**CONCEPT - GUIDANCE**

**Guidance thema onderzoek post-event transactiemonitoringsproces bij betaaldienstverleners**

**30 mei 2017**

In dit document leest u de belangrijkste bevindingen van het in 2016 uitgevoerde thema-onderzoek post-event transactiemonitoring bij betaaldienstverleners.[[1]](#footnote-1) Deze bevindingen laten zien dat de onderzochte betaaldienstverleners witwas- en terrorismefinancieringsrisico’s niet voldoende beheersen omdat hun transactiemonitoringsproces nog niet op orde is. Dit document bevat de belangrijkste uitkomsten van dit onderzoek en biedt guidance om uw transactiemonitoringsproces te verbeteren. 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. Deze guidance is zowel bedoeld voor vrijgestelde als vergunninghoudende betaaldienstverleners.

**Noot: Omwille van de leesbaarheid zijn de in dit document opgenomen figuren opgenomen in een aparte bijlage**

**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 hoofbevindingen 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.

**Inhoud**

[SAMENVATTING 3](#_Toc483922725)

[1. Inleiding 4](#_Toc483922726)

[1.1 Waarom deze guidance? 4](#_Toc483922727)

[1.2 Transactiemonitoring: wettelijke verplichting tot voortdurende controle op transacties 4](#_Toc483922728)

[2. Transactiemonitoring 6](#_Toc483922729)

[2.1 Het transactiemonitoringsproces 6](#_Toc483922730)

[2.2 Volwassenheidsmodel 7](#_Toc483922731)

[3. Guidance 8](#_Toc483922732)

[3.1 SIRA 8](#_Toc483922733)

[3.1.1 Risicoprofiel: verwacht transactiegedrag 9](#_Toc483922734)

[3.2 Beleid en procedures 10](#_Toc483922735)

[3.3 Het transactiemonitoringssysteem 10](#_Toc483922736)

[3.3.1 Gebruik van red flags/scenario’s 11](#_Toc483922737)

[3.3.2 Gebruik van business rules 11](#_Toc483922738)

[3.3.3 Business rules in relatie tot terrorismefinanciering 12](#_Toc483922739)

[3.3.4 Periodieke evaluatie van business rules: back testing 13](#_Toc483922740)

[3.3.5 Data-analyse 13](#_Toc483922741)

[3.3.6 Transactiepatroonanalyses 13](#_Toc483922742)

[3.3.7 IT-beheersingsmaatregelen transactiemonitoring 14](#_Toc483922743)

[3.4 Alertafhandelings- en meldproces 14](#_Toc483922744)

[3.4.1 Alertafhandelingsproces 14](#_Toc483922745)

[3.4.2 Capaciteit en middelen om alerts te beoordelen 15](#_Toc483922746)

[3.4.3 Meldproces 15](#_Toc483922747)

[3.4.4 Heroverwegen risicoclassificatie cliënt 16](#_Toc483922748)

[3.4.5 Objectieve indicatoren 16](#_Toc483922749)

[3.5 Governance 17](#_Toc483922750)

[3.6 Training en awareness 17](#_Toc483922751)

# SAMENVATTING

Transactiemonitoring is een essentiële maatregel om integriteitrisico’s op het gebied van witwassen en terrorismefinanciering te beheersen. DNB heeft bij het in 2016 uitgevoerde thema-onderzoek naar transactiemonitoring bij betaaldienstverleners en andere instellingen geconstateerd dat de onderzochte betaaldienstverleners hun post-event transactiemonitoringsproces nog niet allemaal op orde hebben. Onze belangrijkste bevindingen zijn als volgt:

