassen en terrorismefinanciering vormen. Voor deze cliënten geldt een versoepeld regime voor het cliëntenonderzoek. De aangewezen soorten cliënten zijn voornamelijk bepaalde instellingen die onder de WWFT of vergelijkbare wetgeving vallen en cliënten met een bepaalde rechtspersoonlijkheid. Tevens is er in artikel 7, lid 1 WWFT een aantal producten benoemd waarvoor een versoepeld regime bestaat.

Instellingen verzamelen echter wel voldoende gegevens om te beoordelen of de cliënt voldoet aan de eisen voor een versoepeld regime. Hiertoe kan de instelling vragen naar een uittreksel van de Kamer van Koophandel, inschrijvingen in openbare registers, of andere openbare noteringen.

Enige vorm van monitoring van deze zakelijke relaties is altijd nodig om te beoordelen of de diensten inderdaad gebruikt wordt voor de opgegeven reden. Indien er bijvoorbeeld indicaties zijn dat de cliënt betrokken is bij witwassen of terrorismefinanciering of indien er een risico voor betrokkenheid bij witwassen of terrorismefinanciering is, voert de instelling alsnog het volledige cliëntenonderzoek uit.

Ook beoordeelt de instelling of een rekening wel voor eigen gebruik wordt aangehouden en gebruikt. Bijvoorbeeld, kredietinstellingen houden soms een rekening op eigen naam aan bij een andere instelling maar de gelden op die rekening zijn van een (groep van) cliënt(en) van de kredietinstelling en de transacties vinden voor rekening en risico van die cliënt(en) plaats. In dit soort gevallen overweegt de instelling of nog wel aan het doel van artikel 6 WWFT (vereenvoudigd cliëntenonderzoek vanwege een laag risico) wordt voldaan of dat de instelling toch niet conform artikel 3 WWFT dient te handelen met betrekking tot de cliënt(en) voor wiens rekening en risico wordt gehandeld of dat de relatie met de andere bank als hoger risico (conform artikel 8 WWFT) moet worden behandeld.

Het vereenvoudigd cliëntenonderzoek is toegestaan voor bepaalde cliënten die gevestigd zijn in een EU-lidstaat of voor bepaalde cliënten die zijn gevestigd in niet EU-lidstaten zoals die zijn aangewezen in artikel 3 van de Uitvoeringsregeling WWFT. Artikel 6 WWFT stelt echter artikel 8, lid 1 WWFT niet buiten werking. Dit brengt met zich mee dat indien er feiten en omstandigheden zijn die leiden tot een verhoogd risico op witwassen of terrorismefinanciering, de instelling verscherpt cliëntenonderzoek uitvoert ongeacht waar de cliënt gevestigd is. De toelichting bij de Uitvoeringsregeling WWFT zegt hier nog over dat het een instelling vrij staat om - op grond van een eigen risico-inschatting - geen vereenvoudigd cliëntenonderzoek toe te passen ten aanzien van een instelling gevestigd in een van de equivalente staten.

²² De verplichting voor trustkantoren om de herkomst van vermogen na te gaan en vast te leggen, is opgenomen in artikel 10 Wtt juncto artikel 13 Rib.

Met betrekking tot de derdengeldenrekeningen die beroepsbeoefenaren bij krediet- en financiële instellingen aanhouden, hoeft de krediet- of financiële instelling niet een cliëntenonderzoek te doen naar de cliënt van de beroepsbeoefenaar. De krediet- of financiële instelling heeft al het cliëntenonderzoek van de beroepsbeoefenaar, zijnde de rekeninghouder, gedaan, en omdat deze beroepsbeoefenaren ook onder de WWFT vallen, dienen deze op hun beurt te voldoen aan de verplichtingen van artikel 3 WWFT met betrekking tot het cliëntenonderzoek van hun cliënt. Het is derhalve niet nodig voor de krediet- of financiële instelling een cliëntenonderzoek te doen naar 'de cliënt van de cliënt' bij beroepsbeoefenaren.

Pensioenfondsen en schadeverzekeraars vallen niet onder de WWFT als instelling. Instellingen die een dergelijke instelling als cliënt hebben, kunnen niet van het vereenvoudigd cliëntenonderzoek van artikel 6, lid 1, onderdeel a of b WWFT gebruik maken. Echter, in die gevallen dat een dergelijke instelling beursgenoteerd is (artikelen 6, lid 1, onderdelen c en d WWFT) kan wel worden volstaan met een vereenvoudigd onderzoek.

Instellingen kunnen echter op grond van artikel 3, lid 4 WWFT bij dit soort – onder toezicht staande instellingen – wel het cliëntenonderzoek afstemmen op de risicogevoeligheid voor witwassen en terrorismefinanciering, en doorgaans zal er hier sprake zijn van een lager risico. Overigens, op grond van artikel 7, lid 1 onderdeel b WWFT kunnen instellingen die pensioenproducten aan hun cliënten verkopen wel gebruik maken van het vereenvoudigd cliëntenonderzoek tenzij er een vermoeden van witwassen of terrorismefinanciering is.

In aanvulling op de producten genoemd in artikel 7, lid 1 WWFT wordt in artikel 3 van het Uitvoeringsbesluit WWFT verwezen naar producten die voldoen aan alle voorwaarden genoemd in artikel 3, lid 3 van Richtlijn nr. 2006/70/EG. Deze voorwaarden zijn zeer technisch en gedetailleerd. Het gaat daarom te ver om een uitputtende lijst van soorten producten te geven. Instellingen beoordelen dit van geval tot geval. Wel kan worden gesteld dat het vanzelfsprekend gaat om producten die een laag witwasrisico opleveren, zoals de voorbeelden die in overweging 9 van die richtlijn genoemd worden, namelijk producten waarbij de voordelen niet ten behoeve van derden en alleen op lange termijn kunnen worden gerealiseerd, zoals bij bepaalde beleggingsverzekeringen of spaarproducten, of wanneer met het financiële product materiële activa worden gefinancierd in de vorm van een leaseovereenkomst waarbij de juridische en economische eigendom van het onderliggende actief bij de leaseonderneming blijft, of in de vorm van een consumentenkrediet van lage waarde, mits de transacties over een bankrekening worden verricht en onder een passende drempel blijven.

4.6 Hoogrisico situaties

In bepaalde gevallen, waar er een hoger risico is op witwassen of financieren van terrorisme, neemt de instelling aanvullende maatregelen. Deze maatregelen verschillen per risico. Bij de acceptatie van cliënten die een product met een verhoogd risicoprofiel afnemen, bijvoorbeeld producten of combinaties daarvan die afwijken van standaardproducten, kan niet worden volstaan met alleen standaardprocedures waarbij bijvoorbeeld gecontroleerd wordt of de cliënt of andere betrokkenen voorkomen op de sanctielijsten, of men kredietwaardig is (BKR), of identiteitsdocumenten echt zijn (VIS) en of de cliënt voorkomt in interne of externe waarschuwingssystemen van instellingen. Bij cliënt-product combinaties met een hoger risicoprofiel accepteert de instelling niet voetschoots de door de cliënt zelf verstrekte informatie, maar controleert zij deze, waar mogelijk, met gebruikmaking van onafhankelijke en betrouwbare bronnen en toetst deze in ieder geval op geloofwaardigheid.

Artikel 8, leden 2, 3 en 4 WWFT schrijven voor in welke situaties een instelling in ieder geval verscherpt cliëntenonderzoek dient uit te voeren. Dit moet, kort gezegd, in de volgende situaties: de cliënt is niet fysiek aanwezig, de cliënt is een PEP, of er is sprake van een correspondentbankrelatie. De wet geeft in die gevallen aan welke activiteiten een instelling kan (artikel 8, lid 2) dan wel moet (artikel 8, leden 3 en 4) ondernemen om het hogere risico te mitigeren.

