

Post-event transactie- monitoringsproces bij betaaldienstverleners Guidance

DeNederlandscheBank

EUROSYSTEEM

15 september 2017

© 2017 De Nederlandsche Bank N.V.

Westeinde 1, 1017 ZN Amsterdam – Postbus 98, 1000 AB Amsterdam

Telefoon 020 524 91 11 – E-mail: info@dnb.nl

Website: www.dnb.nl

Inhoud

1	Inleiding	4
1.1	Waarom deze guidance?	4
1.2	Leeswijzer	5
2	Samenvatting	6
3	Wettelijke context en reikwijdte	7
3.1	Transactiemonitoring: wettelijke verplichting tot voortdurende controle	7
3.2	Reikwijdte guidance	9
4	Transactiemonitoring	10
4.1	Het transactiemonitoringsproces	10
4.2	Volwassenheidsmodel	14
5	Guidance	18
5.1	SIRA	18
5.2	Beleid en procedures	21
5.3	Het transactiemonitoringssysteem	22
5.4	Alertafhandelings- en meldproces	30
5.5	Governance	36
5.6	Training en awareness	38
	Begrippenlijst	39

1 Inleiding

4

1.1 Waarom deze guidance?

Financieel-economische criminaliteit is een groot probleem in onze huidige maatschappij. Krantenkoppen laten zien dat de samenleving ongewild slachtoffer is geworden van deze vorm van criminaliteit, denk aan recente incidenten als de Panama Papers en terroristische aanslagen in West-Europa. Financiële instellingen, waaronder betaaldienstverleners, spelen een belangrijke rol bij het voorkomen van witwassen en terrorisme-financiering. Daartoe voeren betaaldienstverleners onder meer cliëntenonderzoek uit: door middel van zogenoemde customer due diligence (CDD) en door transacties van cliënten te monitoren met als doel ongebruikelijke transacties te identificeren. Dit laatste, de transactiemonitoring, is onderwerp van deze guidance.

Een betaaldienstverlener die adequaat monitort welke transacties in het kader van haar dienstverlening worden uitgevoerd, kan tijdig actie ondernemen als sprake is van een mogelijk ongebruikelijke transactie of van een meldenswaardig transactiepatroon. Dit dient de betaaldienstverlener dan nader te onderzoeken en eventueel melden. Gebeurt die monitoring niet of niet goed, dan kan het zijn dat een betaaldienstverlener ongewild bijdraagt aan het financieren van terrorisme of het witwassen van geld.

Deze functie als poortwachter van het Nederlandse financiële systeem vergt onder meer dat betaaldienstverleners adequaat transacties monitoren. Continu en alert. Daarom heeft de wetgever op dit gebied eisen geformuleerd waaraan een instelling moet voldoen en DNB heeft de wettelijke taak om toe te zien op naleving van de wet- en regelgeving. Transactiemonitoring is dus verplicht voor iedere betaaldienstverlener, maar deze verplichting alsook het toezicht hierop is principle-based. Dat wil zeggen dat de praktische invulling hiervan niet in detail voorgeschreven is door wet- en regelgeving of door de toezichthouder. In deze guidance vindt u handvatten voor het inrichten van een transactiemonitoringsysteem. Als betaaldienstverlener maakt u uw eigen keuzes over de precieze invulling. De toezichthouder beoordeelt het resultaat.

Het onderwerp transactiemonitoring is voor betaaldienstverleners niet nieuw. De in dit document opgenomen aandachtspunten en voorbeelden gelden als aanvulling op geldende wet- en regelgeving en eerder uitgebrachte leidraden over dit onderwerp, zoals de DNB Leidraad Wwft en SW, versie 3.0; april 2015¹; Voorkoming misbruik financiële stelsel voor witwassen en financieren van terrorisme en beheersing van integriteitsrisico en de Q&A Beroep Ongoing Due Diligence Proces (WWFT en SW) van december 2013.

¹ 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 verbeteren. Voor deze guidance heeft DNB gebruik gemaakt van de belangrijkste bevindingen van het in 2016 uitgevoerde thema-onderzoek “post-event transactiemonitoring bij betaaldienstverleners”.² Het spreekt voor zich dat u de eigen omstandigheden van uw instelling in aanmerking neemt bij de oplossingen en maatregelen die u treft. U maakt hierin uw eigen afweging.

DNB heeft op het gebied van betaaldienstverleners alleen onderzoek uitgevoerd bij vergunninghoudende betaaldienstverleners. Ook vrijgestelde betaaldienstverleners dienen op grond van de Wet ter voorkoming van witwassen en terrorismefinanciering (Wwft) hun transacties adequaat te monitoren.

Dit document biedt een overzicht van de wettelijke vereisten waaraan betaaldienstverleners dienen te voldoen en hoe DNB de invulling van transactiemonitoring, conform internationale standaarden en good practices, voor ogen heeft. DNB verwacht dat de sector hier goed kennis van neemt en daar waar nodig verbeteringen implementeert in de bedrijfsvoering. Dit document ziet op de bestaande situatie. Dit betekent dat de klanten van betaaldienstverleners veelal merchants zullen zijn.

DNB beraad zich er nog op óf en welke implicaties de PSD2 heeft, met name op de in de PSD2 genoemde nieuwe diensten waar de klanten veelal natuurlijke personen zullen betreffen.

Dit document is als volgt opgebouwd. In hoofdstuk 3 geven wij een schematische weergave van hoe een transactiemonitoringsproces eruit kan zien. Ook kunt u daar het volwassenheidsmodel vinden dat DNB hanteerde bij het onderzoek in 2016. In hoofdstuk 4 leest u per onderdeel van dit model good practices en voorbeelden hoe het niet moet. U treft tot slot een lijst aan van de belangrijkste gebruikte begrippen.

² Het thema Transactiemonitoring was een zogenaamd cross-sectoraal onderzoek, uitgevoerd in verschillende sectoren (vier banken, vier betaalinstituten, drie money transferkantoren en zes trustkantoren). Voor de overige sectoren is een vergelijkbare guidance opgesteld.

2 Samenvatting

6

Transactiemonitoring is een essentiële maatregel om onder meer mogelijk ongebruikelijke transacties te melden bij de FIU, om zo de integriteitsrisico's op het gebied van witwassen en terrorismefinanciering te beheersen. Samengevat betekent dit het volgende:

1. Betaaldienstverleners vertalen de risico's op witwassen en terrorismefinanciering die uit de SIRA voortvloeien zichtbaar naar het transactiemonitoringsproces. Bij de bepaling van het risicoprofiel van de cliënt en/of 'cliënt peergroups' betrekken betaaldienstverleners ook het verwachte transactiegedrag.
2. Betaaldienstverleners hebben voldoende beleid voor transactiemonitoring opgesteld en hebben dit beleid voldoende uitgewerkt in onderliggende procedures en werkprocessen.
3. Betaaldienstverleners beschikken over een (geautomatiseerd) transactiemonitorings-systeem en hebben een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren. Betaaldienstverleners testen deze business rules periodiek, zowel op technische aspecten als effectiviteit.
4. Betaaldienstverleners beschikken over een adequaat meld- en alertafhandelingsproces. Betaaldienstverleners zorgen ervoor dat voorgenomen en uitgevoerde ongebruikelijke transacties onverwijld en volledig aan de FIU-NL worden gemeld. In dit proces zijn per alert overwegingen en conclusies vastgelegd om te komen tot het sluiten dan wel escaleren van alerts.
5. Betaaldienstverleners hebben hun governance ten aanzien van transactiemonitoring zodanig ingericht dat sprake is van een duidelijke functiescheiding, bijvoorbeeld via het *three lines of defense model*.
6. Betaaldienstverleners beschikken over een toegesneden trainingsprogramma voor hun medewerkers. De medewerkers zijn zich bewust van witwas- en terrorismefinancieringsrisico's.

