Post-event transactie-monitoringsproces bij money transfer organisaties

Guidance

DeNederlandscheBank

EUROSYSTEEM

12 september 2017

Westeinde 1, 1017 ZN Amsterdam – Postbus 98, 1000 AB Amsterdam
Telephone +31 20 524 91 11 – E-mail: info@dnb.nl
Website: www.dnb.nl

In dit document leest u onze belangrijkste bevindingen naar aanleiding van het in 2016 uitgevoerde thema-onderzoek post-event transactie-monitoring bij MTO's.[1] Deze bevindingen laten zien dat MTO's hun transactiemonitoringsproces nog niet op orde hebben om witwas- en terrorisme-financieringsrisico's te beheersen. Wij delen met dit document de belangrijkste uitkomsten van dit onderzoek en bieden u guidance hoe u uw transactie-monitoringsproces kunt verbeteren. Deze uitkomsten zijn van toepassing op zowel Nederlandse als buitenlandse MTO's die door middel van notificaties actief zijn op de Nederlandse markt. Het spreekt voor zich dat de eigen omstandigheden van uw MTO ten aanzien van de te treffen oplossingen en maatregelen in aanmerking dienen te worden genomen. U maakt hierin uw eigen afweging.

Toelichting brochure

Deze brochure is als volgt opgebouwd. Na de inleiding vindt u eerst een korte beschrijving van het transactiemonitoringsproces en presenteren wij u het 'volwassenheidsmodel' dat wij bij de uitvoering van het thema-onderzoek hebben toegepast. Daarna leest u per onderdeel van dit model onze guidance. De guidance start met de hoofdbevindingen uit het onderzoek, waarna een toelichting volgt. Vervolgens vindt u per onderdeel van het volwassenheidsmodel praktijkvoorbeelden, voorbeelden van hoe het kan en voorbeelden van hoe het niet zou moeten, die wij in het onderzoek hebben aangetroffen.

Verantwoording

Transactiemonitoring en het onverwijld melden van een ongebruikelijke transactie zijn essentiële maatregelen om integriteitrisico's op het gebied van witwassen en terrorismefinanciering te beheersen. DNB constateerde vorig jaar in een thema-onderzoek dat veel onderzochte MTO's hun transactiemonitoringsproces nog onvoldoende op orde hebben. In deze guidance biedt DNB handvatten voor MTO's om hun transactie-monitoring te verbeteren. Deze guidance is medio mei in concept gepubliceerd, waarna DNB met de sector (eerste- en tweedelijnsverantwoordelijken voor transactiemonitoring) in gesprek is gegaan om feedback te krijgen over dit concept. Op een aantal onderdelen ziet de sector ruimte voor verduidelijking, te weten:

- expliciet benoemen dat transactiemonitoring risicogebaseerd kan plaatsvinden;
- de omgang met verwacht transactiegedrag waar sprake is van incidentele transacties;
- toelichting op het begrip 'voorgenomen transactie';
- proportionaliteit, waaronder voorbeelden data-analyse voor kleinere instellingen;
- het nog concreter maken van voorbeelden in de tekst, waaronder de business rules in het transactiemonitoringssysteem.

De feedback is – voor zover relevant – verwerkt in bijgaande definitieve guidance.

1 Het betrof een cross-sectoraal onderzoek, uitgevoerd bij banken, betaalinstellingen, MTO's en trustkantoren.

Inhoud

1 Inleiding

1.1 Waarom deze guidance?

Financieel-economische criminaliteit is een groot probleem in onze huidige maatschappij. De samenleving is ongewild slachtoffer van deze vorm van criminaliteit, denk aan recente incidenten als de Panama Papers en terroristische aanslagen in West-Europa. Financiële instellingen, waaronder MTO's, spelen een belangrijke rol bij het voorkomen van witwassen en terrorismefinanciering. Daartoe voeren MTO's onder meer cliëntenonderzoek uit: door middel van zogenoemde *customer due diligence* en het monitoren van uitgevoerde transacties van cliënten met als doel ongebruikelijke transacties te kunnen identificeren. Dit laatste, de transactiemonitoring, is onderwerp van deze guidance.

Een MTO die adequaat monitort welke transacties in het kader van haar dienstverlening worden uitgevoerd, kan tijdig actie ondernemen (nader onderzoek en eventueel melden) als sprake is van een (mogelijk) ongebruikelijke transactie of een meldenswaardig transactiepatroon. Gebeurt dit niet, of niet goed, dan kan het zijn dat een MTO (ongewild) bijdraagt aan het financieren van terrorisme of het witwassen van geld. De functie als poortwachter van het Nederlandse financiële systeem vergt onder meer dat MTO's adequaat transacties monitoren. Continu en alert.

Daarom heeft de wetgever op dit gebied eisen geformuleerd waaraan een MTO moet voldoen. DNB heeft in dit verband de wettelijke taak om toe te zien op naleving van de wet- en regelgeving. Transactiemonitoring is verplicht voor iedere MTO; dit vereiste is principle-based, d.w.z. de praktische invulling hiervan wordt niet in detail voorgeschreven door wet- en regelgeving.

Het onderwerp transactiemonitoring is voor MTO's niet nieuw. De in dit document opgenomen aandachtspunten en voorbeelden zijn specifiek bedoeld als handvatten voor het transactiemonitoringsproces van MTO's en gelden daarmee als een aanvulling op geldende wet- en regelgeving en eerder uitgebrachte leidraden over dit onderwerp, zoals de *DNB Leidraad Wwft en SW, versie 3.0; april 2015*[2]*; Voorkoming misbruik financiële stelsel voor witwassen en financieren van terrorisme en beheersing van integriteitrisico en de Q&A Beoordeling Ongoing Due Diligence Proces (WWFT en SW)* (van december 2013).

De in dit document opgenomen handvatten kunnen uw MTO helpen met het op orde brengen van uw transactiemonitoringsproces. DNB verwacht dan ook dat u als sector goed kennis hiervan neemt en daar waar nodig verbeteringen implementeert in uw bedrijfsvoering.

2 Wwft: Wet ter voorkoming van witwassen en financieren van terrorisme; SW: Sanctiewet 1977.

1.2 Leeswijzer

Met dit document biedt DNB u guidance over hoe u uw transactiemonitoringsproces kunt inrichten en kunt verbeteren. Bij de totstandbrenging van deze guidance heeft DNB gebruik gemaakt van de belangrijkste bevindingen van het in 2016 uitgevoerde thema-onderzoek 'post-event transactiemonitoring bij MTO's'.[3] Deze bevindingen hebben laten zien dat de onderzochte MTO's hun transactiemonitoringsproces nog niet op orde hebben om risico's van witwassen en terrorismefinanciering te beheersen. Het spreekt voor zich dat u de eigen omstandigheden van uw MTO in aanmerking neemt bij de oplossingen en maatregelen die u treft. U maakt hierin uw eigen afweging.

Deze guidance is als volgt opgebouwd. Na de inleiding vindt u eerst een korte beschrijving van het transactiemonitoringsproces en presenteren wij u het zogeheten 'volwassenheidsmodel' dat bij de uitvoering van het thema-onderzoek in 2016 toegepast is. Daarna leest u per onderdeel van dit model onze guidance. De guidance start met de hoofdbevindingen uit het onderzoek, waarna een toelichting volgt. Vervolgens vindt u per onderdeel van het volwassenheidsmodel praktijkvoorbeelden, zowel goede als minder goede voorbeelden, die wij in het thema-onderzoek hebben aangetroffen.

3 Het thema Transactiemonitoring was een zogenaamd cross-sectoraal onderzoek, wat wil zeggen uitgevoerd in verschillende sectoren (vier banken, vier betaalinstellingen, drie money transferkantoren en zes trustkantoren). Voor de overige sectoren is een vergelijkbare guidance opgesteld. In verband met de continu verhoogde terreurdreiging in Nederland en Europa lag in het onderzoek extra focus op de wijze van transactiemonitoring in relatie tot risico's op terrorismefinanciering, vandaar dat wij daar ook specifieke uitkomsten over delen.

2 Samenvatting

Transactiemonitoring is een essentiële maatregel om met name mogelijk ongebruikelijke transacties te melden bij de FIU, om zo de integriteitrisico's op het gebied van witwassen en terrorismefinanciering te beheersen. DNB heeft bij het in 2016 uitgevoerde thema-onderzoek Transactiemonitoring geconstateerd dat de onderzochte MTO's hun post-event transactiemonitoringsproces nog niet op orde hebben. De belangrijkste bevindingen ten aanzien van deze MTO's luiden:

1. DNB heeft geconstateerd dat de onderzochte MTO's de risico's t.a.v. witwassen en terrorisme-financiering die uit de SIRA voortvloeien niet voldoende vertalen naar het transactie-monitoringsproces. DNB constateert verder dat de onderzochte MTO's bij de bepaling van het risicoprofiel van de cliënt en/of 'cliënt peergroups' het verwachte transactiegedrag niet (voldoende) betrekt.
2. Gebleken is dat niet alle onderzochte MTO's voldoende beleid voor transactiemonitoring hebben opgesteld en dit derhalve ook niet altijd voldoende hebben uitgewerkt in onderliggende procedures en werkprocessen.
3. De onderzochte MTO's beschikken over een geautomatiseerd transactiemonitoringssysteem, maar hebben veelal geen onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren.
4. Gebleken is dat de onderzochte MTO's voorgenomen en uitgevoerde ongebruikelijke transacties niet altijd onverwijld en volledig aan de FIU-NL melden. Ook bleek dat het alertafhandelingsproces niet altijd adequaat werd gedocumenteerd, met name overwegingen om te komen tot het sluiten dan wel escaleren van alerts en conclusies daaromtrent ontbraken.
5. De governance van de onderzochte MTO's ten aanzien van transactiemonitoring bleek niet altijd op orde te zijn, met name wat betreft een duidelijke rolverdeling tussen de t*hree lines of defence*.
6. Het onderzoek liet zien dat de onderzochte MTO's niet altijd beschikken over een toegesneden trainingsprogramma voor hun medewerkers en de medewerkers zich niet altijd bewust toonden van witwas- en terrorismefinancieringsrisico's.

3 Wettelijke context en reikwijdte

3.1 Transactiemonitoring: wettelijke verplichting tot voortdurende controle

MTO's zijn wettelijk verplicht maatregelen te nemen om witwassen en terrorismefinanciering tegen te gaan. Hierdoor moeten zij bijzondere aandacht besteden aan ongebruikelijke transactiepatronen en transacties van cliënten, die naar hun aard een hoger risico op witwassen of het financieren van terrorisme met zich meebrengen. Indien aanleiding bestaat om te veronderstellen dat een (voorgenomen) transactie verband houdt met witwassen of terrorisme-financiering, moet u als MTO deze als ongebruikelijke transactie melden bij de Financial Intelligence Unit – Nederland (FIU-NL).[4] Om dit te kunnen doen is het van cruciaal belang dat MTO's beschikken over een effectief transactiemonitoringsproces.[5]

Om een adequate voortdurende controle uit te oefenen, dienen Nederlandse MTO's op grond van artikel 10 Besluit prudentiële regels Wft (Bpr) allereerst zorg te dragen voor een systematische integriteitrisicoanalyse (SIRA). Ook van buitenlandse MTO's die actief zijn op de Nederlandse markt verwacht DNB dat zij hun integriteitsrisico's in beeld brengen en mitigerende maatregelen nemen. Integriteitsrisico's zijn daarbij gedefinieerd als het 'gevaar voor aantasting van de reputatie of bestaande of toekomstige bedreiging van vermogen of resultaat van een financiële onderneming als gevolg van een ontoereikende naleving van hetgeen bij of krachtens enig wettelijk voorschrift is voorgeschreven'.[6] Daartoe behoren dus ook de risico's met betrekking tot witwassen en financieren van terrorisme. Indien naar aanleiding van deze analyse (rest)risico's gesignaleerd worden, moeten MTO's hiervoor beleid formuleren, procedures inrichten en maatregelen treffen.