1. DNB heeft geconstateerd dat alle onderzochte betaaldienstverleners financieel economische criminaliteitsrisico’s die uit hun SIRA voortvloeien niet voldoende doorvertalen naar het transactiemonitoringsproces. DNB constateert verder dat slechts één van de onderzochte betaaldienstverleners bij de bepaling van het risicoprofiel van de cliënt het verwachte transactiegedrag van de cliënt meeneemt. Een aantal van de onderzochte betaaldienstverleners maakt in het geheel geen cliëntrisicoprofiel op.
2. Gebleken is dat niet alle onderzochte betaaldienstverleners voldoende beleid voor transactiemonitoring hebben opgesteld en dit derhalve ook niet hebben uitgewerkt in onderliggende procedures en werkprocessen.
3. Een deel van de onderzochte betaaldienstverleners kan tot effectievere monitoring komen door handmatige processen te vervangen door een geautomatiseerd transactiemonitoringsysteem.
4. De onderzochte betaaldienstverleners die beschikken over een geautomatiseerd transactiemonitoringsysteem hebben veelal geen onderbouwde en toereikende set aan business rules (detectieregels met scenario’s en grenswaarden) om witwas- en terrorismefinancieringsrisico’s te detecteren.
5. Gebleken is dat de onderzochte betaaldienstverleners voorgenomen en uitgevoerde ongebruikelijke transacties niet altijd onverwijld en volledig aan de FIU-NL melden, conform een gedocumenteerd meldproces. Het alertafhandelingsproces bleek niet altijd adequaat te zijn gedocumenteerd, met name overwegingen tot het sluiten dan wel escaleren van alerts en conclusies daaromtrent ontbraken.
6. De governance ten aanzien van transactiemonitoring bleek niet altijd op orde te zijn, met name wat betreft een duidelijke rolverdeling tussen de *three* *lines of defense*.
7. Het onderzoek liet zien dat betaaldienstverleners niet altijd beschikken over een toegesneden trainingsprogramma voor hun medewerkers en de medewerkers zich niet altijd bewust toonden van witwas- en terrorismefinancieringsrisico’s.

De uitkomsten van het thema-onderzoek laten zien dat nog niet alle betaaldienstverleners ten aanzien van transactiemonitoring op het niveau zijn dat de financieel economische criminaliteitsrisico’s adequaat worden beheerst.

In het bijgevoegde volwassenheidsmodel staan de niveaus van volwassenheid die DNB voor de sector heeft opgesteld. Vanzelfsprekend verwacht DNB dat u aan de minimale eisen voldoet. Daarnaast verwacht DNB dat u aan de hand van het volwassenheidsmodel en de in dit document opgenomen handvatten waar nodig verbeteringen doorvoert in uw bestaande transactiemonitoringsproces.

# Inleiding

## Waarom deze guidance?

Financieel economische criminaliteit is van alle dag: de krantenkoppen laten zien dat de samenleving ongewild slachtoffer kan worden van deze vorm van criminaliteit, denk aan recente incidenten als de Panama Papers en terroristische aanslagen in West-Europa. Financiële ondernemingen, waaronder betaaldienstverleners, hebben een belangrijke rol bij de bestrijding van financieel economische criminaliteit. Daartoe voeren betaaldienstverleners onder meer cliëntenonderzoek uit, door middel van zogenoemde *customer due diligence* en monitoren zij de uitgevoerde transacties van cliënten. 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 ingrijpen als sprake is van een (mogelijk) ongebruikelijke transactie of een afwijkend transactiepatroon. Gebeurt dit niet, of niet goed, dan kan het zijn dat uw instelling (ongewild) bijdraagt aan het financieren van terrorisme, of dat via uw kantoor crimineel geld witgewassen wordt. Uw functie als poortwachter van het Nederlandse financiële systeem vergt onder meer dat u adequaat transacties monitort. Continu en alert. De wetgever heeft op dit gebied eisen geformuleerd waaraan uw instelling moet voldoen. DNB heeft de wettelijke taak om toe te zien op naleving van de wet- en regelgeving in dit verband. Transactiemonitoring is verplicht voor iedere betaaldienstverlener; de praktische invulling hiervan wordt echter niet in detail voorgeschreven door wet- en regelgeving.

Het onderwerp transactiemonitoring is niet nieuw. De in dit document opgenomen aandachtspunten en voorbeelden zijn specifiek bedoeld als handvatten voor het transactiemonitoringsproces van betaaldienstverleners 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]](#footnote-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 instelling helpen met het op orde brengen van uw transactiemonitoringsproces. DNB verwacht dan ook dat u hier als sector goed kennis van neemt en daar waar nodig verbeteringen implementeert in uw bedrijfsvoering.

## Transactiemonitoring: wettelijke verplichting tot voortdurende controle op transacties

Betaaldienstverleners zijn wettelijk verplicht maatregelen te nemen om witwassen en terrorismefinanciering te voorkomen. 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 er aanleiding is om te veronderstellen dat een transactie verband houdt met witwassen of terrorismefinanciering, dan moet u als betaaldientsverlener deze als ongebruikelijke transactie melden bij de Financial Intelligence Unit – Nederland (FIU-NL).[[3]](#footnote-3) Om dit te kunnen doen is het van cruciaal belang dat betaaldienstverleners beschikken over een effectief transactiemonitoringsproces.[[4]](#footnote-4)

Om een adequate voortdurende controle uit te oefenen, dienen betaaldienstverleners op grond van artikel 10 Besluit prudentiële regels Wft (Bpr) allereerst zorg te dragen voor een systematische integrititeitrisicoanalyse (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”.[[5]](#footnote-5) Daartoe behoren dus ook de risico’s op witwassen en financieren van terrorisme. Indien naar aanleiding van de analyse (rest)risico’s gesignaleerd worden, moeten betaaldienstverleners hiervoor beleid formuleren, procedures instellen en maatregelen treffen.