3 Wettelijke context en reikwijdte

3.1 Transactiemonitoring: wettelijke verplichting tot voortdurende controle

Betaaldienstverleners 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 brengen. Is er aanleiding om te veronderstellen dat een (voorgenomen) transactie verband houdt met witwassen of terrorismefinanciering, dan moet u als betaaldienstverlener deze transactie als ongebruikelijk melden bij de Financial Intelligence Unit – Nederland (FIU-NL).³ Om dit te kunnen doen is het van cruciaal belang dat betaaldienstverleners beschikken over een effectief transactiemonitoringsproces.⁴

Onder verwijzing naar de DNB Leidraad Wwft en SW, versie 3.0, april 2015, bevestigen wij het volgende:⁵ aangezien de Wft (integere bedrijfsvoering) en de Wwft hetzelfde doel beogen, kunnen de maatregelen die een betaaldienstverlener neemt op grond van de Wft en de Wwft worden geïntegreerd en kunt u als betaaldienstverlener op een zelfde wijze invulling geven aan de vereisten van de Wwft en Wft. Maatregelen ter bestrijding van witwassen en het financieren van terrorisme

op grond van de Wft worden gepreciseerd in de Wwft. Het hoofddoel blijft dat u weet met wie u zaken doet en waarvoor de zakelijke relatie gebruikt wordt.

Om een adequate voortdurende controle uit te oefenen, moet u als betaaldienstverlener op grond van artikel 10 Besluit prudentiële regels Wft (Bpr) allereerst zorgdragen voor een systematische integriteitsrisicoanalyse (SIRA). 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 op witwassen en financieren van terrorisme. Signaleert u naar aanleiding van deze analyse (rest)risico's, dan moet u hiervoor beleid formuleren, procedures instellen en maatregelen treffen.

Specifiek ten aanzien van de risico's met betrekking tot witwassen en terrorismefinanciering bepaalt de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) verder nog dat een betaaldienstverlener onderzoek moet doen naar zijn cliënten.⁷ Daarbij dient de betaaldienstverlener onder andere het doel en de beoogde aard van de zakelijke relatie vast te stellen. Ook moet zij een

³ Kort gezegd spreken wij hierna in dit document over "ongebruikelijke transacties".

⁴ Artikelen 2a, lid 1 en 3, lid 2 sub d Wwft.

⁵ Zie pagina's 5 en 6 van deze Leidraad.

⁶ Art. 1 Bpr.

⁷ Art. 2a, lid 1 en art. 3, lid 1 Wwft.

voortdurende controle uitoefenen op de zakelijke relatie en de tijdens de duur van deze zakelijke relatie verrichte transacties.⁸ Op deze manier kan uw instelling 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.⁹ 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 betaaldienstverlener haar zakelijke relaties indelen naar bijvoorbeeld zogenoemde 'peergroups'. Daarbij definieert de betaaldienstverlener haar eigen peergroups aan de hand van een aantal cliëntkenmerken, bijvoorbeeld sectoren, land van vestiging, rechtsvorm, landen waarin de cliënt actief is, et cetera.

Het begrip 'voortdurende controle' staat centraal in het proces van transactiemonitoring en kan door u als betaaldienstverlener op eigen wijze risicogebaseerd worden ingevuld. Risicogebaseerd wil in dit verband zeggen dat u de meeste aandacht zal besteden aan hetgeen u als grootste risico's heeft geïdentificeerd. Deze risicogebaseerde aanpak moet te allen tijde onderbouwd kunnen worden met de uitkomsten van uw integriteitsrisicoanalyse. DNB kan zich voorstellen dat het risico op witwassen bij betaaldienstverleners hoger ligt dan het risico op

terrorismedinanciering, waardoor hier meer aandacht voor zal zijn. Verwacht mag worden dat uw instelling beschikt over een transactiemonitoringssysteem 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 met zich brengen.¹⁰

Een verrichte of voorgenomen ongebruikelijke transactie moet onverwijld gemeld worden aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden.¹¹ U dient dan ook specifieke procedures en werkprocessen te hebben opgesteld om transactiealerts te beoordelen, af te handelen en ongebruikelijke transacties te melden.¹² Ter waarborging van deze procedures en maatregelen dient een betaaldienstverlener 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 leiden.¹³

8 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.

9 Art. 3, lid 2, sub d Wwft.

10 Art. 2a, lid 1 Wwft.

11 Art. 16 Wwft.

12 Art. 16 Wwft jo. artt. 17 en 18 Bpr.

13 Art. 35 Wwft.

3.2 Reikwijdte guidance

9

Deze guidance is van toepassing op:

- Zowel vrijgestelde als vergunninghoudende betaaldienstverleners.
- Elektronisch geldinstellingen indien zij betaaldiensten verlenen.
- Bijkantoren van buitenlandse betaaldienstverleners die in Nederland zijn gevestigd.

Er bestaat een diversiteit aan betaalinstellingen die met de implementatie van de PSD2 alleen maar groter wordt. Zo zijn er bijvoorbeeld issuers, acquirers, psp's, pinbetalingsverwerkers en allerlei mogelijke combinaties. Elke soort instelling heeft een andere informatiepositie ten opzichte van de merchant en de klant van de merchant. In deze guidance worden voorbeelden gegeven - zoals bijvoorbeeld red flags - die voor de ene soort instelling relevanter zijn dan voor de andere soort instelling. Het is aan u te bekijken welke informatie voor uw soort instelling relevant is.

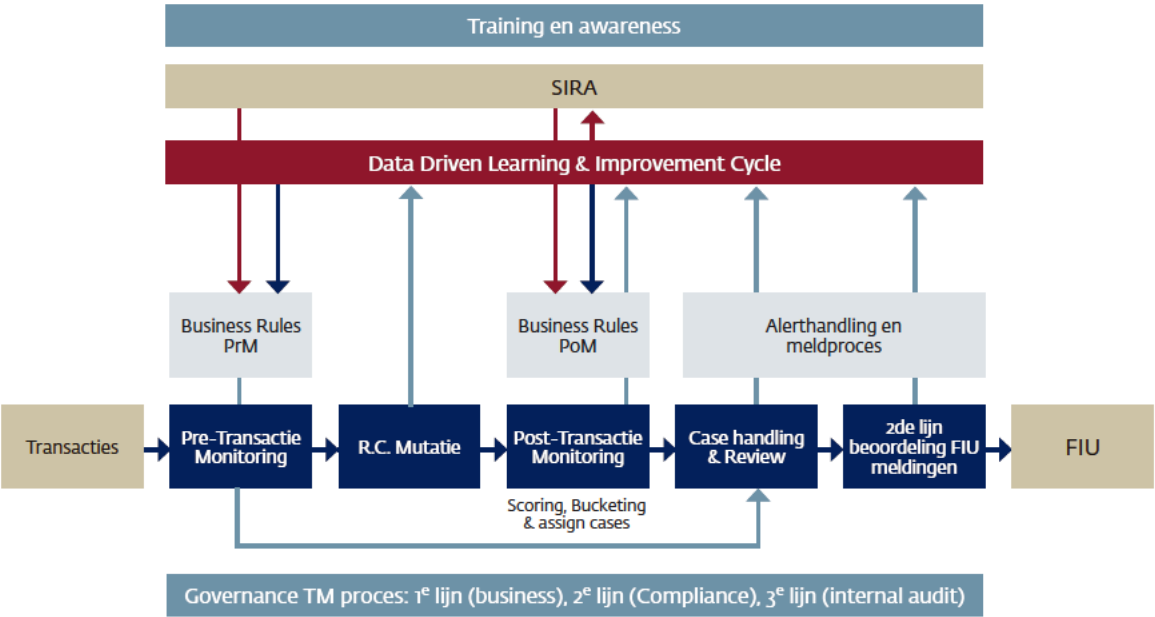
Voor banken, moneytransferkantoren en trustkantoren is een ander guidance-document opgesteld. Deze kunt u ook vinden op de website van DNB.

4 Transactiemonitoring

10 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-transactiemonitoring¹⁴ en post-event transactiemonitoring, dat wil zeggen dat transacties zowel vooraf als achteraf worden gemonitord.

Pre-transactiemonitoring

Pre-transactiemonitoring vindt plaats voordat de transactie is uitgevoerd. Pre-transactiemonitoring zal in uw sector met name gebruikt worden om (creditcard)fraude te detecteren. In andere sectoren zal pre-transactiemonitoring gebruikt worden wanneer contanten worden gewisseld, verstuurd of op rekening worden gestort. Bij post-event transactiemonitoring is de transactie reeds door de betaaldienstverlener uitgevoerd en vindt de transactiemonitoring achteraf plaats.