Specifiek ten aanzien van de risico's met betrekking tot witwassen en terrorismefinanciering bepaalt de Wwft dat money transfers worden beschouwd als zakelijke relaties.[7] Een zakelijke relatie is zakelijke, professionele, of commerciële relatie tussen een instelling en een natuurlijke persoon of een rechtspersoon, die verband houdt met de professionele activiteiten van die instelling en waarvan op het tijdstip dat het contact wordt gelegd, wordt aangenomen dat deze enige tijd zal duren. Indien sprake is van een zakelijke relatie moet een MTO onderzoek doen naar zijn cliënten.[8] Daarbij moet u als MTO het doel en de beoogde aard van de zakelijke relatie vaststellen. Ook moet u een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze zakelijke relatie verrichte transacties uitoefenen.[9] Zo kunt u als

4 Kort gezegd spreken wij hierna in dit document over 'ongebruikelijke transacties'.
5 Artikelen 2a, lid 1 en 3, lid 2 sub d Wwft.
6 Artikel 1 Bpr.
7 Memorie van toelichting bij wijzigingswet Wwft van 19 april 2012.
8 Art. 2a, lid 1 en art. 3, lid 1 Wwft.
9 In artikel 1, lid 1, sub m, Wwft, wordt een transactie als volgt gedefinieerd: een transactie is een handeling of samenstel van handelingen van of ten behoeve van een cliënt, waarvan een instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen.

MTO verzekeren dat de uitgevoerde transacties overeenkomen met de kennis die u heeft van de cliënt en diens risicoprofiel, met zo nodig een onderzoek naar de bron van de middelen die bij de zakelijke relatie of de transactie gebruikt worden.[10]

DNB realiseert zich dat het niet altijd mogelijk is om voor iedere individuele relatie op voorhand een risicoprofiel op te stellen. Om dit praktisch te kunnen doen kan een MTO haar zakelijke relaties bijvoorbeeld indelen naar zogenoemde 'peer groups'. Daarbij definieert de MTO haar eigen peer groups aan de hand van een aantal overeenkomstige cliëntkenmerken (bijvoorbeeld leeftijden natuurlijke personen, landen, et cetera).

Het begrip 'voortdurende controle' staat centraal in het proces van transactiemonitoring en kan door uw MTO op eigen wijze risico gebaseerd worden ingevuld. Risico gebaseerd wil in dit verband zeggen dat u de meeste aandacht zult besteden aan hetgeen u als grootste risico's heeft geïdentificeerd. Deze risico gebaseerde aanpak moet daarom te allen tijde onderbouwd kunnen worden met de uitkomsten van de integriteitsrisicoanalyse. Verwacht mag worden dat uw MTO beschikt over een systeem waarbij transacties worden gemonitord, en mogelijk ongebruikelijke transactiepatronen en transacties worden ingebracht in een alertafhandelingsproces. Om dergelijke transactiepatronen en transacties te kunnen identificeren, heeft u red flags geïdentificeerd en deze uitgewerkt in business rules. Bij dit proces dient u bijzondere aandacht te hebben besteed aan ongebruikelijke transactiepatronen en transacties die naar hun aard een hoger risico op witwassen of financieren van terrorisme meebrengen.[11]

Een verrichte of voorgenomen ongebruikelijke transactie moet onverwijld worden gemeld aan de FIU-NL, zodra het ongebruikelijke karakter van de transactie bekend is geworden.[12] De MTO dient dan ook specifieke procedures en werkprocessen te hebben opgesteld om transactiealerts te beoordelen, af te handelen en ongebruikelijke transacties te melden.[13] Ter waarborging van deze procedures en maatregelen dient een MTO zorg te dragen dat haar werknemers, voor zover relevant voor de uitoefening van hun taken, bekend zijn met de Wwft en periodiek training krijgen. Dit moet hen in staat stellen het cliëntenonderzoek goed en volledig uit te voeren en ongebruikelijke transacties te herkennen en door te geleiden.[14]

DNB heeft in 2016 onderzoek uitgevoerd naar het transactiemonitoringsproces bij MTO's. De uitkomsten van dit onderzoek laten zien dat onderzochte MTO's dit proces op een aantal belangrijke onderdelen nog niet op orde hebben (zie de hiervoor opgenomen samenvatting).

10 Art. 3, lid 2, sub d Wwft.
11 Art. 2a, lid 1 Wwft.
12 Art. 16 Wwft.
13 Art. 16 Wwft jo. artt. 17 en 18 Bpr.
14 Art. 35 Wwft.

Zoals hiervoor is gesteld, leest u in dit document aan welke wettelijke vereisten MTO's dienen te voldoen en hoe DNB de invulling van deze norm, conform internationale standaarden en good practices, voor ogen heeft. Wij illustreren dit aan de hand van onze onderzoeksuitkomsten, waarbij wij zowel good practices geven als voorbeelden waarbij de norm volgens DNB onjuist is ingevuld. In verband met de continu verhoogde terreurdreiging in Nederland en Europa lag in het onderzoek extra focus op de wijze van transactiemonitoring in relatie tot risico's op terrorismefinanciering, vandaar dat wij daar ook specifieke uitkomsten over delen.

Dit document is als volgt opgebouwd. In hoofdstuk 4 geven wij een schematische weergave van hoe een transactiemonitoringsproces eruit kan zien. Ook kunt u daar het door DNB bij het onderzoek gehanteerde volwassenheidsmodel vinden. In hoofdstuk 5 leest u onze belangrijkste bevindingen, good practices en voorbeelden hoe het niet moet.

3.2 Reikwijdte

Deze guidance is op grond van de artikelen 1, lid 1 en 2, lid 1, Wwft, van toepassing op:

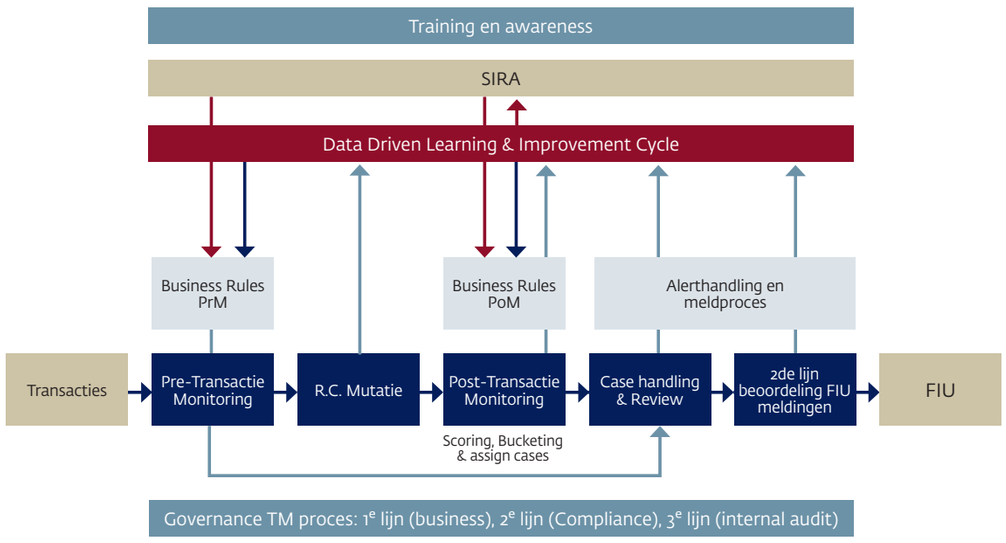
- in Nederland gevestigde MTO's
- betaaldienstagenten en bijkantoren in Nederland van MTO's met een zetel buiten Nederland.
- Deze guidance kent voor internationaal opererende MTO's een brede reikwijdte: wanneer deze instellingen bijkantoren of dochtermaatschappijen hebben in een staat die geen EU lidstaat is dan moeten zij hun transactiemonitoringsproces zo inrichten dat deze gelijkwaardig is aan de eisen die de Wwft stelt.

4 Transactiemonitoring

4.1 Het transactiemonitoringsproces

Het transactiemonitoringproces kan er als volgt uitzien:

Figuur 1 Het transitiemonitoringsproces



Transactiemonitoring kan op verschillende manieren worden uitgevoerd. Zoals uit het schema blijkt kan sprake zijn van pre-transactiemonitoring en post-event transactiemonitoring, en liefst van beide, dat wil zeggen dat zowel vooraf als achteraf transacties worden gemonitord.

Pre-transactiemonitoring

Pre-transactiemonitoring vindt plaats voordat de transactie is uitgevoerd. Een cliënt komt bijvoorbeeld bij de balie van een MTO en wil een bepaalde geldtransactie uitvoeren of een chartale hoeveelheid geld op een bankrekening storten.
Bij post-event transactiemonitoring is de transactie reeds door de MTO uitgevoerd en vindt de transactiemonitoring achteraf plaats.

Hoewel de focus van transactiemonitoring op post-event transactiemonitoring ligt, is DNB van oordeel dat pre-transactiemonitoring (al dan niet in de vorm van een niet-geautomatiseerd proces) een effectieve bijdrage levert omdat juist hier het klantcontact plaatsvindt. De front-office heeft zodoende een grote verantwoordelijkheid met betrekking tot het detecteren van mogelijke ongebruikelijke transacties (waaronder witwassen dan wel terrorismefinanciering). Dit is van belang wanneer bij aanvang van de cliëntrelatie een duidelijk profiel van verwachte transacties wordt gemaakt dat vervolgens gebruikt kan worden voor monitoring.[15] Hierdoor kan een instelling ongebruikelijke transacties mogelijk reeds voor effectuering detecteren en deze voorgenomen transactie onverwijld melden aan de FIU-NL.

Good practice

De baliemedewerkers van een MTO hebben aan de balie direct inzicht in de transactiehistorie van een cliënt. Voor een nieuwe transactie wordt uitgevoerd checkt de baliemedewerker of de voorgenomen transactie past in het patroon van de cliënt. Ook checkt de medewerker of het aantal transacties van de cliënt en de daarbij betrokken bedragen wel passen in het algemene profiel van de 'peer group'.

Good practice

De baliemedewerkers van een MTO zijn erop getraind om van iedere (potentiële) cliënt en bij iedere voorgenomen transactie de ID van de cliënt op te vragen en te scannen of te kopiëren. Zo is de MTO in staat om ook bij voorgenomen ongebruikelijke transacties een melding te doen bij FIU-NL.

15 Voor u als MTO zal het niet altijd mogelijk zijn om effectief een verwacht transactiepatroon op te stellen, bijvoorbeeld bij incidentele transacties. Echter, zie ook wat hiervoor is opgemerkt over 'peer groups' in paragraaf 3.1.

Post-event transactiemonitoring

Ons themaonderzoek had specifiek betrekking op het post-event transactiemonitoringproces, omdat MTO's vooral op deze wijze witwas- en terrorismefinancieringsrisico's kunnen detecteren, bijvoorbeeld op basis van netwerkanalyses. Wij benadrukken echter het belang dat MTO's beschikken over een pre-transactiemonitoringsproces. MTO's treffen daarin adequate maatregelen om ongebruikelijke transacties te detecteren voordat deze uitgevoerd worden dan wel ten tijde van de uitvoering.