Daarnaast volgt uit artikel 8, lid 1 WWFT dat een instelling ook verscherpt cliëntenonderzoek dient toe te passen indien feiten en omstandigheden duiden op een hoger risico op witwassen of

terrorismedinanciering. De aanvullende maatregelen die de instelling treft zijn afhankelijk van risicobeoordeling van de instelling ten aanzien van de betreffende cliënt, transactie of product. Ten aanzien van deze laatste categorie is in het bijzonder te wijzen op de FATF typologie rapporten (http://www.fatf-gafi.org/findDocument/0,3770,en_32250379_32237202_1_43383847_1_1_1,00.html) en de casusbeschrijvingen van de Egmont Group (<http://www.egmontgroup.org/library/cases>).

4.7 Niet fysiek aanwezig zijn van de cliënt

Een hoger risico betreft die gevallen waar de cliënt niet fysiek aanwezig is voor de identificatie en verificatie van de identiteit. Artikel 8, lid 2 WWFT somt een aantal mogelijkheden op om het hogere risico te compenseren in het geval dat een cliënt niet fysiek aanwezig is en de instelling niet aan de hand van de in artikel 4 van de Uitvoeringsregeling WWFT genoemde identiteitsdocumenten de identiteit van cliënt kan verifiëren.

Een instelling kan ook andere maatregelen treffen zolang het hogere risico van de niet-fysieke aanwezigheid van de cliënt maar gemitigeerd wordt. De instelling kan hiertoe aanvullende documenten, gegevens of informatie opvragen. Het gaat om aanvullende documentatie, dus bijvoorbeeld in aanvulling op een kopie van het identiteitsbewijs, of een combinatie van verschillende documenten. Gedacht kan worden aan bankafschriften, gas- en elektriciteitsrekeningen, salarisstroken, en/of arbeidsovereenkomsten zolang deze maar van onafhankelijke, derde instanties komen (vergelijk artikel 4, lid 3 van de Uitvoeringsregeling WWFT).

De instelling zal de overgelegde documenten beoordelen op echtheid. Instellingen zouden bijvoorbeeld de cliënt kunnen vragen kopieën van de documenten te laten certificeren, of de instelling kan bij bepaalde documenten vragen de originelen op te sturen (en deze natuurlijk nadien weer te retourneren).

De 'naam-nummer controle' zoals beschreven in artikel 8, lid 2, onderdeel c WWFT is een veel gebruikte methode om de identiteit te verifiëren. Omdat echter op grond van artikel 4, lid 4 WWFT de identiteit van de klant moet worden geverifieerd voordat de zakelijke relatie wordt aangegaan, zorgt de instelling er voor dat de eerste betaling voorafgaat aan of samenvalt met het begin van de zakelijke relatie en de professionele diensten die de cliënt afneemt. De cliënt zou wel alvast bedragen kunnen storten op de (spaar)rekening, maar de instelling houdt de rekening geblokkeerd en staat niet toe dat de cliënt het geld opneemt of overboekt voordat de gehele verificatie is afgerond. Instellingen kunnen er ook voor kiezen om ten behoeve van de naam-nummer controle een automatische incasso te doen van een klein bedrag.

Bij 'en/of rekeningen' wordt veelal bij een overboeking niet de tweede naam op de rekening doorgegeven. In die gevallen kan een (uitdraai of kopie van een) bankafschrift of een kopie van de bankpas worden opgevraagd om de volledige tenaamstelling te controleren. Bij deze vorm van identificatie is het van belang dat er voldoende zekerheid bestaat dat de cliënt zich elders heeft geïdentificeerd en dat hij dus op die manier via een papieren spoor achterhaald kan worden.

4.8 PEP's

Instellingen treffen verscherpte cliëntenonderzoekmaatregelen bij transacties of zakelijke relaties met politiek prominente personen (Politically Exposed Persons, PEP's) die in een andere (lid)staat wonen. Onder PEP's worden personen verstaan, die een prominente publieke functie bekleden of hebben bekleed en de directe familieleden of naaste geassocieerden van deze personen. De WWFT verwijst in de definitie van dit begrip naar artikel 2 van de Uitvoeringsrichtlijn nr. 2006/70/EG, waar het begrip 'politiek prominente persoon' uitgewerkt wordt. Een persoon blijft een PEP tot een jaar na het feitelijk verliezen van zijn prominente functie, positie of hoedanigheid waardoor hij of zij als PEP werd beschouwd.

De Uitvoeringsrichtlijn²³ overweegt dat publieke functies die op lager dan nationaal niveau worden uitgeoefend gewoonlijk niet als prominent behoeven te worden aangemerkt. Wanneer de politieke invloed ervan echter vergelijkbaar is met die van soortgelijke posities op nationaal niveau, overwegen instellingen naar gelang de risicogevoeligheid, of de personen die deze publieke functies uitoefenen, als PEP moeten worden aangemerkt.

Zakelijke relaties met PEP's vereisen aanvullende maatregelen omdat deze een grotere kans op reputatieschade en andere risico's met zich meebrengen voor instellingen. Daarnaast vergt dienstverlening aan PEP's bijzondere aandacht in het kader van het internationale beleid inzake de bestrijding van corruptie. Volgens overweging 25 van Richtlijn 2005/60/EG kunnen zakelijke relaties met PEP's en dan vooral degenen die afkomstig zijn uit landen waar corruptie veelvuldig voorkomt vooral een groot reputatierisico en/of juridisch risico met zich brengen voor de financiële sector. Gedacht kan worden aan passieve omkoping (het ontvangen van steekpenningen) of de verduistering van overheidsmiddelen. Een instelling neemt dus risicobeheersende procedures en maatregelen om PEP's te kunnen herkennen, de herkomst van het vermogen vast te stellen en doorlopend toezicht te houden op de zakelijke relatie.

De Memorie van Toelichting bij de WWFT geeft met betrekking tot PEP's al veel informatie over hoe instellingen vorm kunnen geven aan de eis van de WWFT om over risicogebaseerde procedures te beschikken teneinde uit te maken of een cliënt een PEP is. Opgemerkt kan worden dat op grond van de Nederlandse wetgeving instellingen alleen hoeven te kijken naar PEP's die niet in Nederland wonen. Instellingen die dus alleen maar of hoofdzakelijk met in Nederland wonende personen zakelijke relaties aangaan, kunnen eenvoudige procedures inrichten voor die enkele gevallen dat een cliënt in het buitenland woont of naar het buitenland verhuist. Om uit te maken of een bepaalde cliënt een PEP is, kan een instelling openbare bronnen raadplegen (zoals het internet) of informatie inwinnen bij een eigen filiaal in het land waar de betreffende cliënt woonachtig is. Voor de grotere instellingen met een aanzienlijk internationaal cliëntenbestand kan het efficiënt zijn om gebruik te maken van lijsten die door erkende commerciële organisaties worden aangeboden.

Die instellingen die PEP's in hun cliëntenbestand hebben, kunnen hun interne procedures om doorlopend controle uit te oefenen op deze zakelijke relatie eveneens risicogebaseerd inrichten. Zo zullen de ouders van een directielid van een buitenlandse centrale bank die in Nederland een eenvoudige betaalrekening aanhouden minder risicogevoelig zijn, dan de echtgenote van een staatshoofd van een land met een verhoogd risico op corruptie die een private banking rekening opent en daar grote contante bedragen op stort. Bij PEP's accepteert de instelling niet voetstoots de door de cliënt zelf verstrekte informatie, maar controleert zij deze waar mogelijk door onderzoek en toetst deze in ieder geval op geloofwaardigheid. In dat kader kan het van pas komen om te weten wat het corruptieniveau is in het land waar de persoon vandaan komt. Hiertoe kan de Corruption Perception Index van Transparency International worden gebruikt.

Daarnaast volgt uit artikel 8, lid 1 WWFT dat een instelling ook verscherpt cliëntenonderzoek dient toe te passen indien feiten en omstandigheden duiden op een hoger risico op witwassen of terrorismefinanciering. De aanvullende maatregelen die getroffen worden zijn afhankelijk van risicobeoordeling van de instelling ten aanzien van de betreffende cliënt, transactie of product. Derhalve zal een instelling, wanneer bekend is dat een cliënt een PEP is die in Nederland woonachtig is, ook een risicobeoordeling maken in welke mate voor deze cliënt aanvullende maatregelen noodzakelijk kunnen zijn.