Post-event transactiemonitoring

Deze guidance beschrijft het post-event transactiemonitoringsproces, omdat betaaldienstverleners vooral op deze wijze, in het kader van met name de girale afwikkeling van transacties, witwas- en terrorismefinancieringsrisico's kunnen detecteren.

Het cliëntenonderzoek is onderdeel van het transactiemonitoringsproces. Door cliëntenonderzoek verkrijgt u als betaaldienstverlener kennis van de cliënt, waaronder het doel en de beoogde aard van de zakelijke relatie met de cliënt. Cliënten zullen in uw sector op dit moment veelal merchants betreffen. Met PSD2 worden nieuwe diensten geïntroduceerd, de cliënten daarvan zullen vaak ook natuurlijke personen zijn. Met de kennis van uw cliënt kunt u risicogebaseerd beoordelen 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 moet u als betaaldienstverlener afstemmen op de cliënt zelf: het soort cliënt (in welke bedrijfstak is de cliënt actief, is er sprake van Politically Exposed Persons (PEP's)), het type dienstverlening aan de cliënt (iDeal, creditcard, betaalautomaten etc.) en het risicoprofiel van de cliënt. Per cliënt en per product kan de monitoring verschillend ingericht worden.

¹⁴ Bij post-event transactiemonitoring is de transactie reeds door de instelling uitgevoerd en vindt de transactiemonitoring achteraf plaats, bij pre-transactiemonitoring is de transactie nog niet uitgevoerd.

Stap 1: risico-identificatie

De eerste stap in het transactiemonitoringsproces is risico-identificatie. Tijdens het identificatieproces analyseert u als betaaldienstverlener systematisch de witwas- en terrorismefinancieringsrisico's die uw verschillende soorten cliënten, producten en transacties met zich brengen. De uitkomsten van deze analyse legt u vast in de zogenoemde SIRA. Deze SIRA vertaalt u vervolgens naar beleid, bedrijfsprocessen en procedures omtrent transactiemonitoring. Een betaaldienstverlener kan overigens beschikken over verschillende SIRA's, denk aan een afzonderlijke SIRA voor dochtermaatschappijen, of een SIRA per business line. Het is van belang om de vertaling van de diverse SIRA-uitkomsten vast te leggen, waarbij u zowel de wijze waarop u vertaalt als de vertaling zelf, vastlegt.

Bij het identificeren en analyseren van de risico's hoort ook dat u de cliënten van uw betaaldienstverlener indeelt in risicocategorieën, bijvoorbeeld hoog, midden en laag, op grond van de witwas- en terrorismefinancieringsrisico's die de zakelijke relatie met de cliënt met zich brengt. Voor de bepaling van het risicoprofiel van een cliënt maakt u een transactieprofiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een cliënt (of cliëntgroep).¹⁵ Door (via zogenoemde 'peergrouping') een dergelijk transactieprofiel aan te maken, kunt u als betaaldienstverlener in voldoende mate monitoren

dat de transacties die tijdens de duur van de relatie verricht worden, 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. Bij het merendeel van de betaaldienstverleners zal een transactieprofiel van een merchant aan de hand van peergrouping worden opgesteld.

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

1. Actueel: het transactieprofiel is up-to-date en voorzien van een datum. Alle relevante wijzigingen worden tijdig verwerkt.
2. Volledig: alle rekeningnummers en alle relevante activiteiten (zoals door de merchant gebruikte websites) zijn opgenomen.
3. Specifiek en onderbouwd: de verwachte geldstromen zijn duidelijk beschreven, onder andere de hoogte van de verwachte bedragen (gelet op het soort merchant) en de frequentie van betalingen (de hoeveelheid bestellingen van klanten van de merchant). Opgenomen (grens) bedragen zijn goed onderbouwd en kunnen daadwerkelijk bijdragen aan het herkennen van ongebruikelijke transacties.
4. Vastgelegd: het transactieprofiel is vastgelegd in het cliëntendossier.

¹⁵ 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.

Stap 2: patronen en transacties detecteren

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. Alvorens hiervan gebruik te maken dient de betaaldienstverlener te borgen dat alle data volledig en juist wordt meegenomen in het transactiemonitoringsproces. Dit kan data betreffen over de cliënt, de diensten en de transacties. Is sprake van grotere hoeveelheden transacties, dan 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 zijn op zijn minst vooraf gedefinieerde business rules opgenomen: detectieregels in de vorm van scenario's en grensbedragen. Daarnaast kunnen ook meer geavanceerde systemen gewenst zijn, en in voorkomende gevallen noodzakelijk, afhankelijk van onder meer aard en omvang van de transacties en de aard van de betreffende instelling. Zo zal bijvoorbeeld bij een kleinere betaaldienstverlener met een beperkt aantal eenvoudige transacties, een zeer geavanceerd systeem minder noodzakelijk zijn. Het kan ook zijn dat een betaaldienstverlener het gebruik van zeer geavanceerde systemen noodzakelijk acht, bijvoorbeeld het gebruik van 'artificial intelligence'.¹⁶

De verantwoordelijkheid voor het effectief detecteren van ongebruikelijke transacties blijft hoe dan ook liggen bij u als betaaldienstverlener. U dient de werking van de systemen goed te begrijpen en kunt daarom niet enkel steunen op door externe leveranciers aangeleverde algoritmes.

Stap 3: data-analyse

Met behulp van uw transactiemonitoringssysteem en gebruik van software analyseert u uw transactiedata. Het systeem genereert op basis van business rules, zogenoemde 'alerts'. Met een alert wordt een signaal bedoeld dat duidt op een mogelijk ongebruikelijke transactie. Deze alerts worden aan onderzoek onderworpen. De bevindingen van uw onderzoek van de alerts dienen adequaat en duidelijk te worden 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. Bij twijfel of een transactie ongebruikelijk is kunt u de transactie beter wél aan de FIU-NL melden dan dat u dat níét doet. Op het moment dat een betaaldienstverlener – al dan niet opzettelijk- niet of niet tijdig voldoet aan de meldplicht, is dat een economisch delict.

¹⁶ De toepassing van kunstmatige intelligentie, waarbij aan de hand van beschikbare data en een herkennings- of cluster-algoritme de computer zelf leert om bepaalde patronen te herkennen of te ontdekken. Een algoritme is een rekenwijze voor het berekenen van bepaalde grootheden en functies.

Stap 4: beoordeling, maatregelen en vastlegging

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 en stelt u vast 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 betaaldienstverlener 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 re-construeerbaar is gedurende vijf jaar na het tijdstip van het doen van de melding.

4.2 Volwassenheidsmodel

Bij de uitvoering van het themaonderzoek (post-event) transactiemonitoring bij betaaldienstverleners gebruikte DNB een zelf ontwikkeld volwassenheidsmodel voor transactiemonitoring. Dit model houdt rekening met de relevante vereisten uit de Wft en Wwft en is bedoeld om aan te geven waar een betaaldienstverlener zich qua volwassenheid in het transactiemonitoringsproces bevindt. In dit model wordt de mate van naleving op zes gebieden toegelicht aan de hand van een vierpuntsschaal:

- Rode score: geheel non-compliant
- Oranje score: onvoldoende compliant
- Gele score: in voldoende mate compliant
- Groene score: best practice

Dit volwassenheidsmodel kunt u als betaaldienstverlener gebruiken om uw eigen ambities te bepalen, waarbij u minimaal 'geel' scoort. Het ambitieniveau van u als betaaldienstverlener is afhankelijk van het risicoprofiel van uw instelling. Een gele score betekent dat een betaaldienstverlener voldoet aan de minimale wettelijke vereisten (in voldoende mate compliant).

In het figuur op de volgende pagina ziet u het volwassenheidsmodel voor post-event transactiemonitoring nader uitgewerkt, inclusief de mogelijke scores op de zes toetsingselementen.

15

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 betaaldienstverlener erin geslaagd is om op dat gebied een gele of groene score te halen.

Figuur 2 Volwassenheidsmodel voor (post-event) transactiemonitoring

1	2	3
SIRA / risicoprofiel	Opzet beleid en procedures	TM systeem/ business rules
■ 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
■ 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
■ 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
■ 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

4	5	6
Alert afhandeling en meldproces	Governance: 1 ^e , 2 ^e en 3 ^e lijn	Training en awareness
■ 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 1^e, 2^e, 3^e lijn ■ Verantwoordelijkheden van 1^e, 2^e en 3^e 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
■ 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)
■ 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)
■ 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)

5 Guidance

18

5.1 SIRA

Betaaldienstverleners vertalen de risico's op witwassen en terrorismefinanciering die uit de SIRA voortvloeien zichtbaar naar het transactiemonitoringsproces.