Door het uitvoeren van cliëntenonderzoek en transactiemonitoring verkrijgt u als MTO doorlopend kennis van de cliënt, waaronder het doel en de beoogde aard van de zakelijke relatie met de cliënt. Daarbij beoordeelt u risicogericht of bij de door de cliënt uitgevoerde transacties sprake is van ongebruikelijke patronen die kunnen duiden op witwassen of terrorismefinanciering. Het monitoren van de transacties van de cliënt stemt u af op de cliënt zelf: het soort cliënt, het type dienstverlening aan de cliënt en het risicoprofiel van de cliënt of het type cliënt. Per (type) cliënt en per product kan de monitoring daarom verschillend ingericht worden ('peer grouping').

De eerste stap in het transactiemonitoringsproces is risico-identificatie. Tijdens het risico-identificatieproces analyseert u als MTO systematisch de witwas- en terrorismefinancieringsrisico's die uw verschillende soorten cliënten, producten, distributiekanalen en transacties met zich brengen. De uitkomsten van deze analyse legt u vast in de zogenoemde SIRA/Integriteitsrisicoanalyse. Deze SIRA vertaalt u vervolgens naar uw beleid, bedrijfsprocessen en procedures omtrent transactiemonitoring.

Bij het identificeren van de risico's hoort tevens het indelen van de cliënten van uw MTO in risicocategorieën (bijvoorbeeld hoog, midden en laag), op grond van de witwas- en terrorismefinancieringsrisico's die de zakelijke relatie met de cliënt met zich meebrengt. Voor de bepaling van het risicoprofiel van een cliënt maakt u waar mogelijk een transactieprofiel op basis van de *verwachte* transacties van een cliënt.[16] Door bijvoorbeeld via 'peer grouping' een transactieprofiel aan te maken kan uw MTO in voldoende mate monitoren dat de tijdens de duur van de relatie verrichte transacties overeenkomen met de kennis die u heeft van de cliënt en diens risicoprofiel. Door het *verwachte* transactiegedrag van de cliënt in beeld te brengen, kunt u toetsen of de door de cliënt uitgevoerde transacties overeenkomen met de kennis die u heeft van de cliënt.

Een goed werkbaar transactieprofiel voldoet in ieder geval aan de volgende eisen:

1. Actueel: het transactieprofiel is up-to-date en voorzien van een datum. Alle (relevante) wijzigingen worden tijdig verwerkt.
2. Volledig: alle namen van de begunstigden en/of buitenlandse opdrachtgevers, betalingsbevoegden en alle relevante activiteiten zijn opgenomen.
3. Specifiek: de verwachte uitgaande en/of inkomende geldstromen zijn duidelijk beschreven, onder andere de bedragen, diensten, doel transacties en de frequentie. Opgenomen (grens) bedragen zijn goed onderbouwd en kunnen daadwerkelijk bijdragen aan het herkennen van ongebruikelijke transacties.
4. Overzichtelijk: met inzichtelijke schema's zijn geldstromen op eenvoudige wijze goed en overzichtelijk weergegeven.
5. Onderbouwd: het transactieprofiel is onderbouwd, waar nodig met relevante stukken die de geprognosticeerde geldstromen toelichten en verklaren.
6. Vastgelegd: het transactieprofiel is vastgelegd in het cliëntendossier.

Voor de tweede stap, het detecteren van ongebruikelijke transactiepatronen en transacties die kunnen duiden op witwassen of financieringen van terrorisme, maakt u gebruik van een (post-event) transactiemonitoringssysteem. Voordat u hiervan gebruik maakt, borgt u dat alle bronsystemen van de te monitoren transacties zijn geïdentificeerd en dat de data volledig en juist wordt meegenomen in het transactiemonitoringsproces (dit betreft bijvoorbeeld data over cliënt en transacties). Indien sprake is van grotere hoeveelheden transacties, ligt het in de rede om de transactiemonitoring geautomatiseerd te laten plaatsvinden om de effectiviteit, consistentie en doorlooptijd van monitoring te kunnen borgen.

In het systeem neemt u op zijn minst vooraf gedefinieerde *business rules* op: detectieregels in de vorm van scenario's en grensbedragen. Daarnaast zijn ook netwerkanalyses een belangrijk detectiemiddel.

Met behulp van uw transactiemonitoringssysteem en gebruik van specifieke en intelligent ingerichte software kunt u – als derde stap – deze data analyseren. Het systeem genereert op basis van *business rules* alerts. Met een alert wordt een signaal bedoeld dat duidt op een mogelijk ongebruikelijke transactie, dan wel een transactie met hoogrisico-karakter dat u op grond van de risicogerichte benadering wilt onderzoeken. De bevindingen van uw onderzoek van de alerts worden adequaat en duidelijk vastgelegd. Wanneer uit de onderzoeksbevindingen blijkt dat de transactie ongebruikelijk is, meldt u deze transactie onverwijld aan de FIU-NL. De overwegingen en besluitvorming om een transactie wel of niet te melden, heeft u voldoende inzichtelijk gemaakt en vastgelegd. Op het moment dat een MTO – al dan niet opzettelijk – niet voldoet aan de meldplicht, dan kan dat een economisch delict zijn.

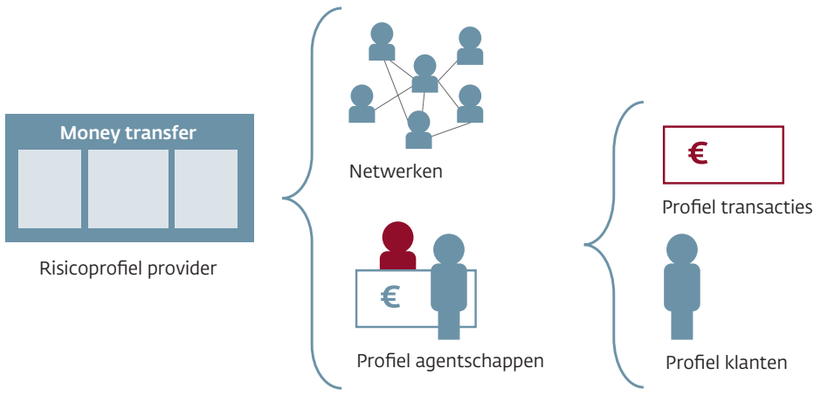
Vervolgens beoordeelt u de gevolgen van een melding aan de FIU-NL en een eventuele terugmelding van de FIU-NL voor het risicoprofiel van de cliënt of eventuele aanvullende beheersmaatregelen genomen moeten worden. Sluitstuk van het transactiemonitoringsproces is de bewaring van gegevens die u verkrijgt in het kader van transactiemonitoring. In dit verband bewaart de MTO de gegevens van de melding van de ongebruikelijke transactie en legt deze vast, op zodanige wijze dat die gegevens opvraagbaar zijn en de desbetreffende transactie reconstrueerbaar is gedurende vijf jaar na het tijdstip van het doen van de melding.

16 DNB verwijst in deze naar de Leidraad Wwft en SW, versie 3.0, april 2015, pagina's 29-32, waar guidance wordt gegeven hoe een instelling dit zou kunnen doen. Zie ook de vorige noot.

4.2 Transactiemonitoringsproces MTO's

U dient bij de inrichting van uw TM-proces rekening te houden met wat hiervoor al is beschreven. Verder is ook het risicoprofiel van uw eigen onderneming van belang. Onderstaand ziet u in een schema hoe een risicoprofiel kan worden weergegeven:

Figuur 2 Risicoprofiel provider



Het risicoprofiel van uw instelling wordt onder andere bepaald door de mate waarin uw agenten de werkzaamheden uitvoeren in overeenstemming met de wettelijke vereisten. Daarnaast wordt uw risicoprofiel ook bepaald door mogelijke netwerken van transacties c.q. van cliënten die verband kunnen houden met witwassen en/of terrorismefinanciering.

Om die reden monitort u uw uitgevoerde transacties, cliënten, en (buitenlandse) agenten en contractpartijen. De uitkomsten van de monitoring geven inzicht in het risico dat de MTO loopt bij de uitvoering van de werkzaamheden. Hoe groter bijvoorbeeld bij een agent het aandeel opvallende transacties en opvallende klantprofielen is, hoe groter de kans is dat bij de betreffende agent de controle gebrekkig is.

In de leidraad Wwft van DNB uit 2015 is het volgende opgenomen over monitoring bij money transfers:

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 cliënten (op bestaan controleren en meervoudig gebruik);
- transacties juist onder de objectieve meldgrens (het zogenaamde 'smurfen');
- analyses per locatie (afzetpunt)

Hieronder ziet u aanvullend enkele andere voorbeelden van scenario's die voor u relevant kunnen zijn, en in de praktijk ook worden toegepast:

Opvallende transacties

1. Eigenschappen
- Bedrag van transactie is hoger dan € 3.000
- Bedrag is net onder de meldgrens (€ 1.950 - € 1.999)
- Verzender is een stichting zonder registratie KvK
- Ontvanger is een stichting zonder registratie KvK

2. Selectiecriteria

Als het profiel van de transactie één van deze eigenschappen bevat dan is het transactieprofiel opvallend

Opvallende klantprofielen

1. Eigenschappen
- Meer dan € 5.000 in een kwartaal verzonden
- Meer dan 3 transacties net onder de meldgrens (€ 1.950 - € 1.999)
- Meer dan 12 transacties per kwartaal
- Meer dan 3 transacties per dag
- Meer dan 3 verschillende verzenders/ontvangers
- Meer dan 3 verschillende bestemmings- en herkomstlanden

2. Selectiecriteria

Als het profiel van de klant één van deze eigenschappen bevat dan is het klantprofiel opvallend

Opvallende agentprofielen

1. Kernprofiel agent

Per agent worden de volgende eigenschappen per kwartaal bepaald:
- Totale omzet
- Aantal transacties
- Aantal verzenders
- Aantal ontvangers

2. Aspecten opvallend agentprofiel
- Aandeel opvallende transacties
- Aandeel opvallende klantprofielen

3. Selectiecriteria

Bepalen welke agenten sterk afwijken van het kernprofiel en/of welke agenten relatief veel opvallende transacties dan wel klantprofielen hebben

Opvallende transacties

Om opvallende transacties (profielen) te detecteren stelt u (geautomatiseerde) indicatoren/scenario's op en implementeert u deze in uw transactiemonitorings-systeem. Hierbij kunt u bijvoorbeeld denken aan transacties die bepaalde limieten overstijg.

Opvallende klanten

Opvallende klanten (profielen) worden kunt u ook identificeren met (geautomatiseerde) indicatoren/ scenario's. Denk bijvoorbeeld aan het geval dat een klant een bepaalde limiet aan transacties per periode overschrijdt.

Risicoprofiel van de agent

Tot slot helpt de analyse van opvallende transacties en opvallende klanten om het risicoprofiel van de agent te bepalen. Om de agenten goed te kunnen monitoren kan per kwartaal een kernprofiel van elke agent worden opgesteld op basis van de totale omzet, aantal transacties, aantal verzenders en aantal ontvangers. Vervolgens kan met gebruikmaking van dit kernprofiel het aandeel ongebruikelijke transacties en klanten van het totaal worden berekend, en daarmee het risicoprofiel van de agent.

4.3 Voorbeeld netwerkanalyses bij terrorismefinanciering

DNB beschikt sinds 2012 over alle in Nederland verrichte inkomende en uitgaande money transfers. DNB heeft de transacties door middel van netwer-kanalyses nader geanalyseerd om te onderzoeken of de uitkomsten bruikbaar zijn voor het detecteren van terrorismefinanciering. De methodiek die DNB hanteert is dat in eerste instantie de transacties van en naar risicolanden worden geïsoleerd. Vervolgens voert DNB hierop netwerkanalyses uit. Indien uit deze analyses belangrijke groepen van personen in beeld komen wordt vervolgens gekeken of de in het netwerk voorkomende personen ook transacties verrichten naar Europese landen. Deze laatste stap wordt uitgevoerd om mogelijke ondersteuning van terreurcellen in Europa te detecteren. MTO's kunnen op vergelijkbare wijze netwerkanalyses uitvoeren op risicolanden om netwerken die mogelijk duiden op terrorismefinanciering te detecteren en te melden aan FIU-NL.