Specifiek ten aanzien van de risico’s op witwassen en terrorismefinanciering bepaalt de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) dat een betaaldienstverlener ter voorkoming daarvan onderzoek moet doen naar zijn cliënten.[[6]](#footnote-6) Daarbij dient u het doel en de beoogde aard van de zakelijke relatie vast te stellen. Ook moet u een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties uitoefenen.[[7]](#footnote-7) Zo kunt u vaststellen of deze transacties overeenkomen met de kennis die u heeft van de cliënt en diens risicoprofiel.[[8]](#footnote-8)

Het begrip ”voortdurende controle” staat centraal in het proces van transactiemonitoring en kan door uw instelling op eigen wijze worden ingevuld. Verwacht mag worden dat u 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 uw instelling indicatoren en red flags opgesteld. 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 meebrengen.[[9]](#footnote-9)

Een verrichte of voorgenomen ongebruikelijke transactie moet onverwijld worden gemeld aan de FIU-NL zodra het ongebruikelijke karakter van de transactie bekend is geworden.[[10]](#footnote-10) U dient dan ook specifieke procedures en werkprocessen te hebben opgesteld om transactiealerts te beoordelen, af te handelen en ongebruikelijke transacties te melden.[[11]](#footnote-11) Ter waarborging van deze procedures en maatregelen dient een betaaldienstverlener er zorg voor 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.[[12]](#footnote-12)

DNB heeft in 2016 onderzoek uitgevoerd naar het transactiemonitoringsproces bij betaaldienstverleners. De uitkomsten van het onderzoek laten zien dat veel van de onderzochte betaaldienstverleners op een aantal belangrijke onderdelen dit proces nog niet op orde hebben. In dit document wordt uiteengezet aan welke wettelijke vereisten betaaldienstverleners 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.

Dit document is als volgt opgebouwd. In hoofdstuk 2 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 3 leest u onze belangrijkste bevindingen, good practices en voorbeelden hoe het niet moet.

# Transactiemonitoring

## Het transactiemonitoringsproces

Het transactiemonitoringproces kan er als volgt uitzien:



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. 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*

Ons themaonderzoek had specifiek betrekking op het post-event transactiemonitoringproces. Het transactiemonitoringproces is onderdeel van het cliëntenonderzoek. 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. Door het cliëntenonderzoek verkrijgt uw instelling doorlopend kennis van de cliënt, waaronder het doel en de beoogde aard van de zakelijke relatie met de cliënt. De betaaldienstverlener beoordeelt daarbij systematisch of er bij de uitgevoerde transacties van betreffende cliënt sprake is van ongebruikelijke patronen die kunnen duiden op witwassen of terrorismefinanciering. Het monitoren van de transacties van de cliënt moet worden afgestemd op de cliënt zelf: het soort cliënt (in welke bedrijfstak is de cliënt actief, is er sprake van *Politicaly 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.

* De eerste stap in het transactiemonitoringsproces is dat u als instelling systematisch de witwas- en terrorismefinancieringsrisico’s analyseert die uw verschillende soorten cliënten, producten en transacties met zich meebrengen. De uitkomsten van deze analyse legt u vast in de zogenoemde SIRA en vertaalt u vervolgens door naar uw beleid, processen en procedures omtrent transactiemonitoring. Daarbij deelt u de cliënten in risicocategorieën (bijvoorbeeld hoog, midden en laag) in, op grond van de witwas- en terrorismefinancieringsrisico's die de zakelijke relatie met de cliënt met zich meebrengt. Voor het risicoprofiel van een cliënt maakt u een transactieprofiel op basis van de *verwachte* transacties van een cliënt of het verwachte gebruik van de betaalrekening.[[13]](#footnote-13) Door een transactieprofiel aan te maken, kan uw instelling zich er in voldoende mate van verzekeren 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 mee te nemen, kunt u toetsen of de door de cliënt uitgevoerde transacties overeenkomen met de kennis die u heeft van de cliënt.
* 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. Informatie en data over de cliënt, diensten aan de cliënt en diens transacties gebruikt u in uw transactiemonitoringssysteem. 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 zijn op zijn minst vooraf gedefinieerde business rules opgenomen: detectieregels in de vorm van scenario’s en grensbedragen. Daarnaast zijn ook meer geavanceerde systemen, zoals artificial intelligence-systemen, gewenst, en in voorkomende gevallen noodzakelijk, afhankelijk van onder meer aard en omvang van transacties. Anderzijds zal bij een betaaldienstverlener met bijvoorbeeld een eenvoudig bedrijfsmodel en een beperkt aantal eenvoudige transacties, een geavanceerd systeem mogelijk minder noodzakelijk zijn.