De beslissing tot het aangaan van een zakelijke relatie met een PEP of het verrichten van een transactie voor een PEP wordt genomen of goedgekeurd door personen die daartoe door de instelling zijn gemachtigd. Dit geldt ook om een relatie te continueren met een cliënt die PEP wordt. De toestemming wordt verleend door de hogere bedrijfsleiding (senior management).

²³ Overweging 3 van Richtlijn 2006/70/EG van de Commissie van 1 augustus 2006 tot vaststelling van uitvoeringsmaatregelen van Richtlijn 2005/60/EG van het Europees Parlement en de Raad wat betreft de definitie van politiek prominente personen en wat betreft de technische criteria voor vereenvoudigde klantenonderzoekprocedures en voor vrijstellingen op grond van occasionele of zeer beperkte financiële activiteiten.

In de volgende documenten zijn in internationaal verband normen geformuleerd die als leidraad kunnen dienen bij het opstellen van beleid hieromtrent:

- Wolfsberg Frequently Asked Questions on Politically Exposed Persons (mei 2008) - <http://www.wolfsberg-principles.com/pdf/PEP-FAQ-052008.pdf>
- Transparency International: <http://www.transparency.org>

4.9 Correspondentbankrelaties

Bij het aangaan van correspondentbankrelaties betracht de instelling zorgvuldigheid. In artikel 8, lid 3 WWFT wordt van banken gevraagd dat zij zich een goed beeld vormen van instellingen uit staten die geen EU-lidstaat zijn en waar correspondentbankrelaties mee aangegaan worden. Bij correspondentbankrelaties treedt een bank feitelijk op als agent voor een andere bank door het verzorgen van betalingen of het verrichten van andere diensten voor een cliënt van deze correspondentbank. Om te voorkomen dat een bank het gevaar loopt misbruikt te worden voor het witwassen van gelden of financieren van terrorisme via dergelijke transacties, is het van belang dat zij de volgende bepalingen in acht neemt:

- Er wordt voldoende informatie verzameld over de betrokken bank om een volledig beeld te krijgen van de aard van haar bedrijfsactiviteiten.
- Op basis van openbaar beschikbare informatie wordt de reputatie van de bank en de kwaliteit van het toezicht dat op de bank wordt uitgeoefend beoordeeld.
- De procedures en maatregelen ter voorkoming van witwassen en financieren van terrorisme van de betrokken bank worden beoordeeld.
- De beslissing tot het al dan niet aangaan van een nieuwe correspondentbankrelatie wordt genomen of goedgekeurd door personen die daartoe door de bank gemachtigd zijn. Zoals in overweging 26 van Richtlijn 2005/60/EG is gesteld, gaat het hier om de hogere bedrijfsleiding (senior management). Dit impliceert niet de raad van bestuur, maar het eerste hiërarchische niveau boven dat van de persoon die de toestemming vraagt (met als uitgangspunt dat het om de hogere bedrijfsleiding gaat).
- De verantwoordelijkheden van beide banken worden schriftelijk vastgelegd.
- Met betrekking tot de cliënten die rechtsreeks toegang hebben tot transitrekeningen heeft de betrokken bank de cliënt geïdentificeerd en zijn identiteit geverifieerd en houdt doorlopend toezicht op de cliënten die rechtsreeks toegang hebben tot transitrekeningen. De betrokken bank is in staat om op verzoek de relevante cliëntgegevens te verstrekken aan de kredietinstelling.

Op grond van de wet moet een instelling verscherpt cliëntenonderzoek uitvoeren indien een correspondentbankrelatie wordt aangegaan met een bank die is gevestigd buiten de EU. Indien een correspondentbank in een EU-lidstaat is gevestigd, betekent dat echter niet dat er nooit verscherpt cliëntenonderzoek uit wordt gevoerd bij het aangaan van de correspondentbankrelatie. Indien er feiten en omstandigheden zijn die in het concrete geval kunnen duiden op een hoger risico op witwassen of terrorismefinanciering of bijvoorbeeld op grond van de interne risicoclassificatie van de instelling van landen en jurisdicties, zal de instelling aanvullende maatregelen kunnen treffen om dit hogere risico te mitigeren.

Alertheid is met name geboden op mogelijk gebruik van een correspondentrekening door (niet-geïdentificeerde) derden (transitrekening of payable-through-account). De reden waarom aan deze categorie verhoogde aandacht geschonken dient te worden, ligt in het feit dat het hier in feite gaat om dienstverlening op afstand. Immers, meestal heeft de correspondentbank zelf geen relatie met de bij de transactie betrokken partijen en heeft zodoende minder of zelfs geen mogelijkheid om de herkomst van de geldstromen te doorgronden. De Memorie van Toelichting bij de WWFT geeft geen verdere toelichting op de definitie van transitrekening zoals gegeven in artikel 1, lid 1, onderdeel h WWFT, noch wat instellingen in het geval van correspondentenrelaties met een transitrekening moeten doen. De FATF definieert een payable-through-account als een correspondentenrekening waar derden direct toegang tot hebben om transacties uit te voeren. Artikel 8, lid 3, onderdeel e WWFT doelt op de situatie dat een bank in Nederland die een correspondentbankrelatie heeft met een buitenlandse bank (in een staat die geen EU-lidstaat is) er voor dient te zorgen dat, indien die buitenlandse bank zijn cliënten direct toegang geeft tot de rekening die wordt aangehouden bij de bank in Nederland, de buitenlandse bank vergelijkbare CDD heeft uitgevoerd op die cliënten en relevante informatie daarover kan verstrekken aan de bank in Nederland.

In het volgende document is in internationaal verband normen geformuleerd die als leidraad kunnen dienen bij het opstellen van beleid hieromtrent:

- Wolfsberg AML Principles for Correspondent Banking - <http://www.wolfsberg-principles.com/corresp-banking.html>

Ten aanzien van openbare bronnen is naast het gebruik van het internet op de volgende in internationale context geaccepteerde documenten te wijzen:

- De Wolfsberg Group heeft een internationale database voor financiële ondernemingen opgezet, the Bankers Almanac Due Diligence Module. Bij aanmelding dienen de instellingen allerlei informatie aan te leveren die nuttig is in het kader van het uitvoeren van due diligence zoals ingevulde, uitvoerige, questionnaire, een overzicht van maatregelen die de instelling treft om witwassen en terrorismefinanciering tegen te gaan, een overzicht van de eigendomsstructuur, etc.
- De evaluatierapporten van internationale organisaties zoals de FATF, IMF en Wereld Bank. Hieruit volgt uiteraard niet direct in hoeverre een bepaalde instelling voldoet aan de internationale standaarden, maar de instelling kan op basis hiervan wel om bepaalde informatie aan de instelling vragen, met name ten aanzien van het toezicht dat wordt uitgeoefend.

4.10 Uitbesteding

Een instelling kan op grond van artikel 10 WWFT het cliëntenonderzoek laten verrichten door een derde. Een instelling kan cliëntenonderzoek uitbesteden waar het gaat om het identificeren van de cliënt en de UBO, het verifiëren van de identiteit van de cliënt en de UBO, alsmede het vaststellen van het doel en de beoogde aard van de zakelijke relatie.

Het monitoren van de zakelijke relatie kan echter alleen door de instelling zelf worden uitgevoerd²⁴. Voor instellingen die onder de Wft vallen en waarbij de derde partij behoort tot dezelfde groep, kan deze voortdurende controle wel door deze partij binnen de groep worden uitgevoerd²⁵.

De uiteindelijke verantwoordelijkheid voor het nakomen van cliëntenonderzoekvereisten blijft berusten bij de instelling die het onderzoek heeft uitbesteed. Waar er uitbesteed wordt, is het dus zaak om een risico-overweging zichtbaar te maken die mede ziet op de deskundigheid en de praktische aanpak van de derde partij inzake compliance met de WWFT.