4.4 Volwassenheidsmodel

Het themaonderzoek (post-event) transactie-monitoring bij MTO's zag op het beoordelen van de opzet, het bestaan en de werking van hun post-event transactiemonitoringsproces. Bij de uitvoering van het themaonderzoek is gebruik gemaakt van een door DNB ontwikkeld volwassenheidsmodel voor transactie-monitoring. Dit model houdt rekening met de relevante vereisten uit de Wft en Wwft en is bedoeld om aan te geven waar een MTO zich qua volwassenheid in het transactiemonitoringsproces bevindt. In dit model wordt de mate van naleving (van non-compliance tot best practice) op zes gebieden toegelicht aan de hand van een vierpuntschaal:
- Rode score: geheel non-compliant
- Oranje score: onvoldoende compliant
- Gele score: in voldoende mate compliant
- Groene score: best practice.

Het ambitieniveau van een MTO kan afhankelijk zijn van het risicoprofiel van de instelling. Een gele score betekent dat u voldoet aan de minimale wettelijke vereisten (in voldoende mate compliant).

In de bijlage ziet u het volwassenheidsmodel nader uitgewerkt, inclusief de mogelijke scores op de zes toetsingselementen.

In hoofdstuk 5 hierna leest u per toetsingselement onze uitkomsten en voorbeelden (goede en minder goede voorbeelden van de invulling van de norm). De goede voorbeelden illustreren hoe een MTO erin geslaagd is om dat gebied een gele of groene score te halen.

5 Guidance

5.1 SIRA/Integriteitsrisicoanalyse

DNB heeft geconstateerd dat alle onderzochte MTO's hun risico's met betrekking tot witwassen en terrorismefinanciering die uit de integriteitsrisicoanalyse (voor Nederlandse vergunninghouders de SIRA) voortvloeien niet in voldoende mate vertalen naar het transactie-monitoringsproces.

Belangrijke integriteitrisico's voor MTO's zijn financieel-economische criminaliteitsrisicio's witwassen, zoals financieren van terrorisme, niet-naleving van sancties, corruptie/omkoping en belangenverstrengeling. Om te waarborgen dat uw MTO de integriteitrisico's adequaat beheerst, heeft de wetgever verschillende verplichtingen opgenomen waaraan moet worden voldaan. Hierbij speelt de SIRA[17] een centrale rol. Deze risicoanalyse op organisatieniveau (waarbij zowel eerste als tweede lijn betrokken zijn geweest) legt de basis voor uw (periodiek te herzien) integriteitsbeleid en dient te worden vertaald naar procedures en maatregelen. De uitkomsten van de SIRA/ integriteitsrisicoanalyse moeten binnen uw gehele organisatie leven en moeten ook terug te vinden zijn in de risicoanalyses op cliëntniveau.

5.1.1 Risicoprofiel: verwacht transactiegedrag

DNB constateert dat MTO's bij de bepaling van het risicoprofiel van de cliënt het verwachte transactiegedrag van de cliënt niet (voldoende) meenemen.

Op grond van de Wwft moeten MTO's bij het cliëntenonderzoek een verwacht transactieprofiel opstellen van de cliënt. Hierbij worden verschillende factoren van de cliënt beoordeeld (zoals de sector(en) en landen waarin de cliënt actief is, de bij de MTO afgenomen producten en diensten). Op basis hiervan bepaalt u de risicoclassificatie van uw cliënt. De review van de cliënt en actualisatie van de cliëntgegevens vindt vervolgens periodiek (en ook tussentijds op basis van relevante gebeurtenissen) plaats. De onderliggende redenen die geleid hebben tot een risicoclassificatie gebruikt u ook voor uw transactiemonitoringsproces. Wanneer cliënten geen risicoclassificatie hebben, is het immers niet mogelijk het transactiemonitoringssysteem risicogericht in te richten. Op basis van de kennis over de cliënt kan bekeken worden of tijdens de duur van de relatie verrichte transacties overeenkomen met het beeld dat u heeft van uw cliënt en het verwachte transactieprofiel.

Om het verwachte transactiegedrag te bepalen kunt u als MTO tijdens periodieke monitoring onder meer informatie inwinnen over:

- (Verwachte) inkomende en uitgaande geldstromen, inclusief volumes, soorten tegenpartijen en landen;
- soorten transacties, distributiekanalen en de mate waarin deze zullen voorkomen (creditcard, girale overboekingen, cash stortingen en uitbetalingen, acceptgirobetalingen, et cetera).

Het verwachte transactieprofiel kan gecreëerd worden door technieken als bijvoorbeeld 'peer grouping', alsmede opgevraagd en vastgelegd worden via de periodieke CDD.

De MTO toetst bij elke nieuwe transactie of de cliënt nog voldoet aan het verwachte transactie-profiel dat is opgesteld bij aanvang van de dienstverlening. MTO's kunnen immers alleen ongebruikelijke transacties opmerken als ze een goed beeld hebben van de activiteiten van de cliënt en van wat gebruikelijke transacties zijn. Indien uit specifieke transacties of het transactieverloop blijkt dat het transactiegedrag van de cliënt afwijkt van het ex ante opgestelde risicoprofiel, gaat de MTO na of mogelijk sprake is van ongebruikelijke transacties, en of dat verdere acties moeten worden ondernomen (bijvoorbeeld een herbeoordeling van het cliëntrisicoprofiel). Daarnaast toetst de MTO de werking van alerts; bij mogelijke ongebruikelijkheid wordt immers een alert gegenereerd. Daarbij is een goede samenwerking tussen verschillende personen of afdelingen, maar ook inzicht in de transactie-historie van cliënten aan de balie, essentieel.

Aangezien het verwachte transactiegedrag bij aanvang van de zakelijke relatie met de cliënt wordt opgesteld, is de MTO primair afhankelijk van gegevens die door de cliënt over de verwachte transacties worden verstrekt. Verwacht mag worden dat MTO's bij elke nieuwe transactie beoordelen of het verwachte transactiegedrag (in hoge mate) nog steeds overeenkomt met de werkelijkheid.

DNB constateerde dat de onderzochte MTO's de uitkomsten met betrekking tot de risico's op witwassen en financieren van terrorisme vanuit hun SIRA niet hadden vertaald naar hun transactiemonitoringsproces. Zo deed een onderzochte MTO relatief veel zaken met een verhoogd risicoland, wat in haar SIRA wel was geïdentificeerd, maar niet was opgenomen in het transactiemonitoringsproces. DNB constateerde bovendien dat de onderzochte MTO's in hun SIRA onderscheid maken tussen witwassen en terrorismefinanciering, maar dit onderscheid niet tot uitdrukking brengen in het transactiemonitoringsproces. Enkele van de onderzochte MTO's bleken nauwelijks aandacht te besteden aan terrorismefinancieringsscenario's.

17 Voor nadere toelichting op de SIRA zie het document: *'De integriteitrisicoanalyse, meer waar dat moet, minder waar dat kan'*, te raadplegen via http://www.toezicht.dnb.nl/2/50-234066.jsp

5.2 Beleid en procedures

Uit het onderzoek is gebleken dat MTO's niet altijd voldoende beleid voor transactiemonitoring hebben en dit derhalve ook niet altijd hebben uitgewerkt in onderliggende procedures en werkprocessen.

Om (potentieel) ongebruikelijke transactiepatronen of transacties, waarbij mogelijk sprake is van witwassen of terrorismefinanciering, goed te kunnen detecteren is een MTO wettelijk verplicht om te beschikken over beleid, procedures en processen. Het hebben van een effectief beleid houdt onder andere in dat van iedere cliënt of cliëntgroep een risicobeoordeling en risicoprofiel wordt gemaakt en dat het verwachte transactiegedrag meeweegt in de risicobeoordeling. Tevens worden van iedere cliënt of cliëntgroep risicoscore en cliëntrisicoprofiel expliciet vastgelegd, inclusief een omschrijving van de verwachte cliëntactiviteiten en transacties (gegeven de afgenomen producten en diensten). Beleid hierover wordt vervolgens in procedures en werkprocessen nader uitgewerkt, met name hoe in voorkomende gevallen door de organisatie en haar medewerkers dient te worden gehandeld.

DNB verwacht dat u de uitkomsten van uw SIRA met betrekking tot de risico's op witwassen en terrorismefinanciering zichtbaar vertaalt naar beleid en procedures ten aanzien van uw transactiemonitoringsproces.

5.3 Het transactiemonitoringssysteem

De onderzochte MTO's hebben een geautomatiseerd transactiemonitoringssysteem, maar zij beschikken veelal niet over een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden om witwas- en terrorisme-financieringsrisico's te detecteren).

DNB verwacht dat een MTO beschikt over een (geautomatiseerd) transactiemonitoringssysteem dat passend is bij haar eigen risicoprofiel. Omdat de hoeveelheid data steeds groter wordt, gebruiken MTO's in principe een geautomatiseerd systeem voor de transactiemonitoring. Het transactiemonitoringssysteem is bij voorkeur een systeem waarin data vanuit meerdere bronnen (zoals bijvoorbeeld open bronnen en bronnen van commerciële aanbieders) wordt geïmporteerd om (patronen van) transacties te detecteren die mogelijk verband houden met witwassen of terrorismefinanciering.

De vraag of een MTO moet beschikken over een geautomatiseerd systeem voor (post-event) transactiemonitoring, is niet zonder meer met *ja* of *nee* te beantwoorden. Om te bepalen op welke wijze een MTO moet monitoren, zal een afweging gemaakt moeten worden tussen kosten, risico's en de in te zetten methode. Dat hangt sterk af van de aard en omvang van de instelling, en van het aantal transacties dat dagelijks door de instelling wordt uitgevoerd. Van belang is op te merken dat de wetgever niet eist dat transactiemonitoring geautomatiseerd moet gebeuren. De keuze voor handmatig of automatisch monitoren is dus aan de MTO, maar moet voldoende onderbouwd kunnen worden. Zo verwacht DNB dat een MTO in staat is om uit te leggen waarom een handmatig transactiemonitoringssysteem volstaat indien de MTO (tien)duizenden transacties op een dag verricht. Dat kan bijvoorbeeld als de MTO kan aantonen dat zij beschikt over voldoende geschikte resources om handmatig te monitoren.

5.3.1 Gebruik van business rules

Tijdens het onderzoek constateerde DNB dat MTO's niet goed in staat waren een onderbouwing te geven van de gebruikte business rules. Tevens bleek dat MTO's beschikten over een te beperkt aantal business rules om ongebruikelijke transacties in relatie tot witwassen of terrorismefinanciering vast te stellen. DNB constateerde voorts dat het periodieke onderhoud en het testen van de business rules bij alle onderzochte MTO's tekortschoot of zelfs geheel ontbrak.

Zoals uiteengezet in paragraaf 2.1, maakt een MTO gebruik van een set aan business rules om ongebruikelijke transacties te detecteren. Met business rules wordt bedoeld de set aan detectieregels die in het transactiemonitorings-systeem wordt toegepast, die bestaan uit de toegepaste scenario's en bepaalde grenswaarden (zoals bedragen in valuta en aantallen transacties of combinaties van bedragen en aantallen transacties). De wijze waarop deze business rules zijn bepaald, is essentieel voor de effectiviteit van het transactie-monitoringsproces van een MTO. DNB verwacht dat de in het transactiemonitoringssysteem opgenomen business rules risico gebaseerd zijn opgesteld en herleidbaar zijn tot de uitkomsten van de SIRA/integriteitsrisicoanalyse. Herleidbaar wil zeggen dat een verband bestaat tussen de business rules en de restrisico's zoals deze uit de SIRA/integriteitsrisicoanalyse volgen.