Integriteitrisico's worden in de wet omschreven als "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".¹⁷ Hieronder vallen de financieel-economische criminaliteitsrisico's, witwassen, financieren van terrorisme, niet-naleving van sancties, corruptie/omkoping en belangenverstrengeling. Om te waarborgen dat uw betaaldienstverlener de integriteitrisico's adequaat beheerst, heeft de wetgever verschillende verplichtingen opgenomen waaraan uw betaaldienstverlener moet voldoen. Hierbij speelt de

SIRA¹⁸ een centrale rol. Deze risicoanalyse op organisatieniveau, waarbij zowel eerste- als tweedelijns functionarissen 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 moeten binnen uw hele organisatie leven en moeten ook terug te vinden zijn in de risicoanalyses op cliëntniveau. Hieronder vindt u een voorbeeld van een betaaldienstverlener die dat niet voldoende gedaan had.

DNB constateerde dat de meeste onderzochte betaaldienstverleners 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 instelling zaken met merchants uit een verhoogd risicoland, wat in haar SIRA wel was geïdentificeerd, maar niet was opgenomen in het transactiemonitoringsproces.

¹⁷ Op grond van artikel 10, lid 1 en 2 Bpr dient een instelling te beschikken over een systematische integriteitrisicoanalyse en indien in de analyse (rest)risico's gesignaleerd worden, dienen deze omgezet te worden in beleid, procedures en maatregelen.

¹⁸ 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>.

5.1.1 Risicoprofiel: verwacht transactiegedrag

Bij de bepaling van de CDD-risicoclassificatie (laag, midden, hoog) van de cliënt betreft de betaaldienstverlener het verwachte transactiegedrag van de cliënt.

Op grond van de Wwft moeten betaaldienstverleners bij het cliëntenonderzoek een cliënt-risicoprofiel opstellen van de cliënt. Hierbij dienen verschillende factoren van de cliënt te worden beoordeeld, zoals de sector(en) en landen waarin de cliënt actief is en de bij de betaaldienstverlener afgenomen producten en diensten. Op basis hiervan bepaalt u als betaaldienstverlener de risicoclassificatie van uw cliënt.

De review van de cliënt en actualisatie van de cliëntgegevens vindt periodiek plaats en ook tussentijds op basis van relevante gebeurtenissen. 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 uw kennis over uw cliënt kunt u bekijken of de transacties van die cliënt overeenkomen met het beeld dat uw betaaldienstverlener heeft van uw cliënt en het verwachte transactieprofiel.

Om het verwachte transactiegedrag te bepalen, kunt u als betaaldienstverlener tijdens periodieke monitoring (lees: periodieke CDD-review) van uw cliënt onder meer informatie inwinnen over:

- (verwachte) inkomende (en uitgaande) geldstromen, inclusief volumes;
- de landen waar de klanten van de cliënt zich bevinden en waar de transacties dus in grote mate vandaan zullen komen;
- soorten transacties en de mate waarin deze zullen voorkomen (creditcard, girale overboekingen, stortingen, vreemde valuta, et cetera);
- de tijdsintervallen tussen de aankoop en de uitbetaling, refunds of charge backs.

Met het verwachte transactieprofiel van een cliënt kunt u vervolgens zien of de daadwerkelijke transacties overeenkomen met dat profiel:

- komt de hoogte van de bedragen overeen met het verwachte transactiegedrag?
- komt de frequentie van de transacties overeen met het verwachte transactiegedrag?
- past het tijdstip waarop de transacties worden uitgevoerd bij het verwachte transactiegedrag?
- komt het totale volume aan transacties overeen met het verwachte transactiegedrag?

De betaaldienstverlener toetst periodiek of de cliënt nog voldoet aan het risicoprofiel dat is opgesteld bij aanvang van de dienstverlening. Betaaldienstverleners kunnen immers alleen ongebruikelijke transacties opmerken als ze een goed beeld hebben van de activiteiten van de cliënt. Indien uit specifieke transacties of het transactieverloop op de rekening blijkt dat het transactiegedrag van de cliënt afwijkt van het risicoprofiel, gaat de instelling na of mogelijk sprake is van ongebruikelijke transacties, en of verdere acties moeten worden ondernomen, zoals bijvoorbeeld een herbeoordeling van het risicoprofiel.

Daarbij is een goede samenwerking tussen verschillende personen of afdelingen essentieel.

Aangezien u het verwachte transactiegedrag opstelt bij aanvang van de zakelijke relatie met de cliënt, is de betaaldienstverlener primair afhankelijk van gegevens die de cliënt zelf verstrekt over de verwachte transacties. Bij met name start ups is dit ook door de cliënt lastig te bepalen. Bij het verwacht transactieprofiel van start ups kan gebruik worden

gemaakt van peers (bijvoorbeeld start ups van cliënten in vergelijkbare sectoren). Verwacht mag worden dat betaaldienstverleners risicogebaseerd periodiek en bij een event-gedreven review beoordelen of het verwachte transactiegedrag nog steeds in voldoende mate overeenkomt met de werkelijkheid. Deze informatie kan ter verificatie worden vergeleken met transactiegedrag van andere cliënten in vergelijkbare sectoren of cliënten met een vergelijkbaar risicoprofiel.

Good practice

Een betaaldienstverlener deelt haar merchants bij de boarding in peer groups in. Deze groepen worden gevormd aan de hand van bepaalde factoren als sectoren waarin de merchants actief zijn. In het monitoringsproces maakt de

instelling gebruik van modellen waardoor de betaaldienstverlener geautomatiseerd bekijkt of het transactiegedrag van de merchant overeen komt met het transactiegedrag van zijn peers.

Good practice (gevonden bij een bank, maar ook interessant voor grotere betaalinstellingen)

Om tot een verwacht transactiegedrag te komen heeft een bank haar cliëntportfolio aan de hand van diverse klantkenmerken opgedeeld in homogene klantgroepen, de 'peer groups'. Voor elk van deze klantgroepen is met behulp van data-analyse en op basis van meerdere relevante risico-indicatoren uit het klantprofiel een verwacht transactiepatroon vastgesteld. Wanneer deze vaststelling niet op basis van bekende klantkenmerken kan worden gedaan, doet de bank dit door middel van een analyse van historisch transactiegedrag, of door een uitvraag aan de klant. Voor iedere cliënt wordt

continue het daadwerkelijke transactiegedrag vergeleken met dit verwachte transactiepatroon. In deze vergelijking worden meerdere risico-indicatoren betrokken, bijvoorbeeld cashstortingen en internationale betalingen. Statistisch significante afwijkingen van het verwachte transactiegedrag worden automatisch gedetecteerd door het transactiemonitoringsysteem, en worden conform het reguliere afhandelingsproces onderzocht om vast te stellen of dit mogelijk een risico op financieel-economische criminaliteit betreft.

5.2 Beleid en procedures

21

Betaaldienstverleners hebben voldoende beleid voor transactiemonitoring opgesteld en dit voldoende 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 betaaldienstverlener wettelijk verplicht te beschikken over beleid, procedures en processen.

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

Good practice

Bij een betaaldienstverlener vormen het beleid en de procedures zichtbaar de basis van het werkproces. Hieruit wordt duidelijk op welke wijze de betaaldienstverlener operationeel invulling geeft aan transactiemonitoring. Daarbij kunnen

de belangrijkste uitkomsten uit de SIRA worden herleid naar haar transactiemonitoringsproces. Het volgen van de procedures wordt afgedwongen door functionaliteiten in het systeem.

5.3 Het transactiemonitoringssysteem

Betaaldienstverleners beschikken over een (geautomatiseerd) transactiemonitoringssysteem en hebben een onderbouwde en toereikende set aan business rules (detectie-regels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren.

DNB verwacht dat u als betaaldienstverlener beschikt over een transactiemonitoringssysteem dat passend is bij uw eigen risicoprofiel. Het transactiemonitoringssysteem is voor grotere instellingen bij voorkeur een systeem waarin data vanuit meerdere bronnen geïmporteerd wordt, bijvoorbeeld open bronnen en bronnen van commerciële aanbieders. Bij kleine vrijgestelde betaaldienstverleners met beperkte volumes qua transacties zal een handmatig transactiemonitoringssysteem vaak kunnen volstaan.