Indien de uitbesteding een structureel karakter heeft wordt er een schriftelijke overeenkomst vastgesteld. In deze overeenkomst kunnen de volgende zaken geregeld worden:

- de informatie-uitwisseling tussen de instelling en de derde;
- de mogelijkheid voor de instelling om te allen tijde aanwijzingen te geven aan de derde met betrekking tot de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt;
- de verplichting door de derde om de instelling in staat te stellen blijvend te voldoen aan het bij of krachtens WWFT bepaalde; en
- het onmiddellijk beschikbaar stellen door de derde van de noodzakelijke CDD informatie en het op verzoek direct beschikbaar stellen van (kopieën van) relevante CDD documenten.

Bij uitbesteding is het van belang dat de uitbestedende instelling niet alleen vastlegt dat de derde aan de wettelijke vereisten zal voldoen, maar dat de instelling dit ook periodiek vaststelt.

4.11 Introduceren van cliënten door derden

Een instelling mag de identificatie- en verificatiegegevens overnemen van een andere instelling indien deze gegevens zijn verkregen door een:

²⁴ Artikel 3, lid 2, onderdeel d WWFT wordt namelijk niet genoemd in artikel 10.

²⁵ Op grond van artikel 32 van het Bpr zijn de regels met betrekking tot uitbesteding niet van toepassing op partijen die bij een groep horen.

- advocaat, (kandidaat)notaris, registeraccountant, accountant-administratieconsulent of belastingadviseur binnen de EU;
- een Nederlands trustkantoor; of
- een gereguleerde financiële instelling (uitgezonderd een betaaldienstagent of betaalinstelling die geldtransfers uitvoeren). Het ligt daarbij wel in de rede dat het een financiële instelling betreft die gevestigd is in een land met vergelijkbare wetgeving als de WWFT en waarbij adequaat toezicht wordt uitgeoefend op de naleving hiervan.

Een instelling mag vertrouwen op deze gegevens aangezien deze aangewezen personen en instellingen zelf instellingen in de zin van de WWFT zijn.

De gegevens dienen echter wel aan de instelling ter beschikking te worden gesteld indien deze daarom vraagt in verband met de controle en vastlegging. Het is belangrijk dat de instelling zich ervan vergewist dat de betreffende elementen van het cliëntenonderzoek hebben plaatsgevonden conform de WWFT (of vergelijkbare wetgeving in internationale situaties). De instelling blijft uiteindelijk zelf verantwoordelijk voor de juiste identificatie en verificatie van de cliënt ook al is dit uitgevoerd door een andere instelling. Een instelling kan zelf de manier bepalen hoe zij zich ervan vergewist dat de eerdere identificatie overeenkomstig de WWFT heeft plaatsgevonden.

De instelling ontvangt bij de eerste introductie alle nodige CDD informatie. Daarnaast is de instelling er zeker van dat zij, op eerste verzoek, alle benodigde documenten krijgt van de introducerende instelling. Voorzover deze documenten al niet direct bij de eerste introductie aangeleverd worden, zou ook hier de instelling steekproefsgewijs kunnen controleren of de gevraagde documenten inderdaad op eerste verzoek verstrekt worden.

Indien de introducerende instelling de gegevens niet kan verstrekken, verricht de andere instelling alsnog het cliëntenonderzoek indien dat op grond van de WWFT of de interne regels noodzakelijk is. Temeer ook omdat de uiteindelijke verantwoordelijkheid voor het cliëntenonderzoek ligt bij de instelling waar de cliënt geïntroduceerd wordt²⁶.

Ook al is door de introducerende instelling op een cliënt het vereenvoudigde cliëntenonderzoek toegepast omdat deze cliënt een laagrisico product afnam, de instelling waar de cliënt wordt geïntroduceerd kan op grond van artikel 9, lid 2 WWFT de introducerende instelling wel vragen om de identificatie- en verificatiegegevens. Het doel van artikel 9 is weliswaar te voorkomen dat het cliëntenonderzoek nodeloos twee maal wordt gedaan, een instelling mag op grond van de interne procedures altijd meer doen dan de WWFT vereist en kan dus ook besluiten zelf alsnog een cliëntenonderzoek te verrichten. Overigens, artikelen 6, lid 1 en 7, lid WWFT (vereenvoudigd cliëntenonderzoek) maken geen uitzondering voor artikel 3, lid 3, onderdelen c en e WWFT: cliëntenonderzoek in geval van vermoeden van witwassen en terrorismefinanciering. Als de instelling waar een cliënt geïntroduceerd wordt een dergelijk vermoeden heeft, dan heeft de instelling een extra reden de gegevens op te vragen.

Een instelling die vertrouwt op de identificatie en verificatie van de identiteit door een andere instelling die onder de WWFT valt, zal hier zorgvuldig mee om gaan. Aangezien de verantwoordelijkheid voor een correct cliëntendossier bij de instelling ligt waar een cliënt wordt geïntroduceerd, is het belangrijk dat deze instelling zich er van vergewist dat de introducerende instelling adequate procedures en maatregelen met betrekking tot de WWFT heeft. Dat houdt in dat de procedures van de introducerende partij in opzet en werking adequaat zijn. Zo kan een instelling die veelvuldig cliënten accepteert die worden geïntroduceerd door andere instellingen, van deze andere instellingen, op risicogebaseerde wijze, de WWFT procedures opvragen en beoordelen. Bij nieuwe samenwerkingsverbanden worden altijd de WWFT procedures opgevraagd ter beoordeling.

Dit is met name voor levensverzekeraars relevant die vertrouwen op het cliëntenonderzoek door financiële dienstverleners die bemiddelen in levensverzekeringen. De verzekeraar is

²⁶ Zie ook overweging 27 bij Richtlijn 2005/60/EG.

verantwoordelijk voor een adequate uitvoering van het CDD beleid. Concreet betekent dit dat een verzekeraar ten aanzien van identificatie en verificatie van cliënten, beleid formuleert over de manier waarop wordt omgegaan met het vertrouwen op de door de relevante financiële dienstverleners uitgevoerde identificatie en verificatie van de identiteit van de cliënt. Daarnaast wordt beleid geformuleerd op grond waarvan de betreffende financiële dienstverleners de gegevens omtrent de identificatie van cliënten desgevraagd onmiddellijk beschikbaar stelt. Financiële dienstverleners die bemiddelen in levensverzekeringen hebben een zelfstandige verplichting met betrekking tot de WWFT. In het geval waarin deze financiële dienstverlener de identiteit van de cliënt heeft vastgesteld en geverifieerd, behoudt de verzekeraar ter zake zijn eigen verantwoordelijkheid. Deze mag de verzekeringsovereenkomst bijvoorbeeld pas sluiten nadat hij zich ervan heeft vergewist dat de tussenpersoon de identiteit van de cliënt heeft vastgesteld en deze identiteit heeft geverifieerd. Verzekeraars zullen periodiek, op risicogebaseerde wijze, nagaan of de betreffende financiële dienstverleners maatregelen hebben om op een adequate uitvoering te geven aan het cliëntenonderzoek. Hier kan op verschillende manieren uitvoering aan gegeven worden. Zo kan bijvoorbeeld de instelling jaarlijks van een aantal financiële dienstverleners die bemiddelen in levensverzekeringen de WWFT procedures opvragen ter beoordeling. Andere mogelijkheden zijn het opvragen van een accountantverklaring (voor met name grote financiële dienstverleners) of het steekproefsgewijs opvragen van een aantal cliëntendossiers.

5. Monitoren

5.1 Algemeen

Tijdens het cliëntacceptatieproces stelt een instelling een risicoprofiel en verwacht transactiepatroon op van de cliënt. Gedurende de duur van de relatie is het van belang dat de instelling periodiek toetst of de cliënt nog steeds aan het risicoprofiel voldoet en het transactiepatroon overeenkomstig de verwachtingen is. De instelling kan de frequentie en intensiteit van reviews afstemmen op de risicoclassificatie van de cliënt. Dit is beschreven in hoofdstuk 3.6.