Bij het opstellen van de business rules wordt rekening gehouden met verschillende factoren, zoals:

- het soort cliënt: bijvoorbeeld een PEP, stichting
- het land waar de transactie naar toe gaat of vandaan komt (bijvoorbeeld hoogrisico land)
- het product (binnenkomende of uitgaande geldtransfer of acceptgirobetalingen)
- distributiekanalen (bijvoorbeeld fysieke aanwezigheid van de klant of online)
- het risicoprofiel van de cliënt, bijvoorbeeld laag, midden of hoog

Good practice

Een MTO die ook zakelijke klanten bedient heeft in zijn beleid opgenomen dat onder meer de sectoren 'horeca' en 'gokken' verhoogd risico zijn. Als beheersmaatregel is opgenomen dat van iedere transactie de herkomst en de bestemming van de gelden duidelijk en gedocumenteerd moeten zijn en dat Compliance de transacties goed moet keuren.

- aard en frequentie van de transacties (giraal of contant) en het doel (ondersteuning goede doelen).

De MTO zorgt voor voldoende diversificatie in de business rules al naar gelang sprake is van meerdere cliëntsegmenten, landen, producten, distributiekanalen en soorten transacties. Een voorbeeld van een business rule is: cliënten binnen een bepaalde leeftijdscategorie, 18 – 25 jaar, met bepaalde grenswaarden van omvang van girale transacties en de frequentie van transacties.

Verder wordt bij het bepalen van de business rules ook gebruik gemaakt van vergelijkingen met andere transacties van de cliënt, met informatie over transacties in eerdere perioden, in relatie tot de maturiteit van de klantrelatie (dus hoe lang de klant al klant is bij uw MTO) of leeftijdsgroep, de risicopostcode en/of risicoland.[18]

Van belang is dat een MTO documenteert op welke wijze zij tot een definitie van een business rule is gekomen, en hoe de MTO doorlopend haar business rules onderhoudt en hoe ze de rules periodiek test, bijvoorbeeld door gebruik te maken van backtesting (zie verder 5.3.6). Met backtesting wordt bedoeld het achteraf toetsen van de effectiviteit van de toegepaste business rules (en waar nodig de business rules aan te passen). Zie hiervoor ook 5.3.3.

5.3.2 Business rules in relatie tot terrorisme-financiering

DNB verwacht dat MTO's specifieke indicatoren voor terrorismefinanciering vertaald hebben in business rules en die vervolgens in hun transactie-monitoringssystemen zijn opgenomen.

DNB constateerde bij een aantal onderzochte MTO's echter dat nagenoeg geen business rules bestonden voor de detectie van terrorismefinanciering.

Good practice

Bij de uitvoering van de SIRA heeft een instelling een inherent corruptierisico geïdentificeerd dat volgt uit transacties van cliënten die geclassificeerd zijn als PEP. De instelling bepaalde dat dit risico diende te worden gemitigeerd tot een acceptabel risico. Besloten werd, gezien het risico, dat Post Transactie Monitoring hier de adequate oplossing voor kon zijn. De instelling anticipeerde hierop door binnen haar transactiemonitoringsproces specifieke business rules te implementeren voor het transactiegedrag van PEPs.[19]

Zo is tijdens de onderzoeken gebleken dat in de transactiemonitoringssystemen veelal gebruik wordt gemaakt van hoge transactielimieten, terwijl terrorismefinanciering vaak gekenmerkt wordt door transacties met lage bedragen. Aangezien uitsluitend een laag transactiebedrag niet duidt op terrorismefinanciering zouden MTO's dit moeten koppelen aan andere indicatoren van terrorismefinanciering (combinaties van verschillende indicatoren). Hierbij kan gedacht worden aan combinaties van lagere grensbedragen voor transacties met terrorisme gerelateerde landen in samenhang met bepaalde soorten cliënten, zoals stichtingen. Het detecteren van terrorisme financiering is dan ook geen statisch proces maar bij uitstek een gebied waarop de business rules voortdurend dienen te worden aangepast: de set aan business rules wijzigt continu mee met het dynamische karakter van de activiteit zelf. Daarnaast kan op basis van het risicoprofiel van een cliënt een lagere limiet worden vastgesteld: voor een voor terrorismefinanciering hoogrisico cliënt is een relatief lagere limiet in het transactiemonitoringssysteem ingesteld.

Nationaal en internationaal zijn er diverse studies verricht naar terrorismefinanciering.[20] DNB verwacht dat MTO's concrete uitkomsten van deze onderzoeken, in de vorm van red flags en indicatoren, incorporeren in hun risicoanalyse en beheersingsmaatregelen.

Tijdens de onderzoeken is gebleken dat de selectie van risicolanden die MTO's in verband brengen met terrorismefinanciering beperkt dan wel niet actueel is. Veelal is een risicolandenlijst aan de hand van de FATF-waarschuwingslijsten en de Corruption Perception Index (CPI) opgesteld, maar is geen rekening gehouden met landen die in verband kunnen worden gebracht met terrorisme en terrorismefinanciering. Zo wijzen recente publicaties op mogelijke financiering van dubieuze Nederlandse charitatieve instellingen, kerkgenootschappen en/of non-profit organisaties, vaak in de vorm van stichtingen door personen of instellingen uit bepaalde landen, zoals de Golfstaten. Niet alle MTO's hebben deze landen (i.c.m. stichtingen) in de risicolandenlijst opgenomen. DNB verwacht dat MTO's de ontwikkelingen op het gebied van terrorisme en terrorismefinanciering nauwgezet volgen, haar risicolandenlijst hierop aanpassen en dit vervolgens vertalen naar haar transactiemonitoringssysteem.

18 Een en ander uiteraard met inachtneming van de geldende privacy-bepalingen.

19 PEP staat voor *Politically Exposed Persons*: voor deze cliënten dient het verscherpt cliëntenonderzoek te worden uitgevoerd.

20 Bijvoorbeeld onderzoeken door de FATF en het rapport van AUSTRAC 'Terrorism financing in Australia 2014'.

5.3.3 Periodieke evaluatie van business rules: back testing

DNB constateerde dat MTO's hun business rules niet periodiek onderhouden noch testen op effectiviteit.

DNB verwacht dat MTO's de effectiviteit van het transactiemonitoringssysteem op het gewenste niveau krijgen en behouden. In dit verband verwacht DNB dat dit systeem periodiek wordt geëvalueerd. Doel van een dergelijke periodieke evaluatie is te beoordelen of in gebruik zijnde business rules effectief zijn. Voorbeelden van mogelijk ineffectieve rules zijn rules die te grofmazig zijn ingesteld.

Evaluatie van de rules kan plaatsvinden door middel van het zogenoemde *back testing*, ook wel de *feedback loop*. Op basis van de uitkomsten van de uitgevoerde back test brengt de MTO eventuele aanpassingen of toevoegingen aan in de business rules van haar transactiemonitoringssysteem. Een MTO kan verschillende manieren van back testing toepassen, zoals het uitvoeren van een back test waarbij business rules met veel of alleen maar *false positive* alerts worden geanalyseerd.

DNB onderscheidt vier verschillende soorten 'back tests':

1. Een test waarbij achteraf een selectie van transacties wordt geanalyseerd die binnen de toenmalige configuratie van het systeem *niet* tot een alert hebben geleid. Het doel hiervan is vast te stellen of deze transacties terecht niet tot een alert hebben geleid ('true negative') of dat bepaalde transacties toch indicatief zijn voor mogelijke ongebruikelijk gedrag ('false negative'). Indien false negatives worden waargenomen, dienen de business rules te worden uitgebreid en/of grensbedragen te worden aangepast. Op deze wijze wordt de effectiviteit van het systeem verhoogd.
2. Een analyse van transacties welke zijn opgemerkt als mogelijk ongebruikelijk via een route anders dan post transactiemonitoring. Het doel van deze vorm van backtesting is te analyseren in hoeverre het transactiemonitoringssysteem deze ongebruikelijke transactiepatronen en transacties te detecteren
3. Een test waarbij business rules met veel of alleen maar 'false positive' alerts worden geanalyseerd. Het doel van deze test is te onderzoeken hoe deze business rules, na aanpassing, verhoudingsgewijs meer 'true positives' kunnen genereren. Op deze manier wordt de efficiency van het transactiemonitoringssysteem verbeterd.
4. Een test waarbij achteraf de tijdigheid van meldingen van ongebruikelijke transacties wordt geanalyseerd met het doel om dit te verbeteren.

Het doel van deze tests is het verder optimaliseren en effectiever maken van de business rules, zodat deze meer *true positive* alerts kunnen generen. Gelijktijdig helpt het de instelling de transactiemonitoring zo efficiënt mogelijk uit te voeren.

Good practice

Voorbeelden van mogelijk ineffectieve rules zijn rules die te grofmazig zijn ingesteld. Een *good practice* laat dan bijvoorbeeld zien dat er sprake is van (te) hoge grenswaarden, waardoor nauwelijks sprake is van alerts op een bepaalde business rule; de MTO voert dan ook een periodieke beoordeling uit teneinde te beoordelen of bepaalde business rules ten onrechte geen alerts hebben gegenereerd en dat derhalve bijstelling van de bestaande rules mogelijk noodzakelijk is.

5.3.4 Transactiepatroonanalyses

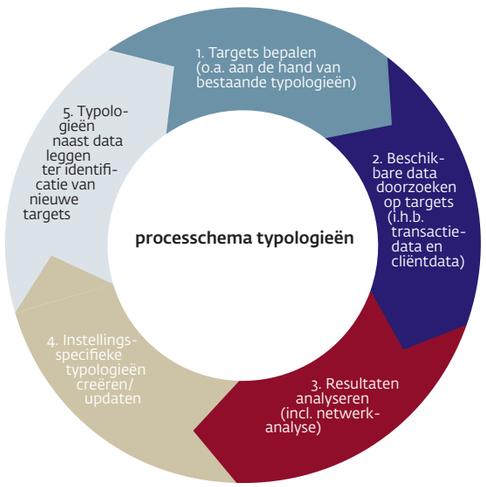
Met behulp van het transactiemonitoringssysteem kunnen MTO's transactiepatronen of netwerken en combinaties van transacties detecteren. Hieronder wordt verstaan een samenstel van transacties van een of meerdere cliënten die op geaggregeerd niveau op witwassen of terrorismefinanciering (kunnen) duiden. Van MTO's wordt verwacht dat zij gebruik maakt van netwerkanalyses om de effectiviteit van de transactiemonitoring te vergroten. De netwerkanalyses zouden de mogelijkheid kunnen bieden om (geautomatiseerd) standaard bredere transactiepatronen en -structuren en netwerken van transacties te detecteren.

5.3.5 Data-analyse in relatie tot terrorismefinanciering

Diverse (internationale) onderzoeksrapporten benadrukken dat MTO's een belangrijk kanaal zijn voor het financieren van terrorisme. Met name het feit dat ook gelden kunnen worden ontvangen in of verzonden uit risicogebieden maakt de kans dat van deze services gebruik wordt gemaakt aanzienlijk. Inzicht in (netwerken van) deze transacties is dan ook belangrijk voor het voor het detecteren van terrorismefinanciering.