Met behulp van uw transactiemonitoringssysteem en gebruik van intelligente software kunt u – als derde stap - deze data continu analyseren. Het systeem genereert op basis van deze *business rules* vervolgens alerts. Met een alert wordt een signaal bedoeld dat duidt op een mogelijk ongebruikelijke transactie dan wel een transactie met hoogrisico-karakter die u als instelling moet onderzoeken. De bevindingen van uw onderzoek van de alerts worden adequaat en duidelijk vastgelegd. Als 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.

U beoordeelt de gevolgen van een melding aan de FIU-NL en een eventuele terugmelding van de FIU-NL voor het risicoprofiel van de cliënt en eventuele aanvullende beheersmaatregelen. Sluitstuk van het transactiemonitoringsproces is de bewaring van gegevens die u verkrijgt in het kader van transactiemonitoring.

## Volwassenheidsmodel

Het themaonderzoek (post-event) transactiemonitoring bij betaaldienstverleners zag toe op het beoordelen van de opzet, het bestaan en de werking van hun post-event transactiemonitoringsproces. Bij de uitvoering van dit themaonderzoek hebben we gebruik gemaakt van een door DNB 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 (van non-compliance tot best practice) op zes gebieden toegelicht aan de hand van een vierpuntschaal:

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

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



Uit het onderzoek is gebleken dat er verschillen bestaan tussen de scores van de onderzochte betaaldienstverleners op alle zes toetsingselementen. In hoofdstuk 3 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.

# Guidance

## SIRA

DNB heeft geconstateerd dat geen van de onderzochte betaaldienstverleners hun financieel economische criminaliteitsrisico’s zoals die uit de SIRA voortvloeien voldoende doorvertaalt naar het transactiemonitoringsproces.

DNB verwacht dat een betaaldienstverlener borgt dat de uitkomsten van haar SIRA worden doorvertaald in haar beleid en procedures omtrent het transactiemonitoringsproces. Uw instelling heeft immers te maken met verschillende integriteitrisico’s, die afhankelijk zijn van de aard van uw dienstverlening en uw cliëntenportfolio. 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”.[[14]](#footnote-14) Belangrijke integriteitrisico’s voor betaaldienstverleners zijn financieel-economische criminaliteitsrisico’s, te weten witwassen, financieren van terrorisme, niet-naleving van sancties, corruptie/omkoping en belangenverstrengeling. Om te waarborgen dat uw instelling de integriteitrisico’s adequaat beheerst, heeft de wetgever verschillende verplichtingen opgenomen waaraan moet worden voldaan. Hierbij speelt de SIRA[[15]](#footnote-15) een centrale rol. Deze risicoanalyse op organisatieniveau legt de basis voor uw (periodiek te herzien) integriteitbeleid 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. In de subparagraaf hieronder vindt u een voorbeeld.

### Risicoprofiel: verwacht transactiegedrag

DNB constateert dat slechts één van de onderzochte betaaldienstverleners bij de bepaling van het risicoprofiel van de cliënt het verwachte transactiegedrag van de cliënt meeneemt. Een aantal van de onderzochte betaaldienstverleners maakt in het geheel geen cliëntrisicoprofiel op.

Op grond van de integriteitswetgeving moeten betaaldienstverleners bij het cliëntenonderzoek een risicoprofiel 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 betaaldienstverlener afgenomen betaalproducten 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; hierbij is de risicoclassificatie een belangrijk uitgangspunt. Deze risicoclassificatie van de cliënt gebruikt u ook voor uw transactiemonitoringsproces. Wanneer cliënten geen risicoclassificatie hebben, is het niet mogelijk het transactiemonitoringssysteem risicogebaseerd in te richten. Op basis van de kennis over de cliënt, maakt u ook het verwachte transactiegedrag inzichtelijk om te zorgen dat de tijdens de duur van de relatie verrichte transacties overeenkomen met de kennis die u heeft van uw cliënt en zijn of haar risicoprofiel.