Naast de periodieke actualisatie van de cliëntgegevens, monitort de instelling ook de rekening en de transacties van cliënten. Met deze monitoring wordt inzicht verkregen en gehouden in de aard en achtergrond van de cliënten en hun financieel gedrag. De controle heeft onder andere tot doel te detecteren of er een afwijkend transactiepatroon plaatsvindt en of zich mogelijk situaties voordoen die een verhoogd risico met zich meebrengen. De instelling controleert systematisch of sprake is van ongebruikelijke of verdachte patronen of activiteiten. Zo zal van transacties worden beoordeeld of deze voor de cliënt gebruikelijk zijn. Voorbeelden van aandachtspunten zijn: dienen de transacties een economisch of commercieel doel, gaat het om uitzonderlijk grote bedragen, betreft het stortingen of opnames die niet in verhouding zijn tot de normale/verwachte business van de cliënt, is het rekening- en transactieverloop in verhouding met de activiteiten van de cliënt, zijn er transacties van en naar landen met een verhoogd risico.

Het monitoren van de relatie met de cliënt en de transacties van de cliënt kan worden afgestemd op het soort relatie. Per sector en per product kan dit verschillend zijn. Zo kan bijvoorbeeld voor levensverzekeringsproducten gedacht worden aan één controlemoment per jaar, bijvoorbeeld bij de betaling van (jaarlijkse) premies, en controlemomenten bij wijzigingen in het contract of de begunstiging. Bij eenvoudige betaalrekeningen zal de intensiteit van monitoring lager kunnen zijn dan bij (gerelateerde) rekeningen van grote, internationaal opererende ondernemingen.

Instellingen bieden steeds minder kasfuncties en zoeken naar alternatieven voor kasstortingen. Daar waar er geen direct contact is met de cliënt, kunnen dit soort contante stortingen een hoger risico opleveren. Deze instellingen voorzien in extra waarborgen om er voor te zorgen dat van degenen die van dergelijke alternatieven gebruik maken op adequate wijze de identiteit is vastgesteld en geverifieerd. Tevens besteden instellingen extra aandacht aan dit soort transacties om te beoordelen of zij binnen het risicoprofiel van de cliënt vallen.

5.2 Monitoring bij money transfers: transactieanalyses

De instelling monitort, zoals gezegd, ook de transacties van cliënten. Voor money transfers geldt dat met name de samenhang tussen bepaalde transacties onderzocht wordt om ongebruikelijke

transacties (met een georganiseerd karakter) te kunnen signaleren. Instellingen die money transfers verrichten, analyseren transacties minimaal volgens de hieronder omschreven methode om effectief ongebruikelijke transacties te signaleren.

Instellingen die money transfers verrichten maken in de praktijk periodiek selecties van de grootste Nederlandse en buitenlandse zenders en ontvangers ten behoeve van hun onderzoek naar vermeend misbruik van money transfers. Bij kleine instellingen zal wellicht een top 10 per categorie volstaan, terwijl bij grote kantoren een top 50 relevanter is. Het is aan de instelling om daar zelf specifieke invulling aan te geven. Analyses worden, voor het beste resultaat, op maand-, kwartaal- en jaarbasis uitgevoerd.

De instelling zal afhankelijk van de resultaten van de analyses nader cliëntenonderzoek uitvoeren, zoals onderzoek naar de herkomst en bestemming van gelden.

Afhankelijk van het aantal transacties en de gesignaleerde risico's, doen instellingen die money transfers verrichten, aanvullend onderzoek. Hierbij kan onder meer gedacht worden aan:

- analyses op specifieke gebieden en/of landen (corridoronderzoeken);
- transacties op adressen van Nederlandse klanten (op bestaan controleren en meervoudig gebruik);
- transacties juist onder de objectieve meldgrens (het zogenaamde 'smurfen');
- analyses per locatie (afzetpunt).

5.3 Methoden van monitoring

Monitoring kan op verschillende niveaus plaatsvinden, afhankelijk van het risico en de omvang van de werkzaamheden. Hoe hoger het risico hoe intensiever (qua frequentie en diepgang) de monitoring is. Voorbeelden van methoden van monitoring zijn de volgende:

- Spot-checks: gerichte controles op rekeningen en transacties van bijvoorbeeld bepaalde cliëntengroepen, dan wel rekeningen en transacties die eerder op basis van meldingen aan FIU-NL of anderszins als verhoogd risico zijn aangemerkt.
- Handmatige monitoring: de accountmanager kent zijn cliënten en hun financieel gedrag. Afwijkingen van het gedrag van de cliënt zullen onmiddellijk bekend worden bij de accountmanager. Een effectieve en realistische 'span of control' alsmede deskundigheid en vaardigheid van de personen die de controle uitvoeren, is bij deze vorm van monitoring essentieel.
- Periodieke managementoverzichten/rapportages: van deze manier van monitoring wordt gebruik gemaakt in geval van redelijk overzichtelijke en beheersbare aantallen cliënten en transacties. Een dagelijkse, wekelijkse of maandelijkse uitdraai van omzet, saldo, overschrijdingen grensbedragen, in rekening gebrachte provisies en dergelijke, kunnen een indicatie geven van welke rekeningen nader onderzoek vereisen.
- Monitoring aan de hand van harde indicatoren: van deze methode wordt gebruik gemaakt bij het doen van een eerste filtering op basis van omzet, maximumsaldo, transactiebedragen, landen van bestemming of herkomst, risicobranche en dergelijke.
- Intelligente transactiemonitoring: bij intelligente transactiemonitoring wordt vaak gebruik gemaakt van profilering van elke rekening of cliënt. Het profiel kan bestaan uit de omzet, de hoogte van transactiebedragen, tegenrekeningen, de frequentie waarmee transacties plaatsvinden, omschrijving en dergelijke. Elke profielbouwsteen kan een eigen gewicht worden gegeven. Elke nieuwe transactie wordt getoetst tegen het profiel, waarbij de transactie die het meest afwijkt van het profiel het hoogste risicogetal krijgt. In alle gevallen van transacties die boven een gekozen risicogetal uitkomen, wordt nader onderzoek ingesteld. Pas dan kan worden vastgesteld of een transactie als verdacht of ongebruikelijk dient te worden aangemerkt.

Verschiede manieren van monitoring kunnen worden gecombineerd. Zo zal monitoring met profilering van betaal- en spaarrekeningen met een relatief lage omzet en saldo wat betreft kosten versus risico weinig interessant zijn. Door middel van harde indicatoren (omzet, maximumsaldo, transacties van en naar bepaalde landen en dergelijke) kan echter wel worden vastgesteld of een dergelijke rekening dient te worden overgeheveld van risicoclassificatie laag naar normaal of verhoogd, waarna zou kunnen worden overgestapt op intelligente monitoring. Bij monitoring zal

een instelling een afweging maken tussen kosten, risico en in te zetten methode. Ten aanzien van private banking activiteiten, die in de klasse hoog risico vallen, is het bijvoorbeeld mogelijk dat handmatige monitoring plaatsvindt. Een accountmanager kent diens cliënt en zal een afwijking in financiële activiteiten herkennen, zonder gebruik te hoeven maken van intelligente monitoringsystemen. Zodra het aantal cliënten per accountmanager zo groot wordt dat het ken-uw-client-principe in het geding komt zullen andere monitoringsmethoden worden ingezet teneinde toch zicht te kunnen houden op de financiële activiteiten van de cliënten.