Data-analyse met behulp van targets[21] en typologieën[22] speelt een centrale rol bij het bestrijden van terrorismefinanciering. MTO's beschikken over een grote hoeveelheid transactie- en cliëntdata. Van belang is om een proces in te richten waarbinnen deze data continu wordt geanalyseerd om te komen tot relaties met personen die mogelijk verband houden met terrorismefinanciering en nieuwe typologieën.

Figuur 3 Processchema typologieën



21 Targets zijn subjecten die in verband worden gebracht met (de financiering van) terrorisme.
22 (Groepen van) kenmerken die duiden op het financieren van terrorisme.

Met inachtneming van de benodigde inspanningen op dit gebied is een voorbeeld van een good practice dat een MTO de transactiedatabase direct doorzoekt op namen van personen die volgens de autoriteiten mogelijk betrokken zijn bij een terroristische aanslag.

Een ander voorbeeld van een good practice biedt het onderstaande processchema[23] afkomstig van een MTO, op grond waarvan de MTO de gedragingen van targets analyseert en daarmee nieuwe typologieën identificeert. Een dergelijke analyse kan ook voor andere MTO's nuttig zijn.

- Stap 1: Op basis van openbare informatie of bestaande typologieën is een target in beeld gekomen.
- Stap 2: De MTO doorzoekt of de target voorkomt in haar bestanden.
- Stap 3: Indien de target voorkomt in de bestanden worden de transacties geanalyseerd waarbij gekeken wordt naar bijvoorbeeld de specifieke kenmerken van de uitgevoerde transacties, betrokken landen en/of gerelateerde personen of entiteiten.
- Stap 4: Indien is vastgesteld dat deze nieuwe transactiepatronen kunnen duiden op terrorismefinanciering, worden deze patronen vertaald in nieuwe typologieën.
- Stap 5: Tot slot vertaalt de MTO de typologieën in scenario's voor haar transactiemonitoring. Met de transactiemonitoring worden vervolgens weer nieuwe targets geïdentificeerd en vangt het proces weer van voren af aan. Dit continue proces is zeer waardevol gebleken voor het detecteren van ongebruikelijke transacties.

5.3.6 IT-beheersingsmaatregelen om kwaliteit en volledigheid data te borgen

DNB heeft bij de onderzochte MTO's geconstateerd dat de kwaliteit van de data die gebruikt wordt in het transactiemonitorings-systeem niet altijd is geborgd, bijvoorbeeld doordat technische functiescheiding en omvattende volledigheidscontroles ontbraken.

DNB verwacht dat de kwaliteit en de volledigheid van de data bij het gebruik van een geautoma-tiseerd transactiemonitoringssysteem adequaat is geborgd. Belangrijke beheersmaatregelen hiervoor zijn (technische) functiescheiding en controles op de volledigheid van de data.

Voor het borgen van de kwaliteit van data is (technische) functiescheiding een wezenlijk onderdeel van de beheersing van processen in betalingsverkeer om te zorgen dat geen ongewenste en ongecontroleerde aanpassingen plaats vinden. Functiescheiding kan op meerdere manieren plaatsvinden, dat wil zeggen functie-scheiding tussen invoeren en autorisatie, maar ook technische functiescheiding tussen de testomgeving en de productieomgeving.

Om de volledigheid te waarborgen is het van belang dat alle transacties met bijbehorende data vanuit de bronsystemen worden geladen in het transactiemonitoringsysteem. Het waarborgen van de volledigheid kan op verschillende manieren en is afhankelijk van het IT landschap en de gebruikte bronsystemen. Welke transacties en bijbehorende data moeten worden gecontroleerd dient vooraf te worden bepaald, waarna controlemaatregelen worden vastgesteld zowel bij de bronsystemen als bij het transactiemonitoringsysteem. Deze maatregelen hebben betrekking op de kwaliteit (inhoudelijk) van de data en de volledigheid (kwantitatief).

Onderliggend aan genoemde maatregelen is een goede beheersing van het IT landschap voor het transactiemonitoringproces. DNB raadt daarom aan om periodiek dit IT landschap te controleren of nog wordt voldaan aan de gestelde eisen en of deze eisen nog overeenkomen met de risico's, dat wil zeggen:

- Nagaan of het IT deel van de risicoanalyse voor transactiemonitoringproces nog voldoet aan de steeds veranderende omstandigheden;
- Nagaan of de getroffen IT beheersingsmaatregelen van alle bronsystemen tot het transactiemonitoringsysteem inclusief alle interfaces en tussenliggende platformen op basis van een risicoanalyse nog effectief zijn;
- Nagaan of het proces geen single-point of failure bevat en dat kennis van het transactie-monitoringsysteem voldoende geborgd is;
- Nagaan of de documentatie, IT technisch en niet IT technisch zoals business rules, de werkelijke situatie beschrijft;
- Nagaan of de general IT controles voldoende worden beheerst.

Tijdens het onderzoek constateerde DNB dat bij het merendeel van de onderzochte MTO's een zogenoemd 'key-man exposure'-risico aanwezig was met betrekking tot het transactiemonitoringssysteem: de kennis van het systeem was bij één of twee medewerkers aanwezig. Het risico van kennisverlies is groot als weinig medewerkers kennis hebben van de systemen, wat als gevolg kan hebben dat deze systemen niet goed onderhouden kunnen worden, of dat incidenten niet opgelost kunnen worden.

23 Bron: Western Union.

5.4 Alertafhandelings- en meldproces

Zoals eerder in dit document gesteld, moeten MTO's een verrichte of voorgenomen ongebruikelijke transactie onverwijld melden aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden. Het melden van ongebruikelijke transacties aan de FIU-NL is een van de belangrijkste onderdelen van het gehele proces ter bestrijding van witwassen en terrorismefinanciering. De FIU-NL onderzoekt gemelde transacties en indien onderzoek ertoe leidt dat de gemelde transactie verdacht verklaard wordt, wordt deze transactie gemeld aan de opsporingsinstanties. Zo kunnen uw meldingen van ongebruikelijke transacties leiden tot strafrechtelijk onderzoek. De meldingsplicht van een MTO vormt daarmee een essentiële rol voor opsporing van witwassen en financiering van terrorisme.

Tijdens het onderzoek is gebleken dat de onderzochte MTO's ongebruikelijke voorgenomen transacties of uitgevoerde transacties niet altijd onverwijld en/of volledig aan de FIU-NL melden. Ook is gezien dat het ontbrak aan een gedocumenteerd intern meldproces of dat het alertafhandelingsproces niet altijd adequaat werd gedocumenteerd.

In onderstaande paragrafen leest u onze uitkomsten voor het alertafhandelingsproces en het meldproces.

5.4.1 Alertafhandelingsproces

Het alertafhandelingsproces bleek niet altijd adequaat te zijn gedocumenteerd: met name conclusies en overwegingen tot het sluiten dan wel escaleren van alerts en conclusies ontbraken.

Een MTO beschikt over procedures en werkprocessen om alerts te beoordelen en af te handelen. DNB verwacht dat een MTO voldoende inzicht heeft in de *audit trail* en doorlooptijden van vervolgacties naar aanleiding van een alert. Deze procedures en werkprocessen moeten eraan bijdragen dat de doorlooptijden vanaf het genereren van de alert tot aan de onverwijlde melding aan de FIU-NL beperkt blijven en dat de juiste prioriteiten in de afhandeling van de alerts kunnen worden gesteld.

Voorts verwacht DNB dat een MTO voor iedere alert vastlegt wat de overwegingen en conclusies zijn om een alert te sluiten of om de transactie als ongebruikelijk te melden aan de FIU-NL. Zoals eerder beschreven is het daarbij van belang te documenteren of de betreffende transactie past in het transactiegedrag van cliënt, maar ook of een dergelijke transactie logisch en plausibel is voor het soort cliënt en de sector waarin de cliënt actief is (bijvoorbeeld coupuregebruik bij contante transacties, wat in sommige sectoren gebruikelijk is). Immers, de transacties van een cliënt die alleen maar witwastransacties en/of transacties in verband met terrorismefinanciering uitvoert, zullen altijd binnen het transactiepatroon van de betreffende cliënt vallen.

DNB constateert dat escalatie van alerts naar de 2e lijn veelal ontbrak in het alertafhandelingsproces. Het is daarom van belang dat MTO's duidelijke richtlijnen bieden voor in welke gevallen escalatie vanuit de 1e lijn naar de 2e lijn (Compliance) moet plaatsvinden. DNB heeft tijdens haar onderzoek gezien dat deze handvatten bij de onderzochte MTO's veelal ontbraken.

Wellicht ten overvloede: DNB verwacht ook dat de MTO beschikt over een adequate onderbouwing van de conclusie *om juist niet* over te gaan tot melding aan FIU-NL (het vastleggen van de eigen risicoafweging om niet te melden).

DNB trof het volgende voorbeeld aan zoals het niet moet:

Bij diverse MTO's heeft DNB geconstateerd dat geen schriftelijke vastlegging plaatsvindt ten aanzien van overwegingen en conclusies die zijn gemaakt om een bepaalde transactie voort te zetten of te weigeren. In bijna alle onderzochte dossiers ontbrak informatie over de herkomst van de gelden. Alleen wanneer een cliënt aan de balie komt voor een chartale transactie van een bedrag van meer dan EUR 2.000 dan wordt deze cliënt gevraagd een formulier in te vullen waarop hij zelf aangeeft wat het doel is van de transactie. Vervolgens is het ter beoordeling aan de baliemedewerker om te beslissen of dit doel voldoende is omschreven. Er wordt niet gedocumenteerd welke overwegingen ten grondslag liggen aan het uitvoeren van een transactie, het weigeren van een transactie of het melden van een transactie aan de FIU-Nederland.

5.4.2 Capaciteit en middelen om alerts te beoordelen

DNB verwacht dat MTO's voldoende capaciteit en (financiële) middelen beschikbaar hebben om risicogebaseerd hun transactiemonitoring en in het bijzonder hun alertafhandeling te verrichten. Daarbij dient de afdeling die belast is met alertafhandeling te beschikken over realistische targets gezien de omvang en het risicoprofiel van de instelling. Om dit te bewerkstelligen kan de instelling zogenoemde kpi's opstellen waarin tijdsinschattingen voor de afhandeling van ieder type alert zijn gedefinieerd. Het spreekt voor zich dat deze ook periodiek worden geëvalueerd.

Uit het onderzoek bleek dat bij een aantal onderzochte instellingen de gemiddelde doorlooptijden van de afhandeling van alerts relatief lang waren. Van belang is dat de processen van de MTO's zodanig zijn ingericht dat risico op vertraging wordt geminimaliseerd.

5.4.3 Alerts in relatie tot risico op terrorismefinanciering

DNB verwacht dat een MTO voor het detecteren van terrorismefinanciering beschikt over een lijst met *red flags* en mogelijke business rules die kunnen duiden op terrorismefinanciering. Deze lijst dient te zijn toegespitst op het risicoprofiel van de MTO en – indien mogelijk – te worden vertaald naar business rules om risico's op terrorismefinanciering te detecteren. Tevens verwacht DNB dat u daarbij gebruik maakt van actuele guidance en nieuwsbrieven die naast DNB ook door FIU-NL worden gepubliceerd.

Good practice

Op basis van berichtgeving uit de pers signaleert een instelling dat een cliënt mogelijk banden zou hebben met jihadstrijders. Hierop heeft de instelling een alert aangemaakt. Dit is een goed voorbeeld van een instelling die de ontwikkelingen via de media nauwgezet volgt en hierop actie onderneemt door een alert op te stellen voor deze cliënt.