Om het transactiegedrag te bepalen kunt u als betaaldienstverlener 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 het verwachte transactiegedrag bij aanvang van de zakelijke relatie met de cliënt wordt opgesteld, is de betaaldienstverlener primair afhankelijk van gegevens die door de cliënt over de verwachte transacties worden verstrekt. Verwacht mag worden dat betaaldienstverleners na een aantal maanden (bijvoorbeeld na een kwartaal) beoordelen of het verwachte transactiegedrag (in hoge mate) overeenkomt met de werkelijkheid. Deze informatie kan ter verificatie worden vergeleken met transactiegedrag van 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.

DNB constateerde dat de onderzochte betaaldienstverleners de uitkomsten vanuit hun SIRA niet hadden doorvertaald naar hun transactiemonitoringsproces. DNB constateerde bovendien dat indien de onderzochte betaaldienstverleners in hun SIRA onderscheid maakten tussen witwassen en terrorismefinanciering, dit niet altijd tot uitdrukking kwam in het transactiemonitoringsproces. Zo bleek dat een groot gedeelte van de onderzochte betaaldienstverleners nauwelijks aandacht hadden voor terrorismefinancieringsscenario’s.

## Beleid en procedures

|  |
| --- |
| Uit het onderzoek is gebleken dat niet alle betaaldienstverleners voldoende beleid voor transactiemonitoring hebben en dit derhalve ook niet hebben uitgewerkt in onderliggende procedures en werkprocessen. |

Voor het detecteren van (potentieel) ongebruikelijke transactiepatronen of transacties, waarbij mogelijk sprake is van witwassen of terrorismefinanciering, moet een betaaldienstverlener beschikken over beleid, procedures en processen. Dit is een wettelijk vereiste. Om te komen tot effectief beleid staat hier onder andere in dat een risicobeoordeling en risicoprofiel worden gemaakt van iedere cliënt en dat dat risicoprofiel ook een omschrijving omvat van het verwachte transactiegedrag: de instelling legt expliciet vast dat een risicoscore en cliëntrisicoprofiel wordt gemaakt van iedere cliënt, inclusief een omschrijving van de verwachte cliëntactiviteiten en transacties. Vervolgens wordt dit beleid in procedures en werkprocessen nader uitgewerkt, met name hoe de organisatie en haar medewerkers in voorkomende gevallen dienen te handelen.

DNB verwacht dat u de uitkomsten van uw SIRA zichtbaar vertaalt naar uw 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.

## Het transactiemonitoringssysteem

Niet alle onderzochte betaaldienstverleners beschikten over een geautomatiseerd transactiemonitoringssysteem. De onderzochte betaaldienstverleners die wel over een geautomatiseerd transactiemonitoringssysteem beschikken, hebben niet allen een onderbouwde en toereikende set aan business rules (detectieregels met scenario’s en grenswaarden) om witwas- en terrorismefinancieringsrisico’s te detecteren.

DNB verwacht dat een betaaldienstverlener beschikt over een (geautomatiseerd) transactiemonitoringssysteem dat passend is bij haar eigen risicoprofiel. Bij kleine vrijgestelde betaaldienstverleners met beperkte volumes qua transacties zal een handmatig transactiemonitoringsysteem 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, 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, het risicoprofiel van de cliënten 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. DNB verwacht dat een betaaldienstverlener in staat is om uit te leggen waarom een handmatig transactiemonitoringssysteem nog volstaat indien zij duizenden 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.

### 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)
* 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 instellingrekening- 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.

### Gebruik van business rules

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

Zoals uiteengezet in paragraaf 2.1, 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 instelling. 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 er een verband bestaat tussen de business rules en de restrisico’s zoals deze uit de SIRA volgen. Bij het opstellen van de business rules wordt rekening gehouden met verschillende factoren:

* het soort cliënt
bijvoorbeeld een PEP
* het cliëntsegment
bijvoorbeeld gambling, gaming, erotiek, charitatieve stichtingen, horeca, kunsthandel, 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 al naar gelang sprake is van meerdere cliëntsegmenten, landen, producten en soorten transacties.

Verder wordt bij het bepalen van de business rules ook gebruik gemaakt van vergelijkingen met andere transacties van de cliënt, bijvoorbeeld transacties over eerdere perioden, in relatie tot de maturiteit van de klantrelatie (dus hoe lang de klant al klant is bij uw instelling) Van belang is dat een instelling documenteert op welke wijze zij tot een definitie van een business rule is gekomen, en hoe de instelling doorlopend haar business rules onderhoudt en periodiek test, bijvoorbeeld door gebruik te maken van *backtesting* (zie verder 3.3.4). Met backtesting wordt bedoeld het achteraf toetsen van de effectiviteit van de toegepaste business rules (en waar nodig de business rules aanpassen).