De vraag of een betaaldienstverlener 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 instelling moet monitoren, moet iedere betaaldienstverlener een afweging maken tussen kosten, risico's en de in te zetten methode. De manier van monitoren hangt zodoende sterk af van de aard en omvang van uw instelling, en van het aantal transacties dat dagelijks door uw 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 betaaldienstverlener, maar moet voldoende onderbouwd kunnen worden. Zo verwacht DNB dat een betaaldienstverlener in staat is om uit te leggen waarom een handmatig transactiemonitoringssysteem volstaat indien de betaaldienstverlener tienduizenden transacties op een dag verricht. Dat kan bijvoorbeeld als de betaaldienstverlener kan aantonen dat zij beschikt over voldoende geschikte resources om handmatig te monitoren.

Good practice

Een betaaldienstverlener gebruikt een geautomatiseerd zelflerend systeem waarin data vanuit meerdere bronnen (zowel open als gesloten

bronnen) wordt geïmporteerd om (patronen van) transacties te detecteren die mogelijk verband houden met witwassen en terrorismefinanciering.

5.3.1 Gebruik van red flags/scenario's

Aan de hand van de uitkomsten van de SIRA dient u als betaaldienstverlener scenario's/red flags op te stellen om (potentieel) ongebruikelijke transactiepatronen en transacties te kunnen identificeren. Deze scenario's kunt u gebruiken om business rules op te stellen. Aan de hand van onderstaande voorbeelden van indicatoren zou u deze scenario's kunnen opstellen:

- het tijdstip van de onderliggende transactie(s) (transacties zijn bijvoorbeeld verricht buiten de openingstijden van de locatie waar een pin-terminal is geplaatst);
- de tijdsintervallen tussen de aankoop en de uitbetaling, refunds of charge backs;
- de frequentie en de omvang van refunds en charge backs aan een individuele klant van de merchant;
- de verhouding tussen het initiële aankoopbedrag en het bedrag van uitbetaling, refunds of charge backs;
- het gebruik van verschillende bankrekening- of creditcardnummers voor de initiële aankoop en de uitbetaling van geld;
- de verhouding tussen spelinleg en speelwinst;
- de tijdsintervallen tussen het moment van spelinleg en de uitbetaling van de speelwinst;
- het gebruik van veel wisselende IP-adressen van de klant van de merchant;
- betalingen vanuit IP-adressen uit hoog-risicolanden;
- het meermalen gebruiken van dezelfde creditcard bij een merchant;
- veel betalingen bij een bepaalde merchant met creditcards met hetzelfde BIN-nummer afkomstig van een exotische bank;

- veranderingen in transactiegedrag die niet verklaarbaar zijn door de activiteiten van de merchant;
- bepaalde merchants die veel betalingen in bitcoins en paypal ontvangen in vergelijking met andere betaalmethoden of in vergelijking met merchants in hetzelfde segment.

Voor creditcardtransacties worden in hoofdstuk 8 van de Leidraad Wwft en SW "red flags" genoemd.

5.3.2 Gebruik van business rules

Zoals uiteengezet in paragraaf 4.1, maakt een betaaldienstverlener gebruik van een set aan business rules om ongebruikelijke transacties te detecteren. Met business rules wordt bedoeld de set aan detectieregels die in het transactiemonitoringssysteem worden 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 transactiemonitoringsproces van een betaaldienstverlener. DNB verwacht dat de in het transactiemonitoringssysteem opgenomen business rules risicogebaseerd zijn opgesteld en herleidbaar zijn tot de uitkomsten van de SIRA. Herleidbaar wil zeggen dat een verband bestaat tussen de business rules en de restrisico's die uit de SIRA volgen. De betaaldienstverlener legt dit verband vast.

Bij het opstellen van deze business rules houdt de betaaldienstverlener rekening met verschillende factoren, zoals:

- het soort cliënt; bijvoorbeeld een PEP
- het cliëntsegment; bijvoorbeeld gambling, gaming, erotiek, charitatieve stichtingen, horeca, kunsthandel, webshops met chemicaliën, webshops waar anoniem bel- en simkaarten worden verkocht, goudhandel, munten, bitcoin/crypto currency exchange, hosting services, administratiekantoren, consultancy, opleidingen, travel of crowdfunding
- het land waar de transactie naartoe gaat of vandaan komt; bijvoorbeeld hoogrisico land, EU of non-EU land
- het product; bijvoorbeeld creditcards uit hoogrisicolanden, bitcoins, prepaid cards, e-wallets of paypal
- de aard van de transactie; bijvoorbeeld customer to customer, customer to merchant, charge backs of refunds

De betaaldienstverlener zorgt voor voldoende diversificatie in de business rules, zeker als sprake is van meerdere cliëntsegmenten, landen, producten, en soorten transacties.

Van belang is dat een betaaldienstverlener documenteert op welke wijze zij tot een definitie van een business rule is gekomen, hoe zij doorlopend haar business rules onderhoudt en hoe zij de rules periodiek test, bijvoorbeeld door gebruik te maken van 'backtesting'. Met backtesting wordt bedoeld dat uw betaaldienstverlener achteraf de effectiviteit van de toegepaste business rules toetst en waar nodig de business rules aanpast; voor een verdere toelichting wordt verwezen naar 5.3.3.

Good practice

Uit de uitkomsten van de SIRA van een betaal-dienstverlener volgde dat zij verhoogde risico's liep door bitcoins te accepteren. De betaal-

dienstverlener anticipeerde hierop in haar transactiemonitoringsproces door voor bitcoins een specifieke business rule te implementeren.

5.3.3 Business rules in relatie tot terrorismefinanciering

DNB is zich ervan bewust dat terrorismefinanciering voor betaaldienstverleners lastiger is te detecteren dan bijvoorbeeld voor banken nu banken meestal over meer informatie beschikken. DNB verwacht echter wel dat betaaldienstverleners specifieke indicatoren voor terrorismefinanciering vertaald hebben in business rules en die vervolgens in hun transactiemonitoringssystemen opgenomen hebben. Alleen transactielimieten volstaan niet, aangezien uitsluitend een laag transactiebedrag uiteraard niet duidt op terrorismefinanciering. Dus zouden betaaldienstverleners business rules over transactielimieten moeten koppelen aan andere indicatoren van terrorismefinanciering, bijvoorbeeld lagere grensbedragen voor transacties met risicolanden of regio's al dan niet in samenhang met bepaalde soorten cliënten, zoals stichtingen, reisbureaus, webshops waar chemicaliën worden verkocht, crowdfunding platformen en e-currency (bitcoin)-handelaren.

Betaaldienstverleners moeten in hun monitoring alert zijn bij het faciliteren van stichtingen die gelden inzamelen ten behoeve van crisis- en conflictgebieden. Red flags bij deze stichtingen kunnen bijvoorbeeld zijn;

- Mediaberichten op de website waar religieuze boodschappen worden verkondigd.
- Nieuwsitems over de betrokkenheid vanuit de stichting of de bestuurders van de stichting bij onverdraagzame uitingen.
- Stortingen van ongewoon hoge bedragen op de stichting.
- Stortingen van veel kleine bedragen van dezelfde bron.

Tijdens de onderzoeken is gebleken dat de selectie van risicolanden die betaaldienstverleners in verband brengen met terrorismefinanciering beperkt of niet actueel is. Veelal is een risicolandenlijst opgesteld aan de hand van de FATF-waarschuwingslijsten en de Corruption Perception Index (CPI), 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 betaaldienstverleners hebben deze landen in combinatie met stichtingen in de risicolandenlijst opgenomen. DNB verwacht dat betaaldienstverleners de ontwikkelingen op het gebied van terrorisme en terrorismefinanciering nauwgezet volgen, hun risicolandenlijst hierop aanpassen en dit vervolgens vertalen naar hun transactiemonitoringssysteem.

Het detecteren van terrorismefinanciering is dan ook geen statisch proces, maar bij uitstek een gebied waarop u als betaaldienstverlener de business rules voortdurend aanpast. Daarnaast kan op basis van het risicoprofiel van een cliënt een lagere limiet worden vastgesteld, voor hoog-risicocliënten zult u bijvoorbeeld lagere limieten instellen in het transactiemonitoringssysteem.