Good practice

Een van de onderzochte instellingen hanteert in de praktijk bij de alertafhandeling als uitgangspunt: 'kwaliteit gaat voor snelheid'. Analisten van alerts krijgen voldoende tijd voor een gedegen onderzoek en vastlegging van hun onderzoek, en hebben daarbij de beschikking over voldoende middelen en toegang tot interne en externe systemen en informatiebronnen. Onderdeel daarvan is dat de analisten bij de beoordeling van alerts het cliëntendossier moeten kunnen raadplegen.

Informatie in het cliëntendossier kan aanvullende informatie geven om een transactie met een verhoogd risico voor witwassen en terrorisme-financiering te detecteren. Met informatie uit het cliëntendossier kan de analist bijvoorbeeld beoordelen of de transacties passen bij de activiteiten van een cliënt. Een andere informatie-bron is bijvoorbeeld inzicht in de gebruikte coupures voor de opnames of stortingen.

5.4.4 Meldproces

Uit het onderzoek bleek dat MTO's niet altijd ongebruikelijke voorgenomen transacties of uitgevoerde transacties onverwijld en volledig aan de FIU-NL melden conform een gedocumenteerd meldproces.

DNB stelde vast dat MTO's niet altijd onverwijld melden als gevolg van achterstanden in de alertafhandeling en door reactieve opstelling van de alertbehandelaars. Volgens de wet moeten instellingen onverwijld melden, zodra het ongebruikelijke karakter van een transactie bekend is geworden. Naast een melding aan FIU-NL is het mogelijk dat u als MTO bij een sterk vermoeden van witwassen of financiering van terrorisme gelijktijdig aangifte doet bij de politie. Indien niet onverwijld wordt gemeld, bestaat immers het risico dat FIU-NL en de opsporingsdiensten relevante informatie mislopen. Wellicht ten overvloede kan ook, mocht sprake zijn van een incident, gemeld worden bij DNB.[24]

Het spreekt voor zich dat u als MTO ongebruikelijke voorgenomen en uitgevoerde transacties onverwijld en volledig aan de FIU-NL meldt. Daarbij is belangrijk dat u beschikt over een procedure hoe intern het meldproces er uit ziet en waaruit blijkt hoe in voorkomende gevallen gehandeld dient te worden. Belangrijk is dat eerdere en aanverwante transacties van de cliënt in het onderzoek worden betrokken en dat daarbij het risicoprofiel van de klant en het bijbehorende transactieprofiel wordt heroverwogen.

De MTO draagt zorg voor adequate (beschreven) processen om onverwijld transacties, waarbij aanleiding is om te veronderstellen dat deze verband kunnen houden met witwassen of financieren van terrorisme, aan de FIU-NL te melden. Dit betekent ook dat alle relevante informatie rondom een melding binnen de in de wet gestelde voorwaarden en uitzonderingen geheim wordt gehouden. De uitgangspunten daarvoor zijn in het beleid en procedures van de MTO vastgelegd. DNB verwacht dat de MTO erop toeziet dat beleid en procedures worden vertaald in bijvoorbeeld de juiste toegangsrechten van kernsystemen die worden gebruikt voor case management en meldingen ongebruikelijke transacties, beveiliging van informatiestromen en dat hierover guidance en training wordt verstrekt aan betrokken medewerkers. Deze guidance en training is vooral van belang voor eerstelijnmedewerkers die contact hebben met cliënten. Voor deze medewerkers is het essentieel om te weten wanneer mogelijk sprake is van ongebruikelijke transacties, welke vragen dan aan een cliënt gesteld moeten worden en welke informatie onder geen beding aan de cliënt mag worden gegeven.

24 Zie ook artikel 12 Bpr.

Good practice

Een goed voorbeeld uit de praktijk is dat een instelling voldoende guidance geeft aan haar medewerkers over het melden van ongebruikelijke transacties door iedere maand voorbeelden te bespreken en op te nemen in het reguliere opleidingsprogramma. De uitkomsten van een onderzoek weegt de MTO mee in de bestaande risicobeoordeling van de cliënt.

De MTO meldt onverwijld voorgenomen ongebruikelijke transacties aan FIU-NL

Van een voorgenomen transactie is sprake als een cliënt aangeeft een transactie te willen laten uitvoeren, maar de transactie annuleert voordat deze is uitgevoerd (omdat er bijvoorbeeld teveel vragen worden gesteld). Ook kan de MTO de transactie annuleren.

De voorgenomen (geannuleerde) transactie kan als ongebruikelijk kwalificeren, zowel op grond van de objectieve als de subjectieve indicatoren. Als bijvoorbeeld een cliënt aangeeft een geldtransactie van EUR 2.300 te willen doen, en hij annuleert deze, dan is er sprake van een voorgenomen ongebruikelijke transactie op basis van de objectieve indicator. Ook in die gevallen moet er gemeld worden aan FIU-NL.

In diverse casussen heeft DNB vastgesteld dat medewerkers van MTO's niet altijd op de hoogte waren van de verplichting tot het onverwijld melden van voorgenomen ongebruikelijke transacties. Bij het weigeren van klanten namen de medewerkers vaak onvoldoende actie om minimaal de identiteit van de klant te achterhalen, waardoor meldingen van deze voorgenomen transacties niet mogelijk was.

5.4.5 Heroverwegen risicoclassificatie cliënt

Indien de MTO transacties van een cliënt meldt aan de FIU-NL, verwacht DNB dat de instelling het bestaande risicoprofiel van de cliënt (opnieuw) bekijkt om te bepalen of er redenen bestaan om dit profiel aan te passen. Op deze wijze borgt de instelling dat het risicoprofiel van de cliënt en daarmee diens risicoclassificatie na melding van een ongebruikelijke transactie, aansluit bij de witwas- of terrorismefinancieringsrisico's van de cliënt. Ook indien de MTO van de FIU-NL een terugmelding ontvangt dat de transactie als verdacht is doorgemeld naar de opsporingsautoriteiten, beoordeelt de instelling het risicoprofiel van de cliënt en past deze indien nodig aan.

DNB gaat ervan uit dat MTO's er voor zorgen dat de analisten die de alerts beoordelen en terugmeldingen ontvangen, mogelijkheden hebben om het risicoprofiel van de cliënt zelf te herbeoordelen, of dat zij aan de medewerkers die verantwoordelijk zijn voor de klantbeoordeling aan kunnen geven dat herbeoordeling noodzakelijk is. DNB verwacht dat door middel van het quality assurance proces wordt gemonitord of dergelijke herbeoordelingen adequaat worden uitgevoerd.

De MTO heroverweegt haar risico-classificatie cliënt naar aanleiding van melding bij FIU-NL-Nederland, dan wel terugmelding van FIU-NL

Door een medewerker van een MTO wordt bij een onderzoek naar de cliënt (stichting) uit nieuwsberichten opgepikt dat deze cliënt mogelijk banden onderhoudt met Salafistische bewegingen. De cliënt verklaart desgevraagd dat deze banden inmiddels zijn doorgesneden. De MTO staat deze cliënt toe grote contante bedragen te verzenden naar een hoog-risicoland. De transacties worden door de MTO gemeld aan FIU-NL. Pas nadat de MTO een bevestiging van FIU-NL ontvangt dat de transactie als verdacht zijn doorgemeld wordt de risicoclassificatie van deze cliënt heroverwogen en wordt deze op onacceptabel geplaatst.

5.4.6 Objectieve indicatoren

Diverse MTO's hebben gezien de aard van hun werkzaamheden vaak te maken met transacties die voldoen aan één van de objectieve indicatoren voor het melden van ongebruikelijke transacties. Om er voor te zorgen dat deze onverwijld aan de FIU-NL gemeld worden zou een tool of functionaliteit binnen het transactiemonitoringssysteem ingesteld kunnen worden, waardoor transacties die aan deze objectieve indicator voldoen, automatisch worden gemeld aan de FIU-NL. Hiermee voorkomen deze instellingen dat deze transacties mogelijk niet onverwijld gemeld worden en halen ze een administratieve last weg bij degene die hiervoor verantwoordelijk is.

5.5 Governance

De governance ten aanzien van transactie-monitoring bleek met name wat betreft de rolverdeling van de lines of defense niet op orde te zijn.

Uit de onderzoeken is gebleken dat MTO's de governance omtrent transactiemonitoring op verschillende wijzen hadden ingericht. Bij meerdere MTO's ontbrak de controle door de tweede lijn ten aanzien van de door de eerste lijn uitgevoerde transactiemonitoring activiteiten. Wel hadden MTO's veelal een controleprogramma voor het cliëntenonderzoek door de tweede lijn ingericht, maar de alerts vanuit het transactiemonitorings-systeem werden niet altijd door de tweede lijn getoetst.

DNB verwacht dat de organisatie van de MTO zodanig is ingericht dat de eerste lijn een duidelijke verantwoordelijkheid heeft voor de transactie-monitoring en dat de tweede lijn (Compliance) een adviserende en controlerende taak heeft, maar daarbij ook een taak kan hebben bij het melden van ongebruikelijke transacties aan de FIU-NL. De MTO heeft binnen de tweede lijn de controlerende taak (quality assurance) voor transactiemonitoring belegd. In de praktijk heet dit *Second Line Monitoring*. In het verlengde hiervan is het van belang dat procedures en processen periodiek en op systematische wijze worden getoetst. Compliance voert als tweedelijns organisatieonderdeel structureel een monitorende rol uit en test daarnaast periodiek of maatregelen adequaat zijn of moeten worden aangepast.

Vervolgens verwacht DNB dat de derdelijnsfunctie, de onafhankelijke interne controlefunctie, met voldoende frequentie het functioneren van de eerste en tweede lijn controleert. Daarbij zorgt de organisatie ervoor dat zij voldoende capaciteit beschikbaar stelt om invulling te geven aan deze rollen en taken.

DNB verwacht dat signalen uit de eerste, tweede en derde lijn over mogelijke tekortkomingen in het transactiemonitoringsproces en de uitkomsten hiervan door het senior management worden opgepakt. Daarom is het van belang dat een MTO beschikt over adequate en periodieke management-informatie die inzicht geeft in deze signalen en uitkomsten opdat zij daarop tijdig kan sturen. Zodoende vervult Compliance naast haar adviserende en controlerende rol, tevens een rapporterende rol ten aanzien van transactiemonitoring.

Tijdens het onderzoek heeft DNB geconstateerd dat geen van alle onderzochte instellingen beschikten over een onafhankelijke interne controle functie (de derdelijnsfunctie, veelal de interne accountantsfunctie) die door middel van het uitvoeren van audits periodiek een oordeel vormt over de opzet, bestaan en werking van het transactiemonitoringssysteem en -proces.

5.6 Training en awareness

Het onderzoek liet zien dat de onderzochte MTO's niet altijd beschikten over een toegesneden trainingsprogramma en dat MTO's zich niet altijd bewust toonden van witwas- en terrorisme-financieringsrisico's.

DNB verwacht dat MTO's trainingen ten aanzien van Wwft hebben opgenomen in het (jaarlijkse) trainingsprogramma. DNB verwacht dat hierbij de inhoud van dit programma is afgestemd op competenties en ervaring van de medewerker (van bestuur en senior management tot junior medewerker) en gebruik wordt gemaakt van casuïstiek vanuit het transactiemonitoringsproces.

Begrippenlijst

Alert
Een signaal dat duidt op een mogelijk ongebruikelijke transactie.

Alert afhandelaar
De medewerker die de alert analyseert, onderzoekt en vastlegt.

Backtesting
Het testen en optimaliseren van een bepaalde aanpak op basis van gegevens uit het verleden.

Business rules
De set aan detectieregels die in het transactiemonitoringssysteem wordt toegepast, die bestaan uit de toegepaste scenario's en bepaalde grenswaarden.

Cliënt
Natuurlijke persoon of rechtspersoon met wie een zakelijke relatie wordt aangegaan of die een transactie laat uitvoeren.