**Good practice**

Uit de uitkomsten van de SIRA van een betaaldienstverlener volgde dat zij verhoogde risico’s liep door bitcoins te accepteren. De betaaldienstverlener anticipeerde hierop in haar transactiemonitoringsproces door voor bitcoins een specifieke business rule te implementeren.

### Business rules in relatie tot terrorismefinanciering

DNB constateerde bij een aantal onderzochte betaaldienstverleners dat er nagenoeg geen business rules in het systeem waren voor detectie van terrorismefinanciering. DNB verwacht dat betaaldienstverleners specifiek indicatoren voor terrorismefinanciering vertaald hebben in business rules die vervolgens in hun transactiemonitoringssystemen zijn opgenomen.

Tijdens de onderzoeken is 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 betaaldienstverleners 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. 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.

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 in verband worden gebracht met terrorismefinanciering beperkt dan wel 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, haar risicolandenlijst hierop aanpassen en dit vervolgens vertalen naar haar transactiemonitoringssysteem.

### Periodieke evaluatie van business rules: back testing

DNB constateerde dat niet alle betaaldienstinstellingen hun business rules periodiek onderhouden en testen op effectiviteit.

DNB verwacht dat betaaldienstverleners de effectiviteit van het transactiemonitoringssysteem op het gewenste niveau krijgen en behouden. In dit verband verwacht DNB dat het systeem periodiek wordt geëvalueerd. Doel van een dergelijke periodieke evaluatie is te beoordelen of in gebruik zijnde business rules te grofmazig zijn ingesteld, bijvoorbeeld of er sprake is van (te) hoge grenswaarden, waardoor nauwelijks sprake is van alerts op een bepaalde business rule. Deze evaluatie kan plaatsvinden door middel van het zogenoemde *back testing*. Op basis van de uitkomsten van de uitgevoerde back test brengt de betaaldienstverlener eventuele aanpassingen of toevoegingen aan in de business rules van haar transactiemonitoringssysteem. Een instelling 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. Het doel van deze test is onder meer voor de toekomst meer *true positive* alerts te generen op de business rules, door deze na de test dusdanig aan te passen dat ze het gewenste resultaat bereiken. Doel van de back test is om de effectiviteit van business rules te testen.

### Data-analyse

DNB constateert dat een aantal betaaldienstverleners initiatieven nemen om te komen tot meer geavanceerde technologieën om transactiedata en cliëntdata te analyseren. Betaaldienstverleners beschikken over een grote hoeveelheid (historische) data die kan worden ingezet om het transactiegedrag van individuele cliënten, dan wel transactiepatronen en netwerken van cliënten beter te voorspellen, te analyseren en uiteindelijk ook te beoordelen. DNB moedigt betaaldienstverleners aan geavanceerde data-analyse en *artificial intelligence*[[16]](#footnote-16) in te zetten bij de uitvoering van haar transactiemonitoring. Geavanceerde technologie (zoals gebruik van ‘big data’ en data modeling technieken) vergroot de mogelijkheden van een instelling om ongebruikelijke transactiepatronen en afwijkend transactiegedrag op te sporen.

Door het gebruik van meer geavanceerde technologie in haar transactiemonitoringsproces zal een betaaldienstverlener haar witwas- en terrorismefinancieringsrisico verminderen: de instelling is effectiever in staat om mogelijk ongebruikelijk gedrag van een cliënt te detecteren. De technologie kan zich richten op verschillende onderdelen van beschikbare data, zoals:

* Patroonanalyses, en;
* Netwerkanalyses uitvoeren om onderlinge verbanden tussen transacties te detecteren;
* Peer-group analyses; het transactiegedrag van de merchant wordt aan de hand van patroonanalyse vergeleken met het transactiegedrag van haar peers.

DNB trof het volgende voorbeeld aan als een ‘good practice’ van data-analyse.

|  |
| --- |
| **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. |

### Transactiepatroonanalyses

Met behulp van het transactiemonitoringssysteem kunnen betaaldienstverleners transactiepatronen of netwerken en combinaties van transacties detecteren. Hieronder wordt verstaan een samenstel van transacties die op geaggregeerd niveau op witwassen of terrorismefinanciering (kunnen) duiden. 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 volledig geautomatiseerd en standaard bredere transactiepatronen en -structuren en netwerken van transacties te detecteren.