5.3.4 Periodieke evaluatie van business rules: back testing

De business rules worden periodiek onderhouden en getest op effectiviteit.

DNB verwacht dat betaaldienstverleners de effectiviteit van het transactiemonitoringssysteem op het gewenste niveau krijgen en houden. In dit verband verwacht DNB dat u als betaaldienstverlener dit systeem periodiek evalueert om te beoordelen of gebruikte business rules effectief zijn of mogelijk ineffectief. Dat kan bijvoorbeeld wanneer uw business rules te grofmazig zijn of te hoge grenswaarden hebben, waardoor nauwelijks sprake is van alerts op een bepaalde business rule. Betaaldienstverleners voeren daarom een periodieke beoordeling uit, om te beoordelen of bepaalde business rules ten onrechte geen alerts hebben gegenereerd en dat derhalve bijstelling van de bestaande rules mogelijk noodzakelijk is.

Evaluatie van de rules kan plaatsvinden door middel van het zogenoemde 'backtesting'. Op basis van de uitkomsten van uw backtest past u eventueel de business rules van uw transactiemonitoringssysteem aan.

Backtesting kan op verschillende manieren, zoals:

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, een 'true negative' of dat bepaalde transacties toch indicatief zijn voor mogelijke ongebruikelijk gedrag, een 'false negative'. Indien false negatives worden waargenomen, breidt u de business rules uit of verhoogt u de grensbedragen.
2. Een analyse van de transacties die als mogelijk ongebruikelijk zijn opgemerkt via een andere route dan post-transactiemonitoring. Het doel van deze vorm van backtesting is te analyseren in hoeverre uw transactiemonitoringssysteem in staat is 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.
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 de business rules verder te optimaliseren en effectiever te maken, zodat deze meer true positive alerts kunnen generen. Gelijktijdig helpen dergelijke tests uw betaaldienstverlener de transactiemonitoring zo efficiënt mogelijk uit te voeren.

Good practice (gevonden bij een bank, maar ook interessant voor betaalinstellingen)

Een bank beschikt over een systeem dat periodiek de effectiviteit van alle business rules evalueert en uit een ruime set aan variabelen (100+) een overzicht creëert van de variabelen die de business rules potentieel verbeteren. In de periodieke controle is een business rule op internationale transacties omhoog gekomen met veel meer false positives op transacties binnen de Europese Unie (EU) dan op transacties buiten de EU. De bank heeft deze waarneming aangevuld met een data-

en risicoanalyse, om te na te gaan of bij potentiële aanpassingen de business rule het beoogde risico nog voldoende afdekt. Vervolgens heeft de bank een aanpassing gedaan in de business rule door de grenswaarde voor transacties binnen de EU op te hogen ten opzichte van de grenswaarde voor transacties buiten de EU. De feedback-loop heeft zo geleid tot een business rule met een hogere effectiviteit.

27

5.3.5 Data-analyse

DNB constateert dat betaaldienstverleners verschillende initiatieven nemen om te komen tot meer geavanceerde technologieën om transactiedata en cliëntdata te analyseren. Grotere betaaldienstverleners beschikken over een flinke hoeveelheid (historische) data die kan worden ingezet om het transactiegedrag van individuele cliënten, dan wel transactiepatronen en netwerken van cliënten beter te kunnen voorspellen, te analyseren en uiteindelijk ook te beoordelen. DNB moedigt betaaldienstverleners aan om geavanceerde data-analyse en artificial intelligence in te zetten bij de uitvoering van haar transactiemonitoring. Geavanceerde technologie, zoals het gebruik van 'big data' en datamodeling-technieken, vergroot namelijk de mogelijkheden van een instelling om in de beschikbare data mogelijke ongebruikelijke transactiepatronen en afwijkend transactiegedrag op te sporen.

Door meer geavanceerde technologie te gebruiken, zal een betaaldienstverlener het risico verminderen dat zij meewerkt aan het witwassen van geld of het financieren van terrorisme. De betaaldienstverlener is immers effectiever in staat om mogelijk ongebruikelijk gedrag van een cliënt te detecteren en daarop te anticiperen. DNB merkt hier wel bij op dat dit alleen geldt voor grotere instellingen omdat bij kleinere instellingen minder data beschikbaar zal zijn.

Bij de toepassing van geavanceerde technieken als machine learning en clustering, is het van belang de kwaliteit van de algoritmes te meten aan de hand van een referentie-set waarin handmatig verdachte patronen zijn geannoteerd. Dat wil zeggen dat u de patronen 'labelt', zodat bekend is welke patronen en waar in de geteste data de verborgen patronen zitten. Meting kan ook door handmatige analyse van uitgevoerde steekproeven.

Good practice

Een betaaldienstverlener beschikt over een zelflerend systeem (gebaseerd op 'artificial intelligence') waarin data vanuit meerdere bronnen geïmporteerd wordt om vervolgens real-time

geldstromen in kaart te brengen. Hierbij zijn historische transacties bepalend om het mogelijk ongebruikelijke karakter van te verwachten transacties vast te stellen.

5.3.6 Transactiepatroonanalyses

Met behulp van het transactiemonitoringssysteem kunnen betaaldienstverleners transactiepatronen of netwerken en combinaties van transacties detecteren. Hieronder wordt verstaan een samenstel van transacties van een of meerdere cliënten die op geaggregeerd niveau kunnen duiden op witwassen of terrorismefinanciering.

DNB moedigt het gebruik van voorspellende data-analyse, 'predictive analytics', aan om de effectiviteit van de transactiemonitoring te vergroten. Predictive analytics zou de mogelijkheid kunnen bieden om geautomatiseerd en standaard bredere transactiepatronen en -structuren en netwerken van transacties te detecteren.

Good practice

Een betaaldienstverlener heeft meerdere cliënten die handelen in goud. Uit de patroonanalyse valt op dat met hetzelfde IBAN nummer vlak na elkaar twee grote betalingen worden gedaan voor de aankoop van goud bij twee verschillende

handelaren. Het is opvallend dat één persoon in een korte tijdspanne bij twee verschillende handelaren aankoopt. De betaaldienstverlener meldt beide transacties als ongebruikelijk bij de FIU.

5.3.7 IT-beheersingsmaatregelen om kwaliteit en volledigheid data te borgen

Betaaldienstverleners borgen de kwaliteit en de volledigheid van de data die gebruikt wordt in het transactiemonitoringssysteem, bijvoorbeeld door technische functiescheiding en volledigheidscntroles.

DNB verwacht dat de kwaliteit en de volledigheid van de data bij het gebruik van een geautomatiseerd transactiemonitoringssysteem adequaat zijn 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 om te zorgen dat geen ongewenste en ongecontroleerde aanpassingen plaatsvinden. Functiescheiding kan op meerdere manieren plaatsvinden: functiescheiding tussen twee processen als 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 transactiemonitoringssysteem. 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 u vooraf te bepalen, waarna u controlemaatregelen moet vaststellen zowel bij de bronsystemen als bij het transactiemonitoringssysteem. 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 te controleren of dit IT-landschap nog voldoet aan de gestelde eisen en of deze eisen nog overeenkomen met de risico's:

- Voldoet het IT-deel van de risicoanalyse voor transactiemonitoringproces nog aan de steeds veranderende omstandigheden?
- Zijn de getroffen IT-beheersingsmaatregelen van alle bronsystemen tot het transactie-monitoringssysteem inclusief alle interfaces en tussenliggende platformen op basis van een risicoanalyse nog effectief?
- Bevat het proces geen single-point of failure en is kennis van het transactiemonitoringssysteem voldoende geborgd?
- Beschrijft de documentatie de werkelijke situatie, IT-technisch en niet-IT-technisch zoals business rules?
- Worden de general IT-controles voldoende beheerst?

Tijdens het onderzoek heeft DNB bij diverse onderzochte betaaldienstverleners vastgesteld dat de ontwikkelaars van business rules toegang hebben tot de productie-, de test- en acceptatie-omgeving van het transactiemonitoringssysteem. Daarmee zijn ontwikkelaars in staat om met hun rechten direct, zonder tussenkomst van de

verantwoordelijke eigenaar, de business rules voor transactiemonitoring in de productie-omgeving aan te passen. Het zonder controle doorvoeren van aanpassingen door ontwikkelaars van business rules kan alleen verhinderd worden door de interne procedures na te leven en deze periodiek te controleren.