In het volgende document is in internationaal verband normen geformuleerd die als leidraad kunnen dienen bij het opstellen van beleid hieromtrent:

- Monitoring Screening and Searching Wolfsberg Statement <http://www.wolfsberg-principles.com/monitoring.html>

5.4 Monitoring bij hoogrisico jurisdicties

De FATF wijst regelmatig op jurisdicties die tekortkomingen hebben in hun systeem ter bestrijding van witwassen en terrorismefinanciering²⁷. Het onderhouden van zakelijke relaties met ingezetene van deze jurisdicties of het uitvoeren van transacties van of naar deze jurisdicties kan een hoger risico op witwassen en terrorismefinanciering met zich meebrengen, hetgeen zou kunnen leiden tot verscherpte maatregelen. De FATF herziet de lijsten indien daar aanleiding voor is, en DNB verwijst naar deze lijsten op haar website.

Naast de waarschuwingen van de FATF en de 'mutual evaluation reports' van de FATF of een zogenoemde FATF-Style Regional Body (FSRB)²⁸ zijn er ook andere betrouwbare bronnen over de mate van implementatie van internationale standaarden op het gebied van financiële criminaliteit of terroristische activiteiten door een land of jurisdictie die voor een instelling aanleiding kunnen zijn om verhoogde aandacht te geven aan de zakelijke relaties en transacties met mensen uit die landen en jurisdicties. Van instellingen nemen in het kader van de monitoring de witwas- of terrorismefinancieringsrisico's in bepaalde landen in acht.

Aanvullende informatie is te vinden op:

- FATF: http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236992_1_1_1_1_1,00.html
- OECD: http://www.oecd.org/document/57/0,3343,en_2649_33745_30578809_1_1_1_1,00.html
- VN: <http://www.un.org/sc/committees/1267/index.shtml>

5.5 Beoordeling en vastlegging

Indien de instelling transacties aantreft die buiten het verwachte patroon vallen of die geen economisch of juridisch doel hebben, zal de instelling onderzoeken wat de achtergrond en doel van de transactie was. De bevindingen zullen in het cliëntendossier worden vastgelegd. Indien een transactie aanleiding geeft om te vermoeden dat deze verband houdt met witwassen of terrorismefinanciering zal de transactie gemeld worden aan FIU-NL. De overwegingen en besluitvorming om een transactie wel of niet te melden worden door de instelling vastgelegd.

6. Bij elektronische geldovermakingen te voegen gegevens

De FATF heeft in 2001 een aanbeveling over 'wire transfers' opgesteld (Special Recommendation VII) waarin staat dat een elektronische overboeking bepaalde gegevens van degene die de betalingsopdracht doet, moet bevatten. Deze FATF Aanbeveling is in Europa verwerkt in Verordening (EG) nr. 1781/2006 van het Europees Parlement en de Raad van 15 november 2006

²⁷ Zo geeft de FATF na elke vergadering een 'public statement' uit en een document genaamd 'improving global AML/CFT compliance: 'ongoing process' waarin wordt gewezen op jurisdicties met tekortkomingen in hun systeem ter bestrijding van witwassen en terrorismefinanciering.

²⁸ FSRB's zijn: Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Eurasian Group (EAG), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering measures and the Financing of Terrorism (MONEYVAL), Financial Action Task Force on Money Laundering in South America (GAFISUD), Inter Governmental Action Group against Money Laundering in West Africa (GIABA) and the Middle East and North Africa Financial Action Task Force (MENAFATF).

betreffende bij geldovermakingen te voegen informatie over de betaler. De verordening heeft rechtstreekse werking in Nederland. In de WWFT zijn sanctiebepalingen opgenomen inzake de niet-naleving van deze EG-Verordening en is DNB opgedragen toezicht te houden op naleving van deze verordening.

De Verordening stelt voorschriften vast voor de bij geldovermakingen te voegen informatie over de betaler om ervoor te zorgen dat de voor de bestrijding van het witwassen van geld en terrorismefinanciering verantwoordelijke autoriteiten onmiddellijk beschikken over de basisinformatie die hen kan helpen bij de uitvoering van hun taak.

De term 'cover payment' is een specifieke invulling van 'wire transfer' en wordt gebruikt in internationale betalingstransacties waarbij de opdrachtgevende bank of instelling geen rechtstreekse relatie heeft met de begunstigde bank of instelling en de transactie via (tussenliggende) correspondentbanken wordt gedaan. Een dergelijke betalingstransactie heeft twee onderdelen. Het ene deel betreft de informatie tussen de opdrachtgevende en de ontvangende cliënt en bevat de door de EG-Verordening verplicht gestelde cliëntinformatie. Het andere deel, de cover payment, betreft de informatie-uitwisseling tussen de correspondentbanken. Ook bij deze cover payment dient informatie over de opdrachtgever te worden gevoegd en de correspondentbanken zorgen ervoor dat alle ontvangen informatie over de opdrachtgever welke bij een geldovermaking is gevoegd, bij de overmaking blijft. Indien er nog gebruik wordt gemaakt van zogenaamde SWIFT MT202 berichten (waarbij de instelling als intermediaire bank optreedt) zal de instelling aan DNB aantonen dat het risico dat de bank wordt gebruikt in een transactie waarbij sprake is van twee onbekende partijen in voldoende mate wordt beheerst. Er zou hier alleen sprake mogen zijn van bank-to-bank transacties en niet van een onderliggende transactie tussen twee niet-banken.

Volledige informatie over de betaler bestaat uit zijn naam, adres en rekeningnummer. Het adres mag worden vervangen door de geboorteplaats en -datum van de betaler, zijn cliëntidentificatienummer of zijn nationaal identiteitsnummer. Bij gebreke van het rekeningnummer van de betaler vervangt de instelling van de betaler dit door een unieke identificatiecode aan de hand waarvan de transactie terug kan worden getraceerd naar de betaler.

De begunstigde instelling legt op basis van een risicobeoordeling bijzondere alertheid aan de dag wanneer informatie over de betaler ontbreekt of onvolledig is. Ingeval de vereiste informatie over de betaler onvolledig is, weigert de instelling de overmaking of verzoekt om de volledige informatie over de betaler. Wanneer een opdrachtgevende instelling regelmatig nalaat de vereiste informatie over de betaler te verstrekken, onderneemt de begunstigde instelling stappen, die aanvankelijk kunnen bestaan uit het sturen van waarschuwingen of het opleggen van uiterste termijnen, alvorens te besluiten alle toekomstige geldovermakingen van deze instelling te weigeren of te besluiten zijn zakelijke relatie met deze instelling al dan niet te beperken of te beëindigen. De begunstigde instelling meldt dit feit aan FIU-NL.

In internationaal verband is er aanvullende informatie en guidance van:

- EU: http://ec.europa.eu/internal_market/payments/transfers/index_en.htm
- 3L3 Anti-money laundering and terrorism financing group (3L3 AMLTF): <http://www.c-ebs.org/getdoc/64c0be05-9e6e-44b5-a8de-da6a2ba6813e/2008-16-10-AMLTF-Common-understanding-on-payment-f.aspx>
- BCBS/ILG Anti-money laundering and terrorism financing Expert Group (AMLEG): <http://www.bis.org/publ/bcbs154.htm>
- The Wolfsberg Group: http://www.wolfsberg-principles.com/pdf/WG-NYCH_Statement_on_Payment_Message_Standards_April-19-2007.pdf

7. Vastlegging en bewaarplicht

Uit diverse wetgeving²⁹ volgt dat instellingen gegevens omtrent de cliënten en de transacties moeten bewaren. Het betreft gegevens die zijn verkregen tijdens het CDD proces, zoals kopieën van de identiteitsdocumenten, rekeninggegevens, correspondentie, gespreksnotities over en met

²⁹ Artikel 33 WWFT, artikel 14 BPR, artikel 10 Boek 2 BW, artikel 52 AWR.

de cliënt, transacties van en andere dienstverlening aan die cliënt. Uit het dossier blijkt ook hoe het besluitvormingsproces rond de cliëntacceptatie tot stand gekomen is, bijvoorbeeld in het geval van hoogrisico cliënten.

Instellingen bewaren deze gegevens minimaal 5 jaar tot na het beëindigen van de zakelijke relatie of na de dienstverlening. In het geval van een incidentele transactie betreft de bewaartermijn minimaal 5 jaar na het uitvoeren van de transactie.

Het doel van de bewaarplicht is dat de autoriteiten inzicht kunnen krijgen in de activiteiten van een cliënt, bijvoorbeeld in het geval van een (strafrechtelijk) onderzoek. De diverse dossiers en bestanden zijn dan ook goed toegankelijk voor de toezichthouder. Hierbij maakt het niet uit of de gegevens in elektronische vorm of als fysiek document worden bewaard.

8. Melden ongebruikelijke transacties

Instellingen zijn verplicht om ongebruikelijke transacties te melden aan FIU-NL. Of een transactie ongebruikelijk is, wordt beoordeeld aan de hand van de indicatorenlijst.

8.1 Meldplicht

Ingevolge artikel 16 WWFT dient een instelling een verrichte of voorgenomen ongebruikelijke transactie te melden. De bijlage van artikel 4 van het Uitvoeringsbesluit van de WWFT bevat de lijst met indicatoren op grond waarvan gemeld moet worden. Deze lijst kan gebruikt worden ten behoeve van de beoordeling of een transactie als ongebruikelijk moet worden aangemerkt. De indicatoren zijn onderverdeeld in objectieve en subjectieve indicatoren. De objectieve indicatoren beschrijven een situatie waarin een transactie altijd moet worden gemeld.

Bij de meldplicht ligt de nadruk echter op de subjectieve indicator. De subjectieve indicator verplicht een instelling om een transactie te melden indien er aanleiding is om te veronderstellen dat de transactie verband kan houden met witwassen of financiering van terrorisme. De instelling zal zich derhalve buigen over de vraag of een bepaalde transactie wellicht melding behoeft omdat er mogelijk sprake is van witwassen of financieren van terrorisme. Daarmee wordt de verantwoordelijkheid van de instellingen voor hun meldgedrag benadrukt.

Bij indicatoren die zijn gerelateerd aan een grensbedrag beoordeelt de instelling ook of er sprake is van een verband tussen twee of meerdere transacties. Dit kan aan de hand van het soort transactie en de bedragen waar het om gaat. Indien er een verband is, zouden deze transacties onder de subjectieve indicator gemeld kunnen worden.

Voorbeelden:

Terrorismefinanciering:

In het FIU-jaaroverzicht 2009 van FIU-NL wordt als aandachtspunt met betrekking terrorismefinanciering aangegeven dat het risico bestaat dat studenten uit landen zoals Pakistan, Afghanistan en Somalië die met een studentvisum naar Nederland komen gerelateerd zijn aan terroristische groepen.

Aanvullende informatie:

- http://www.fiu-nederland.nl/nl/informatie/cat_view/19-nederlandse-informatie/7-jaaroverzichten.html

Levensverzekeraars:

Wat betreft levensverzekeraars bestaat de perceptie dat het bij levensverzekeringen vaak om standaard producten gaat met een laag risico. Deze gedachte wordt versterkt doordat verzekeraars niet met contant geld te maken hebben en geldstromen ook via banken lopen. Het ligt echter voor de hand dat banken de betalingen die gaan naar of komen van een levensverzekeraar minder diepgaand bekijken omdat het een transactie betreft met een instelling die ook onder de WWFT valt. Daarbij hebben banken geen inzicht in de onderliggende verzekeringscontracten. Voorbeelden van transacties waar een verzekeraar extra aandacht aan kan besteden, zijn:

- Koopsompolissen met een hoge waarde (bijvoorbeeld boven 100.000 euro) die vervroegd zijn afgekocht, vooral wanneer dat ongebruikelijk vroeg is of zonder economische reden.
- Direct ingaande koopsompolissen voor een hoog bedrag, bijvoorbeeld boven 100.000 euro.
- Koopsompolissen waar begunstigde of verzekeringnemer een (buitenlandse) rechtspersoon is.
- Universal life polissen met hoge eenmalige stortingen.
- Polissen waarop wijziging van begunstiging heeft plaatsgevonden en de nieuwe begunstigde een persoon is zonder duidelijke band met de verzekeringsnemer.
- Koopsompolissen of universal life polissen waar betaling plaatsvindt van rekeningnummer niet op naam gesteld van de verzekeringnemer of begunstigde, of waar betaling plaatsvindt van een buitenlands rekeningnummer.
- Polissen die gebruikt worden als zekerheidsstelling voor een verstrekte geldlening, anders dan ten behoeve van hypothecaire geldleningen.
- Polissen met zeer hoge premies of koopsommen die niet in relatie staan tot het verifieerbare legitieme inkomen.
- Polissen met verzekeringsdekkingen die niet in verhouding staan tot het economisch profiel of de behoefte van cliënt.
- Polissen die binnen de wettelijke opzegtermijn van 30 dagen opgezegd worden en waar restitutie van de reeds betaalde premie plaatsvindt op een rekeningnummer die niet op naam is gesteld van de verzekeringnemer en/of op een buitenlands rekeningnummer.

Aanvullende informatie:

- FATF typologie rapport, FATF Money Laundering and Terrorist Financing 2004-2005, <http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>

Meldprocedure

De WWFT heeft geen expliciete eis voor instellingen om processen en procedures te hebben waarmee het ongebruikelijke karakter van transacties te herkennen is. Het is echter inherent dat instellingen dergelijke procedures hebben omdat het anders niet mogelijk is om het ongebruikelijke karakter van transacties te herkennen en te melden. Daar komt bij dat de toezichthouder op grond van artikel 32 WWFT een instelling kan verplichten interne procedures en controles ter voorkoming van witwassen en terrorismefinanciering te ontwikkelen indien een instelling niet voldoet aan haar verplichting om ongebruikelijke transacties te melden. Daarnaast zijn er natuurlijk ook eisen die op grond van de andere financiële toezichtwetgeving worden gesteld aan instellingen met betrekking tot het hebben van procedures en maatregelen om integriteitrisico's te beheersen. Zoals al gezegd, in de brief van de minister van Financiën aan de Tweede Kamer van 15 oktober 2008 (Kamerstuk 31237, nr. 9) wordt vermeld dat de procedures die gelden voor de Wft en de WWFT kunnen worden geïntegreerd en kan op eenzelfde wijze invulling worden gegeven aan de vereisten van de WWFT en de Wft.

De transacties worden zo snel mogelijk, maar in ieder geval binnen het wettelijke maximum van veertien dagen nadat het ongebruikelijke karakter van de transactie is bekend geworden, gemeld. Verder ligt het in de rede, zoals ook in de indicatorenlijst (zie hoofdstuk 8.1) vermeld, dat transacties die in verband met witwassen of terrorismefinanciering aan politie of Openbaar Ministerie worden gemeld, ook aan FIU-NL worden gemeld; er is immers een vermoeden van witwassen of terrorismefinanciering.

De WWFT geeft een opsomming van de gegevens die bij een melding moeten worden verstrekt. Deze gegevens zijn voor FIU-NL van essentieel belang om een ongebruikelijke transactie te kunnen analyseren. Indien een instelling stelselmatig bepaalde gegevens niet aanlevert, kan FIU-NL deze omissie in het meldgedrag aan de toezichthouder doorgeven en zou de toezichthouder de instelling een aanwijzing kunnen geven om interne procedures en controles ter voorkoming van witwassen en terrorismefinanciering te ontwikkelen.

8.2 Vrijwaringen

De WWFT kent een strafrechtelijke vrijwaring in artikel 19 WWFT en een civielrechtelijke vrijwaring in artikel 20 WWFT. De strafrechtelijke vrijwaring ziet er op toe dat gegevens of inlichtingen die de instelling bij melding verstrekt, niet kunnen worden gebruikt ten behoeve van een

opsporingsonderzoek of strafrechtelijke vervolging van de instelling ter zake van witwassen of financieren van terrorisme. De wet breidt deze vrijwaring uit tot degene die de melding heeft gedaan. Gedacht kan worden aan een medewerker van een bank die voor de melding heeft zorg gedragen of die aan het opstellen van het meldingsbericht heeft meegewerkt. Uiteraard geldt de vrijwaring alleen, indien de melding op correcte wijze, conform de vereisten van de WWFT heeft plaatsgevonden.