### IT-beheersingsmaatregelen transactiemonitoring

DNB heeft geconstateerd dat de kwaliteit van de data die gebruikt wordt in het transactiemonitoringssysteem niet altijd is geborgd, bijvoorbeeld doordat technische functiescheiding ontbrak.

DNB verwacht dat de kwaliteit van de data bij het gebruik van het geautomatiseerde transactiemonitoringssysteem adequaat is geborgd. Daarbij 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 functiescheiding tussen invoeren en autorisatie, maar ook technische functiescheiding tussen de testomgeving en de productieomgeving.

Tijdens het onderzoek heeft DNB bij diverse betaaldienstverleners vastgesteld dat de ontwikkelaars van business rules toegang hebben tot de productie-, de test- en acceptatieomgeving 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 productieomgeving aan te passen. Het zonder controle doorvoeren van aanpassingen door ontwikkelaars van business rules kan alleen gewaarborgd worden door de interne procedures na te leven (en periodieke controle hierop). Daarnaast is een belangrijke beheersmaatregel dat de betaaldienstverlener beschikt 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 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.

## 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 melden van ongebruikelijke transacties aan de FIU-NL is een belangrijk onderdeel van de bestrijding van witwassen en terrorismefinanciering. De FIU-NL onderzoekt alle gemelde transacties. Indien dit onderzoek ertoe leidt dat de gemelde transactie verdacht verklaard wordt, wordt deze transactie doorgemeld aan de opsporingsinstanties. Zo kunnen uw meldingen van ongebruikelijke transacties leiden tot strafrechtelijk onderzoek. De meldingsplicht vormt daarmee een essentiële rol voor opsporen van witwassen en financiering van terrorisme.

De onderzochte betaaldienstverleners bleken ongebruikelijke voorgenomen transacties of uitgevoerde transacties niet altijd onverwijld en volledig aan de FIU-NL te melden conform een gedocumenteerd meldproces. Ook het alertafhandelingsproces en meldproces bleken niet altijd adequaat te zijn gedocumenteerd.

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

### Alertafhandelingsproces

Het alertafhandelingsproces bleek niet altijd adequaat te zijn gedocumenteerd: met name overwegingen om alerts en conclusies te sluiten of te escaleren ontbraken.

Een betaaldienstverlener beschikt over procedures en werkprocessen om alerts te beoordelen en af te handelen. DNB verwacht dat u beschikt over een workflow-managementsysteem dat uw instelling voldoende inzicht geeft in de *audit trail* en doorlooptijden van vervolgacties naar aanleiding van een alert. Zo zorgt u dat de doorlooptijden vanaf het genereren van de alerts tot het sturen van een (eventueel) informatieverzoek aan de cliënt 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 uw instelling 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. Bij het alert onderzoek is het van belang om niet alleen te kijken of de betreffende transactie past in het transactiegedrag van cliënt; ook is het van belang of een dergelijke transactie logisch en plausibel is voor het soort cliënt en de sector waarin de cliënt actief is.

DNB constateert verder dat procedures voor eventuele escalatie van alerts naar de 2e lijn veelal ontbraken. Van belang is dat betaaldienstverleners concrete handvatten bieden wanneer escalatie vanuit de 1e lijn naar de 2e lijn (Compliance) moet plaatsvinden. Deze handvatten ontbraken nu veelal.

Ook verwacht DNB dat uw instelling beschikt over een adequate onderbouwing van de conclusie van een alert *om juist niet* over te gaan tot melding aan FIU-NL.

DNB trof de volgende voorbeelden aan zoals het niet moet:

**Bad practice**

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.

### Capaciteit en middelen om alerts te beoordelen

DNB verwacht dat betaaldienstverleners voldoende capaciteit en 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.

**Good practice**

Uit het thema-onderzoek bleek dat één van de onderzochte betaaldienstverleners in de praktijk bij de alertafhandeling het volgende uitgangspunt hanteert “kwaliteit gaat voor snelheid[[17]](#footnote-17)”. 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.

### Meldproces

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

DNB stelde vast dat betaaldienstverleners 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. Het is denkbaar 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.