Tijdens het onderzoek bleek dat de onderzochte betaaldienstverleners nauwelijks beschikken over een end-to-end controle tussen bronsystemen en het transactiemonitoringssysteem. Als deze end-to-end controle ontbreekt, is er geen controle op de volledigheid van de transacties uit de bronsystemen die worden ingelezen in het transactiemonitoringssysteem. Daarmee bestaat het risico dat niet alle transacties worden gemonitord. Tevens wordt hierdoor een onvolledige historie opgebouwd.

Tijdens het onderzoek constateerde DNB dat bij het merendeel van de onderzochte betaaldienstverleners een zogenoemd key-man exposure-risico aanwezig was met betrekking tot het transactiemonitoringssysteem: de kennis van het systeem was maar 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.

5.4 Alertafhandelings- en meldproces

Zoals eerder in dit document gesteld, moeten betaaldienstverleners een verrichte of voorgenomen ongebruikelijke transactie onverwijld melden aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden. Het tijdig 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 alle gemelde transacties en meldt deze, indien dit onderzoek ertoe leidt dat de gemelde transactie verdacht verklaard wordt, aan de opsporingsinstanties. Zo kunnen uw meldingen van ongebruikelijke transacties leiden tot strafrechtelijk onderzoek. De meldingsplicht van een betaaldienstverlener is daarmee essentieel voor het opsporen van witwassen en financiering van terrorisme.

In onderstaande paragrafen leest u handvatten voor het alertafhandelingsproces en het meldproces.

5.4.1 Alertafhandelingsproces

Betaaldienstverleners beschikken over een adequaat alertafhandelingsproces. In dit proces zijn per alert overwegingen en conclusies vastgelegd om te komen tot het sluiten dan wel escaleren van alerts.

Een betaaldienstverlener beschikt over procedures en werkprocessen om alerts te beoordelen en af te handelen. DNB verwacht dat een betaaldienstverlener 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 onverwijld 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 betaaldienstverlener 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 hierbij 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.

DNB constateerde bij de onderzochte betaaldienstverleners dat escalatie van alerts naar de 2e lijn veelal ontbrak in het alertafhandelingsproces. Het is daarom van belang dat betaaldienstverleners duidelijke richtlijnen bieden voor de gevallen waarin escalatie vanuit de 1e lijn naar de 2e lijn (Compliance) moet plaatsvinden.

Wellicht ten overvloede: DNB verwacht ook dat de betaaldienstverlener het adequaat kan onderbouwen als zij vanuit de risicoafweging de conclusie trekt om juist niet over te gaan tot melding aan FIU-NL.

DNB trof het volgende voorbeeld aan zoals het niet moet:

Door een onderzochte betaaldienstverlener met een aantal buitenlandse gambling-sites als klanten werden hoge gokwinsten (EUR 60.000) uitgekeerd. Op de vraag van DNB of dit niet ongebruikelijk was, werd als antwoord gegeven dat het voor deze sites heel gebruikelijk was dergelijke winsten uit te keren. De instelling kon niet zien wat de inleg van de betreffende personen was, want hiervoor gebruikte de betreffende merchant een andere betaaldienstverlener.

Het sluiten van de alert, alleen omdat het uitkeren van grote bedragen past in het transactieprofiel geldt als onvoldoende onderzoek. Betaaldienstverleners moeten zich daarnaast afvragen of zij uitkeringen willen faciliteren waarvan zij geen zicht hebben op de inleg.

5.4.2 Capaciteit en middelen om alerts te beoordelen

DNB verwacht dat betaaldienstverleners voldoende capaciteit en (financiële) middelen beschikbaar hebben om risicogebaseerd hun transactie-monitoring 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 betaaldienstverlener. Om dit te bewerkstelligen kan de betaaldienstverlener 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.

Good practice

Uit het thema-onderzoek bleek dat één van de onderzochte betaaldienstverleners in de praktijk bij de alertafhandeling het uitgangspunt hanteert "kwaliteit gaat voor snelheid."¹⁹ 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 terrorismefinanciering te detecteren. Met informatie uit het cliëntendossier kan de analist bijvoorbeeld beoordelen of de transacties passen bij de activiteiten van een cliënt.

¹⁹ Snelheid wil zeggen zo snel mogelijk afwerken van de alerts teneinde achterstanden te voorkomen.

5.4.3 Meldproces

Betaaldienstverleners beschikken over een adequaat meldproces. Betaaldienstverleners zorgen ervoor dat voorgenomen en uitgevoerde ongebruikelijke transacties onverwijld en volledig aan de FIU-NL worden gemeld.

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 betaaldienstverlener 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 moet ook, mocht sprake zijn van een incident, gemeld worden bij DNB.²⁰

Het spreekt voor zich dat u als betaaldienstverlener ongebruikelijke voorgenomen en uitgevoerde transacties onverwijld en volledig aan de

FIU-NL meldt.²¹ Daarbij is belangrijk dat u als betaaldienstverlener beschikt over een procedure hoe het meldproces er intern 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 worden heroverwogen. Wanneer een subjectieve melding wordt gedaan dient duidelijk te worden aangegeven waarom de (reeks van) transactie(s) ongebruikelijk is. Hierbij wordt u verzocht zoveel mogelijk aanvullende informatie uit het onderzoek over zowel de betaler als de begunstigde met de melding mee te geven (bijvoorbeeld ook informatie van open bronnen en transactiepatronen).

U draagt zorg voor adequate (beschreven) processen om transacties, waarbij aanleiding is om te veronderstellen dat deze verband kunnen houden met witwassen of financieren van terrorisme, onverwijld 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.

²⁰ Zie ook artikel 12, Bpr.

²¹ Alle gemelde transacties worden door FIU-NL vergeleken met relevante databestanden vanuit onder andere verschillende opsporingsinstanties. Tevens worden transacties in onderzoek genomen indien de FIU-NL wordt bevraagd door opsporingsinstanties of buitenlandse FIU's. Daarnaast onderzoekt de FIU-NL de ongebruikelijke transacties volgens een thematische benadering. Hierin worden de transacties geanalyseerd om het belang en hun relevantie te bepalen voor de inlichtingen- en opsporingsdiensten. Zodra die relevantie aanwezig is, wordt een ongebruikelijke transactie verdacht verklaard en doorgemeld. Van dit verdacht verklaren ontvangt de betaaldienstverlener - behoudens in bepaalde uitzonderingssituaties - bericht. De FIU-Nederland publiceert op haar website per meldergroep relevante informatie, waaronder casuïstiek, zie <https://www.fiu-nederland.nl/nl/wetgeving/casuïstiek>. Voor meer informatie en vragen over het melden van ongebruikelijke transacties zie www.fiu-nederland.nl of 088-6629500.

34

De uitgangspunten daarvoor zijn in het beleid en de procedures van de betaaldienstverlener vastgelegd. DNB verwacht dat de betaaldienstverlener erop toeziet dat beleid en procedures worden vertaald in bijvoorbeeld de juiste toegangsrechten van kernsystemen die worden gebruikt voor case management en meldingen van ongebruikelijke transacties, beveiliging van informatiestromen en dat hierover guidance en training wordt verstrekt aan betrokken medewerkers. Deze guidance en training zijn vooral van belang voor eerstelijnsmedewerkers 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.

Good practice

Een goed voorbeeld is dat een betaaldienstverlener voldoende guidance geeft aan haar medewerkers over het melden van ongebruikelijke transacties, door periodiek (op kwartaalbasis) voorbeelden

te bespreken en op te nemen in het reguliere opleidingsprogramma. De uitkomsten van een onderzoek weegt de betaaldienstverlener mee in de bestaande risicobeoordeling van de cliënt.

Good practice

Een betaaldienstverlener heeft een bitcoin-exchange partij als klant. Deze partij staat als hoog-risico geclassificeerd waardoor extra aandacht aan de transacties wordt geschonken. Uit de analyse valt op dat met hetzelfde IBAN-nummer

op meerdere momenten voor grote bedragen aan bitcoins worden aangekocht. Deze transacties worden door de betaaldienstverlener onverwijld aan de FIU-NL gemeld.