De civielrechtelijke vrijwaring houdt in dat een instelling niet civielrechtelijk aansprakelijk is voor de schade die iemand anders (de cliënt of een derde) als gevolg van een melding lijdt, tenzij aannemelijk wordt gemaakt dat, gelet op de feiten en omstandigheden, in redelijkheid niet tot melding had mogen worden overgegaan. Hierbij kan gedacht worden aan eisen gesteld in een civielrechtelijke procedure op grond van wanprestatie, indien de instelling heeft besloten een transactie niet uit te voeren en deze te melden. Ook is een actie op grond van een onrechtmatige daad voorstelbaar, wegens eventuele schade die mogelijk is ontstaan ten gevolge van de melding door een instelling.

8.3 Geheimhouding

De WWFT kent een zware geheimhoudingsplicht. Instellingen zijn verplicht geheim te houden dat een melding is gedaan. Uitzonderingen hierop zijn mogelijk voorzover dat uit de wet voortvloeit. De uitzonderingen op de geheimhoudingsplicht staan het de instelling toe om informatie uit te wisselen met – kort gezegd – onderdelen van de eigen organisatie of het netwerk elders en/of andere instellingen die onder de reikwijdte van de WWFT of gelijkwaardig regelgeving vallen, in het kader van de doelstelling van deze wetgeving. Zonder deze uitzonderingen zouden bestaande waarschuwingssystemen, zoals het interbancaire waarschuwingssysteem, tussen de financiële instellingen kunnen worden belemmerd. Hoewel ingevolge artikel 28 van Richtlijn 2005/60/EG de geheimhoudingsplicht niet enkel dient te gelden ten opzichte van cliënten maar ook ten opzichte van derde personen, kan het niet de bedoeling van de richtlijn zijn om dergelijke systemen, die bijdragen aan de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of financiering van terrorisme, te belemmeren.

9. Training en opleiding

Bij de instellingen hangt de toereikende implementatie van de processen en procedures inzake de WWFT en SW voornamelijk af van de mate van ervaring en kennis van de medewerkers. Toereikende kennis en ervaring van het personeel met betrekking tot de beheersing van de risico's van witwassen en terrorismefinanciering zijn dan ook belangrijke voorwaarden voor een toereikend beheersingskader. Opleidingen en trainingen van het personeel zijn dan ook belangrijke manieren om kennis van de WWFT en de SW, de integriteitbeleidsuitgangspunten en procedures te communiceren en te borgen.

Instellingen bieden daartoe opleidingen aan die de medewerkers bekend maken met de bepalingen van de WWFT en de SW en die de medewerkers in staat stellen de CDD maatregelen uit te voeren en ongebruikelijke transacties te herkennen. Deze opleidingen behandelen witwas- en terrorismefinancieringstechnieken, methodes en trends, de internationale context en standaarden, en nieuwe ontwikkelingen op dat gebied. Om op de hoogte te blijven van de nieuwe ontwikkelingen en de bewustwording blijvend te bevorderen, is een training in de regel niet eenmalig, maar wordt deze regelmatig en ook op verschillende niveaus aangeboden.

10. Sanctieregelgeving

De Algemene leidraad van het ministerie van Financiën van februari 2011 geeft uitgebreid informatie omtrent de sanctiemaatregelen. In aanvulling daarop wordt hieronder beknopt het toezicht door DNB op de naleving van de SW en de meldprocedure beschreven.

Met betrekking tot het financieel verkeer zijn de AFM en DNB belast met het toezicht op de naleving van de SW. Daartoe hebben de beide toezichthouders gezamenlijk de Regeling Toezicht Sanctiewet 1977 vastgesteld. Deze regeling omvat onder meer een meldingsplicht voor het geval dat de identiteit van een relatie overeenkomt met die van een (rechts)persoon of entiteit als bedoeld in de sanctieregelgeving. In dat geval moet er melding van worden gedaan aan de toezichthouder.

De AFM en DNB beoordelen en handhaven vanuit hun toezichhoudende taak de effectiviteit van de door de instellingen getroffen procedures en maatregelen die zijn gericht op de naleving van de sanctiewetgeving. Praktisch gezien kan een instelling voor het treffen van maatregelen aansluiting zoeken bij bestaande administratieve organisatie en interne controle (AO/IC) voorschriften, die voortvloeien uit andere regelgeving zoals de Wft en de WWFT. Bij het vormgeven van de AO/IC door de financiële instelling is het uitgangspunt dat zij handelen in lijn met de doelstellingen van de sanctieregelgeving. Kort gezegd, instellingen zijn in staat hun administratie zodanig te controleren dat de in de sanctieregelgeving genoemde (rechts)personen en entiteiten (en hun financiële middelen) kunnen worden opgemerkt. De financiële middelen moeten direct bevroren kunnen worden en/of voorkomen moet worden dat financiële middelen en/of diensten aan deze (rechts)personen en entiteiten ter beschikking worden gesteld. Als de instelling constateert dat de identiteit van een relatie overeenkomt met een (rechts)persoon of entiteit als bedoeld in de sanctieregelgeving (zogenaamde 'hit'), dient de instelling dit direct aan de toezichthouder te melden. Ter ondersteuning van de beoordeling of er sprake is van een zogenaamde 'hit' hebben AFM en DNB een meldprocedure opgesteld.

Een adequate controle omvat onder meer het vergelijken van de identiteit van nieuwe en bestaande relaties met de identiteit van (rechts)personen of entiteiten genoemd in de sanctieregelgeving. Onder relatie wordt verstaan een ieder die betrokken is bij een financiële dienst of een financiële transactie, zoals;

- cliënten;
- begunstigen van een product (bijvoorbeeld bij een uitkering op een leveringsverzekering) of (internationale) overboeking van gelden;
- uiteindelijk belanghebbende bij financiële middelen;
- correspondentbanken;
- wederpartij bij een financiële transactie/product (bijvoorbeeld bij uitkering van een schadeverzekering³⁰);
- gemachtigden;
- betrokkene(n) bij een financiële transactie waarbij een doelvennootschap van een trustkantoor partij is.

Als de identiteit van een relatie overeenkomt met die van een (rechts)persoon of entiteit genoemd in de sanctieregelgeving (een zogenaamde 'hit') moet dit worden gemeld aan de toezichthouder. Het gaat dan om overeenkomsten tussen namen en overige te identificeren gegevens, zoals geboortedatum en woonplaats. Gemeld worden: identiteitsgegevens als bedoeld in de WWFT, de omvang van het bevroren saldo, het rekeningnummer, de aard van de relatie, naam- en adresgegevens van de contactpersoon binnen de instelling en de toepasselijke sanctieregeling. Er bestaat een door AFM en DNB opgesteld meldformat dat voor de melding moet worden gebruikt en ingevuld naar de betreffende toezichthouder moet worden verstuurd.

Tegoeden moeten bevroren blijven totdat de betreffende sanctieregeling gewijzigd wordt en de verplichting om te bevriezen ophoudt te bestaan of anderszins tegenbericht van de toezichthouder wordt ontvangen. DNB hanteert de lijn dat er naar aanleiding van een melding van een bevroren tegoed alleen bericht aan de meldende instelling wordt verstuurd indien het tegoed vrijgegeven kan worden. Indien de instelling niets verneemt van DNB dient er van uit gegaan te worden dat het tegoed als een daadwerkelijke 'hit' moet worden beschouwd en dat het bevroren dient te blijven tot nader bericht.

Gemelde gegevens moeten worden bewaard tot 5 jaar nadat de betreffende sanctieregeling niet meer van kracht is of buiten werking is gesteld.

³⁰ De WWFT is alleen van toepassing op levensverzekeraars, echter de SW is ook van toepassing op schade- en natura-uitvaartverzekeraars.