Het spreekt voor zich dat u als betaaldienstverlener ongebruikelijke voorgenomen en uitgevoerde transacties onverwijld en volledig aan de FIU-NL meldt conform een adequaat en gedocumenteerd meldproces. Belangrijk bij dit meldproces 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. 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 er zorg voor dat er adequate (beschreven) processen zijn 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 instelling vastgelegd. DNB verwacht dat de instelling erop toeziet dat beleid en procedures worden doorvertaald in bijvoorbeeld de juiste toegangsrechten van kernsystemen die worden gebruikt voor case management en meldingen, 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 er mogelijk sprake is van ongebruikelijke transacties, welke vragen dan gesteld moeten worden en welke informatie onder geen beding aan de cliënt mag worden gegeven.

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

### Heroverwegen risicoclassificatie cliënt

Indien uw instelling 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 u van de FIU-NL een terugmelding ontvangt dat de transactie als verdacht is doorgemeld naar de opsporingsautoriteiten, beoordeelt uw 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 terugmeldingen ontvangen, mogelijkheden hebben om zelf het risicoprofiel van de cliënt 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.

### Objectieve indicatoren

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 creditcardtransacties boven de EUR 15.000,- zult u altijd aan de FIU-NL moeten melden[[18]](#footnote-18). Op het moment dat een instelling – al dan niet opzettelijk- niet voldoet aan de meldplicht, is dit een economisch delict.

**Bad practice**

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.

## Governance

De governance ten aanzien van transactiemonitoring bleek met name wat betreft de rolverdeling van de 3 lines of defense niet op orde te zijn

Uit de onderzoeken is gebleken dat betaaldienstverleners de governance omtrent transactiemonitoring op verschillende wijzen hadden ingericht. Bij meerdere betaaldienstverleners ontbrak de controle door deze 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 geconstateerd dat nog niet alle onderzochte instellingen beschikten over een onafhankelijke controle functie (de derdelijnsfunctie, veelal de interne 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 een 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. Uw instelling heeft 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 tweedelijnsorganisatieonderdeel 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 internecontrolefunctie, 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 uw instelling beschikt over adequate en periodieke managementinformatie 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.

## Training en awareness

Het onderzoek liet zien dat de onderzochte betaaldienstverleners niet altijd beschikten over een toegesneden trainingsprogramma en dat betaaldienstverleners zich niet altijd bewust toonden van witwas- en terrorismefinancieringsrisico’s.

DNB constateert dat de meeste betaaldienstverleners 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 eigen transactiemonitoringsproces.

**Good practice**

Een van de onderzochte betaaldienstverleners beschikte 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 werden

* **aan de achterkant van de brochure afdrukken -**

|  |
| --- |
| **Disclaimer** In deze brochure geeft De Nederlandsche Instelling 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. |

1. Het betrof een cross-sectoraal onderzoek, uitgevoerd bij vier banken, vier betaaldienstverleners, drie money transferkantoren en zes trustkantoren. [↑](#footnote-ref-1)
2. Wwft: Wet ter voorkoming van witwassen en financieren van terrorisme; SW: Sanctiewet 1977 [↑](#footnote-ref-2)
3. Kort gezegd spreken wij hierna in dit document over “ongebruikelijke transacties” [↑](#footnote-ref-3)
4. Artikel 14, lid 4 Bpr, artikelen 2a, lid 1 en 3, lid 2 sub d Wwft. [↑](#footnote-ref-4)
5. Art. 1 Bpr [↑](#footnote-ref-5)
6. Art. 2a, lid 1 en art. 3, lid 1 Wwft. [↑](#footnote-ref-6)
7. 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 [↑](#footnote-ref-7)
8. Art. 3, lid 2, sub d Wwft. [↑](#footnote-ref-8)
9. Art. 2a, lid 1 Wwft. [↑](#footnote-ref-9)
10. Art. 16 Wwft. [↑](#footnote-ref-10)
11. Art. 16 Wwft jo. artt. 17 en 18 Bpr. [↑](#footnote-ref-11)
12. Art. 35 Wwft. [↑](#footnote-ref-12)
13. 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. [↑](#footnote-ref-13)
14. 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. [↑](#footnote-ref-14)
15. 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> [↑](#footnote-ref-15)
16. De toepassing van kunstmatige intelligentie, waarbij aan de hand van beschikbare data de computer zelf algoritmen ontwikkelt. Een algoritme is een rekenwijze voor het berekenen van bepaalde grootheden en functies. [↑](#footnote-ref-16)
17. Snelheid wil zeggen zo snel mogelijk afwerken van de alerts teneinde achterstanden te voorkomen [↑](#footnote-ref-17)
18. De bijlage van artikel 4 van het Uitvoeringsbesluit van de Wwft bevat de lijst met indicatoren op grond waarvan altijd gemeld moet worden. [↑](#footnote-ref-18)