5.4.4 Heroverwegen risicoclassificatie cliënt

Indien de onderzoeksresultaten van de alert daar aanleiding toe geven, verwacht DNB dat de instelling het bestaande risicoprofiel van de cliënt opnieuw bekijkt om te bepalen of redenen bestaan om dit profiel aan te passen. Dit kan bijvoorbeeld door middel van een zogenoemd 'event driven review'. Op deze wijze borgt de instelling dat het risicoprofiel van de cliënt en daarmee diens risicoclassificatie aansluit bij de witwas- of terrorismefinancieringsrisico's van de cliënt. Ook indien u als betaaldienstverlener 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 betaaldienstverleners ervoor zorgen dat de analisten die de alerts beoordelen (en indien van toepassing terugmeldingen ontvangen) mogelijkheden hebben om zelf het risicoprofiel van de cliënt te herbeoordelen. Ook verwacht DNB dat deze analisten aan de medewerkers die verantwoordelijk zijn voor de klantbeoordeling aan kunnen geven dat herbeoordeling noodzakelijk is. DNB verwacht in dit verband ook dat betaaldienstverleners door middel van het quality assurance-proces monitoren of dergelijke herbeoordelingen adequaat worden uitgevoerd. Het alertafhandelingsproces kan daarnaast ook inzichten bieden in de effectiviteit van de ingestelde business rules. De eerstelijnsmedewerker kan hier een belangrijke rol spelen en input leveren voor het periodiek evalueren van de business rules.

5.4.5 Objectieve indicatoren voor automatisch melden

Diverse betaaldienstverleners 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 ervoor 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.

Bepaalde transacties, bijvoorbeeld creditcard-transacties boven de EUR 15.000,- zult u altijd aan de FIU-NL moeten melden.²² Op het moment dat een instelling – al dan niet opzettelijk- niet voldoet aan de meldplicht, is dit een economisch delict.

22 De bijlage van artikel 4 van het Uitvoeringsbesluit van de Wwft bevat de lijst met indicatoren op grond waarvan altijd gemeld moet worden.

Een onderzochte betaaldienstverlener gaf aan dat zij dermate veel creditcard transacties boven de EUR 15.000 per week faciliteert dat zij was gestopt met het melden aan de FIU-NL. Het kostte te veel tijd om steeds handmatig het formulier van de FIU-NL in te vullen. Hiervoor was geen capaciteit beschikbaar. Op de vraag waarom geen tool aanwezig was waarmee automatisch werd gemeld aan FIU-NL werd DNB meegedeeld dat voor het maken van deze tool ook geen capaciteit beschikbaar was.

5.5 Governance

Betaaldienstverleners hebben hun governance ten aanzien van transactiemonitoring zodanig ingericht dat sprake is van een duidelijke functiescheiding, bijvoorbeeld via het *three lines of defense model*.

Bij de beoordeling van dit onderdeel van het volwassenheidsmodel, is als uitgangspunt genomen het zogenoemde '*three lines of defence model*'. Hiervoor is gekozen omdat de huidige praktijk leert dat betaaldienstverleners veelal dit model toepassen in hun governance. Dit wil echter niet zeggen dat andere assurance-modellen niet zouden kunnen volstaan. Van belang is echter dat in het model te allen tijde het element van onafhankelijke controletechnische functiescheiding voldoende is geborgd. Het spreekt daarbij voor zich dat betaaldienstverleners dienen te beschikken over een onafhankelijke compliancefunctie²³ en een onafhankelijke interne controlefunctie, veelal de internal audit-functie.

Uit de onderzoeken is gebleken dat betaaldienstverleners de governance omtrent transactiemonitoring op verschillende wijzen hadden ingericht. Bij meerdere betaaldienstverleners ontbrak de controle door de tweede lijn ten aanzien van de door de eerste lijn uitgevoerde transactiemonitoring activiteiten. Veel betaaldienstverleners hadden ook geen controleprogramma voor het cliëntenonderzoek door de tweede lijn ingericht.

Tijdens het onderzoek heeft DNB verder geconstateerd dat nog niet alle onderzochte instellingen beschikten over een onafhankelijke controle functie (de derdelijnsfunctie, veelal de intern of extern belegde auditfunctie) die door middel van audits periodiek een oordeel vormt over de opzet, bestaan en werking van het transactiemonitoringssysteem en –proces. DNB verwacht dat de organisatie van de betaaldienstverlener zodanig is ingericht dat de eerste lijn een duidelijke verantwoordelijkheid heeft voor de transactiemonitoring 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.

DNB verwacht dat u duidelijk heeft aangegeven wat de adviserende taak van compliance in relatie tot transactiemonitoring inhoudt, bijvoorbeeld hoe dient te worden omgegaan met het advies van compliance ten aanzien van hoog–risico-gevallen. Ook heeft u binnen de tweede lijn de controlerende

taak (quality assurance) voor transactiemonitoring belegd. In de praktijk noemt men dit veelal 'second line monitoring'. In het verlengde hiervan is het van belang de procedures en processen periodiek en op systematische wijze te toetsen.

Compliance voert als tweedelijnsorganisatie-onderdeel 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 – zowel kwantitatief als kwalitatief – 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 u als betaaldienstverlener beschikt over adequate en periodieke managementinformatie die inzicht geeft in deze signalen en uitkomsten, opdat u daarop tijdig kunt sturen. Zodoende vervult Compliance naast haar adviserende en controlerende rol, tevens een rapporterende rol ten aanzien van transactiemonitoring. DNB verwacht in de periodieke verantwoordingsrapportage van Compliance expliciete managementinformatie over de belangrijkste uitkomsten van haar transactiemonitoring.

5.6 Training en awareness

Betaaldienstverleners beschikken over een toegesneden trainingsprogramma voor hun medewerkers. De medewerkers zijn zich bewust van witwas- en terrorismefinancieringsrisico's.

competenties en ervaring, alsmede dat gebruik wordt gemaakt van casuïstiek vanuit het eigen transactiemonitoringsproces. Bij het opstellen van de inhoud van het trainingsprogramma kan gebruik worden gemaakt van de casuïstiek van de FIU-NL: iedere twee weken publiceert de FIU-NL nieuwe casussen.

DNB constateert dat betaaldienstverleners trainingen over de Wwft hebben opgenomen in een (jaarlijks gewijzigd) trainingsprogramma. DNB verwacht dat hierbij de inhoud van dit programma is afgestemd op de medewerkers, bijvoorbeeld door een juiste adressering per doelgroep: van bestuur en senior management tot junior medewerker. Daarnaast verwacht DNB dat de training is aangepast op het niveau van de medewerkers, rekening houdend met

Good practice

Een van de onderzochte betaaldienstverleners beschikt over een trainingsprogramma voor de alertafhandelingsanalisten gebaseerd op vier verschillende ervaringsniveaus. In het trainingsprogramma waren de verwachte competenties per ervaringsniveau vastgelegd, alsmede de doelen die met training moeten worden behaald. Ook was in het trainingsprogramma vastgelegd hoe gemeten werd of deze doelen behaald waren.

Een andere onderzochte betaaldienstverlener had zowel voor de eerste, tweede als derde lijn een (jaarlijks) trainingsprogramma beschikbaar. Daarin werd aan de hand van casuïstiek uit de praktijk doorgenomen wat de nieuwste ontwikkelingen waren, zowel qua wet- en regelgeving, als praktijkvoorbeelden rondom mogelijk witwassen en financiering van terrorisme en hoe de instelling hiermee omgaat. Dat wil zeggen dat de vertaling werd gemaakt naar beleid, procedures en onderliggende werkprocessen. Daarmee werd duidelijkheid gecreëerd over hoe in voorkomende gevallen gehandeld diende te worden.

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.

40

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 gedrag van de transacties van de cliënt.

Verwacht transactiegedrag

Het verwachte patroon van de transacties van de cliënt.

Voortdurende controle

Continue bewaking, permanente controle.

Disclaimer

In deze guidance 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 deze brochure ook praktijkvoorbeelden gegeven.

Deze brochure dient altijd tezamen met de regelgeving en de DNB Leidraad Wwft en SW, versie april 2015, te worden gelezen. U kunt de good practices uit deze brochure meenemen bij uw invulling van uw 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