Cliëntenonderzoek
Het onderzoek zoals bedoeld in artikel 3 van de Wwft.

Cliëntrisicoprofiel
Beschrijving van een cliënt in risicocategorieën; zie ook DNB Leidraad Wwft/SW, pagina 11 en 12.

Event-driven review
Op grond van gebeurtenis of incident verricht de bank een cliënten onderzoek.

Financieel Economische Criminaliteit
Witwassen, corruptie (omkoping), financiering van terrorisme, handel met voorwetenschap, niet naleven van sancties en ander crimineel gedrag (bijvoorbeeld verduistering, oplichting en valsheid in geschrifte).

Indicatoren
Aanwijzing en/of signaal, waarbij mogelijk sprake is van witwassen of financiering van terrorisme.

Meldproces
Het proces van melden bij de FIU-NL; een melding als bedoeld in artikel 16, eerste lid van de Wwft.

Peergrouping
Het definiëren van cliëntgroepen met soortgelijke kenmerken.

SIRA
Systematische integriteitsrisico analyse, zoals bedoeld in artikel 10 Bpr.

Targets
Targets zijn subjecten die in verband worden gebracht met (de financiering van) terrorisme.

Transactie
Handeling of samenstel van handelingen van of ten behoeve van een cliënt waarvan de instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen.

Transactiedata
Alle gegevens die betrekking hebben op de transactie.

Transactieprofiel
Het bepalen van het profiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een cliënt.

Typologie
(groepen van) Kenmerken die duiden op het financieren van terrorisme.

Verwacht transactiegedrag
Het verwachte patroon van de transacties van de cliënt.

Voortdurende controle
Continue bewaking, permanente controle.

Bijlage

1 SIRA / risicoprofiel	2 Opzet beleid en procedures	3 TM systeem/ business rules	4 Alert afhandeling en meldproces	5 Governance: 1e, 2e en 3e lijn	6 Training en awareness
■ SIRA niet uitgevoerd ■ Geen clientrisico profielen	■ Geen transactiemonitoring beleid en procedures	■ Geen systeem aanwezig voor transactiemonitoring dat passend is bij risicoprofiel van de instelling ■ Geen AML/CFT indicatoren en business rules om ongebruikelijke transacties te herkennen	■ Geen alert afhandelings- en meldproces gedefinieerd ■ Afhandeling transactiemonitoring alerts wordt niet vastgelegd en opgevolgd ■ (Voorgenomen) ongebruikelijke transacties worden structureel niet onverwijld gemeld aan de FIU	■ Geen functiescheiding 1e, 2e, 3e lijn ■ Verantwoordelijkheden van 1e, 2e en 3e lijn niet beschreven ■ Geen second line monitoring ■ Geen onafhankelijke interne controle ■ Periodieke managementinformatie over uitkomsten TM niet beschikbaar	■ Geen kennis en awareness ten aanzien van witwas- en/of terrorismefinancieringsrisico's en controls bij relevante medewerkers ■ Geen trainingen op het gebied van AML/CFT beschikbaar
■ Er is een SIRA uitgevoerd, echter onvoldoende diepgang in scenario's en risico's ■ Scenario's en risico's uit de SIRA zijn niet vertaald naar transactiemonitoring beleid en procedures ■ Er zijn clientsicoprofielen, echter geen ex-ante transactierisicoprofielen	■ Instelling heeft in opzet transactiemonitoring beleid en procedures, echter dit is te algemeen en onvoldoende uitgewerkt waardoor materiële onderdelen ontbreken	■ Systeem voor transactiemonitoring sluit onvoldoende aan bij het risicoprofiel van de instelling ■ Instelling hanteert een te beperkt aantal (enkele) AML/CFT indicatoren en business rules om ongebruikelijke transacties te herkennen	■ Alert afhandelings- en meldproces is capaciteit gedreven en niet risico gebaseerd ■ Afhandeling alerts wordt onvoldoende vastgelegd (geen overwegingen / conclusies) en er vindt geen opvolging plaats ■ (Voorgenomen) ongebruikelijke transacties worden incidenteel (onverwijld) gemeld aan de FIU	■ Functiescheiding 1e, 2e en 3e lijn in opzet aanwezig ■ Onvoldoende beschrijving van de verantwoordelijkheden van 1e, 2e en 3e lijn ■ In opzet is er second line monitoring (SLM) en onafhankelijke interne controle, echter in werking onvoldoende in frequentie en/of kwaliteit (SLM programma, testwerkzaamheden, rapportage) ■ Periodieke managementinformatie over uitkomsten TM in beperkte mate beschikbaar	■ Onvoldoende kennis en awareness ten aanzien van witwas en/of terrorismefinancieringsrisico's en controls bij de medewerkers ■ Incidentele trainingen op het gebied van AML/CFT (reactief bv naar aanleiding van audit bevindingen of incidenten) en/of inhoud is van onvoldoende kwaliteit (ontbreken materiële onderdelen)
■ Er is een SIRA uitgevoerd waarin voldoende diepgang zit in scenario's en risico's ■ Scenario's en risico's uit de SIRA (inclusief red flags en modus operandi witwassen / terrorismefinanciering)zijn in voldoende mate vertaald naar transactiemonitoring beleid en procedures, echter op een generiek niveau ■ Instelling heeft cliënten vertaald naar groepen van transactierisico profielen	■ Instelling heeft in opzet en bestaan transactiemonitoring beleid en procedures welke voldoende uitgewerkt zijn en waarin materiële onderdelen aanwezig zijn ■ Instelling is op basis van het raamwerk in staat om de transacties op een juiste, tijdige en volledige manier te monitoren	■ Systeem voor transactiemonitoring is voldoende passend bij risicoprofiel van de instelling ■ De instelling hanteert volledige set aan AML/CFT indicatoren en business rules (inclusief red flags en modus operandi witwassen / terrorismefinanciering) om ongebruikelijke transacties te herkennen ■ Instelling maakt gebruik van backtesting bij het periodiek evalueren van haar business rules ■ Aanpassen van systeem en business rules naar aanleiding van ontwikkelingen t.a.v. witwassen en terrorismefinanciering gebeurt reactief	■ Alert afhandelings- en meldproces is voldoende gedefinieerd, inclusief escalatie naar de 2e lijn ■ Afhandeling transactiemonitoring alerts wordt voldoende vastgelegd en opgevolgd ■ (Voorgenomen) ongebruikelijke transacties worden onverwijld gemeld aan de FIU	■ Functiescheiding 1e, 2e en 3e lijn is in opzet en bestaan aanwezig ■ Verantwoordelijkheden van 1e, 2e en 3e lijn zijn voldoende beschreven ■ In opzet en bestaan is er second line monitoring en onafhankelijke interne controle, voldoende in frequentie en kwaliteit (werking suboptimaal) ■ Bevindingen uit 2e en 3e lijns monitoring activiteiten worden adequaat opgevolgd door de 1e lijn (reactief) ■ Managementinformatie over uitkomsten toereikend, in de basis sturend	■ Voldoende kennis en awareness ten aanzien van witwas- en terrorismefinancieringsrisico's en controls bij alle medewerkers incl. senior management ■ Trainingsprogramma is ingericht op basis onderscheidende niveaus in de organisatie (van management tot medewerker) ■ Periodiek worden (verplichte) trainingen op het gebied van AML/CFT aangeboden en inhoud is van voldoende kwaliteit (bevat materiële onderdelen)
■ Scenario's en risico's in de SIRA zijn een juiste en volledige afspiegeling van het specifieke risicoprofiel van de instelling ■ SIRA wordt 'a tempo' aangepast naar aanleiding van nieuwe ontwikkelingen op het gebied van witwassen en terrorismefinanciering ■ SIRA vormt de basis voor het periodiek updaten van het transactiemonitoring raamwerk ■ Gedetailleerde ex-ante transactierisico profielen	■ Transactiemonitoring beleid en procedures zijn zichtbaar geïncorporeerd in het werkproces van de instelling en de effectieve werking ervan is aangetoond ■ Transactiemonitoring beleid en procedures zijn actueel en volledig afgestemd op de meest recente ontwikkelingen op het gebied van witwassen en terrorismefinanciering ■ Actieve samenwerking met financiële instellingen over beleid	■ Instelling heeft een geautomatiseerd en zelflerend transactiemonitoring systeem passend bij risicoprofiel van de instelling ■ Er wordt proactief ingespeeld op ontwikkelingen op het gebied van witwassen en terrorismefinanciering en daarmee aanpassngen van systeem en business rules ■ Instelling maakt gebruik van backtesting bij het toevoegen van nieuwe AML/CFT indicatoren en business rules ■ Er wordt structureel gebruik van patroonherkenning en netwerkanalyses om ongebruikelijke transacties te herkennen	■ Alert afhandelings- en meldproces is gedefinieerd en er wordt proactief ingespeeld op ontwikkelingen m.b.t. witwassen en terrorismefinanciering ■ Afhandeling transactiemonitoring alerts wordt consequent vastgelegd en opgevolgd ■ Instelling fungeert als volwaardige gesprekspartner van opsporingsautoriteiten en ketenpartners	■ Functiescheiding 1e, 2e en 3e lijn is in opzet, bestaan aanwezig en effectieve werking is aangetoond ■ Verantwoordelijkheden van 1e , 2e en 3e lijn zijn helder en volledig beschreven en 1e lijn neemt proactief eindverantwoordelijkheid voor transactiemonitoring ■ Second line monitoring wordt hoog frequent uitgevoerd en is van goede kwaliteit (effectieve werking) ■ Onafhankelijke interne controle op transactiemonitoring vindt regelmatig plaats en is van goede kwaliteit (effectieve werking) ■ Uitgebreide managementinformatie over TM uitkomsten beschikbaar, werkt sterk sturend	■ Kennis en awareness ten aanzien van witwas- en terrorisme-financieringsrisico's en controls is in hoge mate aanwezig bij alle medewerkers en senior management ■ Senior management toont een voorbeeldhouding ■ Periodiek worden (verplichte) trainingen op het gebied van AML/CFT aangeboden waarvan de inhoud is toegesneden op casuïstiek relevant voor instelling ■ Nieuwe ontwikkelingen op het gebied van witwassen en terrorisme-financiering worden direct vertaald naar de organisatie (o.a. FIU-NL casuïstiek)

Disclaimer

In deze brochure geeft De Nederlandsche Bank N.V. (DNB) haar bevindingen weer over door haar geconstateerde of verwachte gedragingen in de toezichtpraktijk, die naar haar oordeel een goede toepassing inhouden van het wettelijk kader met betrekking tot de vereisten van transactiemonitoring. Voor een betere duiding worden in de toelichting ook praktijkvoorbeelden gegeven.

Deze brochure dient altijd tezamen met de regelgeving en de DNB Leidraad Wwft en SW te worden gelezen. U kunt de good practices uit deze brochure meenemen bij uw invulling van de transactiemonitoring. Daarbij kunnen eigen omstandigheden in aanmerking worden genomen. Niet uitgesloten is dat in voorkomende gevallen een strengere toepassing van onderliggende regels geboden is.

Dit document is geen juridisch bindend document of beleidsregel van DNB als bedoeld in artikel 1:3 lid 4 Algemene Wet Bestuursrecht en heeft of beoogt geen rechtsgevolg. Dit document komt niet in de plaats van wet- en regelgeving en beleids- of toezichthouderregelingen op dit gebied. De in dit document opgenomen voorbeelden zijn niet uitputtend en zullen niet per definitie in alle gevallen als voldoende zijn aan te merken. Zij zijn een handreiking voor de uitleg en toepassing van de wettelijke verplichtingen.

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl