# Inzicht verplicht?

## *De positie van banken bij detectie en aanpak van risicovolle en ongebruikelijke geldstromen*

**Drs. H.A. Lesscher, mr. B. Peters en J. van Leeuwen MSc**

### 1. Inleiding

Uit praktijkonderzoek wordt steeds duidelijker dat in kwetsbare wijken met een cumulatie van problemen een voedingsbodem aanwezig is voor criminele activiteiten. Voor een deel bestaan die criminele activiteiten uit 'zichtbare' aangiftecriminaliteit, waar doorgaans door betrokkenen aangifte van wordt gedaan, voor een ander deel uit minder zichtbare georganiseerde vormen van criminaliteit, zoals hennepteelt, fraude, productie van synthetische drugs, arbeidsuitbuiting en witwassen. Er lijkt hierbij sprake te zijn van een soort 'normvervaging' dan wel een alternatief normstelsel bij bewoners die niet actief aan criminaliteit deelnemen, maar er in het grijze gebied tussen legaal en illegaal van profiteren om in voorkomende gevallen 'de andere kant op te kijken'. Hierdoor ontstaat een samenleving waarin criminaliteit en crimineel geld als 'normaal' worden beschouwd.[1]

Ook in verschillende bedrijfssectoren, zoals de haven- en de transportsector, is hier sprake van. De gevolgen hiervan zijn dat er gelegenheid wordt geschept voor het plegen en afschermen van criminele activiteiten en de innesteling hiervan in de bovenwereld, doordat bedrijven en personen zich opstellen als facilitators.

Daarnaast biedt de georganiseerde criminaliteit een 'alternatieve kansenstructuur'. De rijkdom en status die met georganiseerde vormen van criminaliteit gepaard gaan (zoals bijvoorbeeld de handel in drugs) vertalen zich vaak in patsergedrag: het bezit van grote hoeveelheden contant geld en de aanschaf van dure voertuigen, sieraden of kleding. Doordat jongeren zo zien dat criminaliteit blijkbaar loont, hebben deze vormen van criminaliteit een aanzuigende werking op hen.

1 Tops , P. & Tromp J., (2016) *De achterkant van Nederland, hoe onder- en bovenwereld verstrengeld raken*, Balans Uitgeverij.

In dit artikel gaan we aan de hand van een aantal concrete en geanonimiseerde verdachte transacties nader in op de inzichten die zijn ontstaan met betrekking tot de positie van financiële instellingen, in het bijzonder van banken (gegeven de casuïstiek).

## 2. Anders kijken

Op Rotterdam-Zuid zijn bovenstaande negatieve effecten van de georganiseerde en criminaliteit duidelijk waarneembaar en hebben een scala aan problemen als gevolg. Dit heeft er toe geleid dat de gemeente samen met haar veiligheidspartners, zoals OM, politie, en Belastingdienst, samenwerkend binnen het Regionaal Informatie- en Expertise Centrum (RIEC), een meerjarig programma is gestart dat gericht is op het terugdringen en aanpakken van ondermijnende en georganiseerde criminaliteit. Het doel hiervan is het verbeteren van de veiligheid, leefbaarheid en maatschappelijke integriteit op Rotterdam-Zuid.

Een van de uitdagingen waar de samenwerkende overheidspartners bij de aanpak op Zuid voor staan is het onzichtbare zichtbaar maken. Ondermijnende vormen van criminaliteit zijn per definitie slecht of nauwelijks zichtbaar omdat criminelen erbij gebaat zijn en investeren in het verhullen en verbergen van hun activiteiten en opbrengsten. Naast onderzoek naar de criminele activiteiten is onderzoek naar de achterliggende structuren en financiële opbrengsten en stromen die daarbij horen of er het gevolg van zijn eveneens van belang. Dat maakt een succesvolle aanpak en daarmee blijvende maatschappelijke effecten ook complex. Voor de overheidspartners op Zuid lag er dus een uitdaging: meer informatie ontsluiten en benutten.

Bij het volledig tot stand brengen en organiseren van een crimineel bedrijfsproces leunen criminelen netwerken zoals gezegd mede op de lokale mogelijkheden. Denk hierbij aan de opslag, transport, ontmoetingsruimten en het verkrijgen van apparatuur ten behoeve van bijvoorbeeld drugshandel- en productie, maar ook aan juridische en financiële ondersteuning. Dit zorgt voor lokale en sociale inbedding van criminelen en hun activiteiten in de legale economie. Het is hierom, dat vrije beroepsuitoefenaars, zoals notarissen, makelaars, accountants, maar ook financiële instellingen zoals banken, verzekeraars, beleggingsinstellingen en trustkantoren een poortwachtersfunctie vervullen bij het vroegtijdig signaleren van witwassignalen en belangrijke actoren zijn in de strijd tegen de georganiseerde criminaliteit.[2] Zo zijn voor dit proces bankrekeningen en vergunningen nodig, moeten er transacties uitgevoerd worden en moet crimineel geld geïnvesteerd worden in bijvoorbeeld onroerend goed. Deze poortwachtersfunctie komt onder andere tot uiting

2 Kruisbergen, E.W., van de Bunt, H.G., Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland, Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*, p. 277.

in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Wet toezicht trustkantoren (Wtt), welke onder meer bovenstaande genoemde meldingsplichtige instellingen verplichten ongebruikelijke transacties te melden bij de Financial Intelligence Unit Nederland (FIU-Nederland). De ongebruikelijke transacties worden door de FIU geanalyseerd en indien daar aanleiding toe is verdacht verklaard. Deze verdacht verklaarde transacties worden ter beschikking gesteld aan de diverse opsporings-, inlichtingen- en veiligheidsdiensten, waar ze worden gebruikt als informatie voor het starten van opsporingsonderzoeken, als sturingsinformatie bij onderzoeken, als bewijsvoering en als een bron voor het opmaken van criminaliteitsbeelden.[3]

In het kader van de aanpak op Zuid is daarom geëxperimenteerd met het aanbrengen van een puur financiële focus op het gebied door in te zoomen op de verdachte transacties (hierna: VT's). De hypothese daarbij was dat wanneer de bestaande en beschikbare informatie van de FIU proactief geanalyseerd en consistent en consequent benut wordt, er zicht ontstaat op personen, bedrijven en criminele infrastructuren die mogelijk anders onder de radar blijven. De gegenereerde inzichten zouden nieuwe kansen kunnen opleveren voor de aanpak van ondermijnende en georganiseerde criminaliteit.

## 3. Verdachte transacties

Als het gaat om VT's, dan geven de jaarverslagen van de FIU enig zicht op de omvang daarvan. In bijvoorbeeld 2014 worden er bij de FIU bijna 277.000 ongebruikelijke transacties gemeld. Bijna 29.000 worden hiervan om verschillende redenen verdacht verklaard. Deze verdachte transacties hebben een totale waarde van € 2,4 miljard. Opvallend is dat 90% hiervan bestaat uit kleine bedragen van onder de € 2.000, -.
In 2015 zien wij een vergelijkbaar beeld maar stijgt het aantal VT's licht. Het totale bedrag aan VT's is dat jaar € 2 miljard en wederom bestaat dit voor bijna 90% uit kleine transacties.

In 2016 ontvangt de FIU-Nederland 417.067 ongebruikelijk gemelde transacties, wat een toename van meer dan 25% betekent in vergelijking met 2015. Daarmee nam in 2016 tevens het aantal verdacht verklaarde transacties verder toe tot 53.533. De totale waarde van de verdachte transacties bedroeg daarbij € 4,6 miljard, wat meer dan een verdubbeling betekent in vergelijking met 2015.[4]

3 Financial Intelligence Unit - Nederland (2017) FIU-Nederland, *Jaaroverzicht 2016*, p. 22.
4 Financial Intelligence Unit - Nederland (2017) FIU-Nederland, *Jaaroverzicht 2016*, p. 2.

De analyse van VT's ten behoeve van de integrale aanpak van georganiseerde criminaliteit in Rotterdam heeft geleid tot zicht op concrete en nieuwe namen van betrokkenen (natuurlijke personen en bedrijven) bij verdachte transacties. Daarnaast heeft de analyse geleid tot inzichten in de betrokkenheid en rol van meldingsplichtige instellingen zoals banken. In het bijzonder waar het gaat om het cliëntenonderzoek, het meldproces en de onderliggende dienstverlening door banken.

## 4. Inzichten

Op basis van de analyse vallen er zoals gezegd een aantal zaken op als het gaat om de positie van de banken. Hierbij moet opgemerkt worden dat dit beeld is gevormd op basis van de volledig geanonimiseerde casuïstiek die in Rotterdam integraal behandeld is en daarmee slechts een klein gedeelte is van het totale aantal transacties gemeld door banken. Daarmee is het niet generaliseerbaar, maar geeft het wel een beeld van wat we veelvoudig in de praktijk tegenkomen bij het analyseren van verdachte transacties en wat voor effecten dit heeft voor het vroegtijdig signaleren van witwasrisico's

Een van de opvallendste zaken is dat de risicoprofilering en het daaruit voortvloeiende risicogebaseerde cliëntenonderzoek per situatie en per instelling nog alkan verschillen. Hierin kan meespelen dat de Wwft vrij duidelijk over welke stappen er genomen moeten worden indien er sprake is van een verhoogd risico en indien er cliëntenonderzoek wordt uitgevoerd. De wettekst geeft slechts een aantal indicaties wanneer er daadwerkelijk sprake is van een verhoogd risico. Deze beoordeling in het concrete geval is overgelaten aan de instelling zelf. In de praktijk blijkt dat de ruimte die bestaat voor banken om een eigen risicoschatting te doen, vragen oproept aan de kant van de opsporing: hoe kan het dat deze instelling dergelijke transacties heeft gefaciliteerd? En ook: waarom zijn deze transacties niet eerder gemeld? Dit laatste is relevant, aangezien het 'onverwijld melden' uit de Wwft een duidelijk opsporingsbelang dient.

Hieronder willen we aan de hand van een aantal concrete casus deze vragen, die aan de kant van de opsporing opkomen, verduidelijken.

We hopen dat door het delen van onze praktijkervaring en het adresseren van deze vragen de casuïstiek ook aanknopingspunten biedt voor aanscherping en verbetering van het detectie- en meldproces en keuzes met betrekking tot de onderliggende dienstverlening.

**Voorbeeld 1: verhoogd risico bij voortgaande dienstverlening**

In 2016 wordt door een bank gemeld dat een cliënt in enkele maanden meer dan één ton contant stort op haar betaalrekening. De gelden worden in meerdere transacties overgeboekt naar een bananenexporteur in Zuid-Amerika. Bij de exporteur wordt dat jaar tot drie keer toe een lading cocaïne aangetroffen, waarvan eenmaal een lading met een straatwaarde van enkele tientallen miljoenen. Het valt de bank op dat de rekening van de onderneming, van welke haar partner de eigenaar is, bijna volledig gevoed wordt door contante stortingen. De contante stortingen bevatten meerdere tonnen in een paar maanden tijd en worden vrijwel altijd in bedragen van 10.000,- euro direct weer contant opgenomen. Op vragen van bank reageren beiden niet, waardoor de herkomst onduidelijk blijft. De bank vermoedt dat het tweetal betrokken is bij een witwasconstructie. De transacties worden ongebruikelijk gemeld, waarna er analyse door de FIU plaatsvindt. Dit leidt tot de vermoedens dat beide betrokken zijn bij internationale handel in drugs en onderdeel uitmaken van een omvangrijke internationale witwasconstructie, welke gebruik maakt van banken om het contante geld te storten.

Bron: rijnmond.nl

In het bovenstaande voorbeeld blijkt duidelijk dat er sprake is geweest van een risicoschatting door de betreffende bank en ziet men bekende witwastypologiëen zoals contante opnames, stortingen en transacties naar risicolanden. Hierbij worden door de bank ook vraagtekens gezet en wordt er nader onderzoek naar gerelateerde cliënten uitgevoerd. De opvallendheden uit het nadere onderzoek worden uiteindelijk gemeld in een (geclusterde) ongebruikelijke transactie. Dit houdt in dat meerdere transacties die over een langere periode gevat worden in een enkele ongebruikelijk gemelde transactie. Naast de voor de hand liggende vraag over het tijdstip van melden, leeft aan de kant van de opsporing ook de vraag naar welke aanvullende maatregelen de instelling treft, naast het melden van de ongebruikelijke transactie. Uit de gemelde transacties valt namelijk op te maken dat de dienstverlening op zijn minst negen maanden is voorgezet. Ondanks dat de risicoprofilering en het cliëntenonderzoek uitwezen dat er mogelijk sprake kon zijn van een witwasconstructie. Hierdoor faciliteert de bank mogelijkerwijs negen maanden lang een crimineel netwerk. Dit is in potentie een zeer hoog risico.

**Voorbeeld 2: alertheid t.o.v. nieuwe ontwikkelingen**

In 2015 begint het rekeningverloop van een cliënt op te vallen bij de security afdeling van een bank. De cliënt ontvangt in een paar maanden tijd een groot bedrag van een Bitcoin-exchange (een handelsplatform voor het kopen en verkopen van bitcoins). Opvallend is dat de ontvangen gelden vrijwel altijd dezelfde dag contant worden opgenomen in enkele duizenden euro's per keer. Dit, zo stelt de bank, is om de sporen van witwassen uit te wissen en de herkomst van de gelden te versluieren. Het lijkt er niet op dat de cliënt speculeert met bitcoins aangezien er geen girale aankopen van bitcoins of andere uitgaven zichtbaar op de rekening zijn. Hierdoor lijkt een legitieme herkomst van de gelden nog onwaarschijnlijker. De bank meldt een aantal ongebruikelijke transacties bij de FIU en de cliënt wordt een half jaar op 'verhoogd risico' geplaatst. Indien de ongebruikelijke transacties verdacht worden verklaard door FIU of de bitcoinhandel na een half jaar nog steeds gaande is, dient er nader onderzoek plaats te vinden, zo stelt de bank. Nader onderzoek bij de FIU leert dat het adres dat bij het openen van de rekening is opgegeven overeenkomt met andere personen in hun systemen. Deze personen blijken via social media in relatie te staan tot een aantal andere personen, welke tevens in relatie te brengen zijn met andere verdachte transacties. Er ontstaat zicht op een relatief jong, hoog opgeleid netwerk dat in één jaar tijd miljoenen ontvangt van verschillende buitenlandse bitcoin-exchanges. Hierop wordt er een strafrechterlijkonderzoek gestart naar internationale drugshandel via een ontoegankelijk deel van het internet genoemd het 'darkweb'. De personen blijken betrokken te zijn bij een internationaal opererend crimineel netwerk bestaande uit honderden personen en bedrijven.

Bron: rivento-spark.nl

In dit concrete voorbeeld is er sprake van een melding van een aantal geclusterde ongebruikelijk transacties. Wat echter nog interessanter is, is het fenomeen bitcoins waarmee de bank hier te maken krijgt. De bitcoin is een virtuele valuta welke gebruikt maakt van 'peer-to-peer-technologie'. Dit betekend dat het systeem wordt onderhouden door het gehele collectief dat gebruik maakt van de munt en dat deze werkt zonder centrale instantie. Bijkomend gegeven is dat de bitcoin relatief anoniem is ten opzichte van reguliere valutasoorten. Dit leidt ertoe dat de bitcoins veelal worden gebruikt op de zogenaamde 'cryptomarkets' oftewel 'darknet markets'. Dit zijn online marktplaatsen, vergelijkbaar met marktplaats.nl en ebay.com, die alleen toegankelijk zijn met behulp van speciale encryptiesoftware en waarop verschillende verboden goederen en diensten worden verhandeld. Deze versleutelde en verborgen markten maken het voor politie en justitie ingewikkeld om illegale transacties op deze sites op te sporen en te vervolgen. Het gevolg hiervan is dat bitcoins gebruikt worden bij online drugshandel en witwasconstructies.

In recent onderzoek wordt gesteld dat Nederlandse verkopers verantwoordelijk zijn voor 8% van de totale drugsomzet op acht geanalyseerde online markten.[5] Dit fenomeen leidt ertoe dat in augustus 2017 een aantal nieuwe witwastypologieën zijn vastgesteld met betrekking tot virtuele valuta, waaronder het meermalen binnen een relatief korte periode opnemen van aanzienlijke contante bedragen vanaf bankrekeningen zonder economische verklaring, in combinatie met het meermalen giraal ontvangen van aanzienlijke bedragen van bitcoin exchanges.[6]

Deze typologieën komen tevens terug in het bovenstaande voorbeeld en hadden in combinatie met het klantprofiel, er is immers sprake zeer opvallend rekeningverloop, mogelijk in een vroeger stadium moeten leiden tot het melden van ongebruikelijke transacties en interne maatregelen bij de bank. Daarnaast wordt de cliënt op 'hoog risico' geplaatst voor een half jaar in afwachting van de verdacht verklaring van de voorgaande ongebruikelijk gemelde transactie, alvorens aanvullend onderzoek te doen. Dit zorgt voor vertraging in het meldproces. Tijd die kostbaar is in de opsporing. Opleiding en training van het personeel van de banken (conform artikel 35 Wwft) met inbegrip van nieuwe witwastypologieën en het actief, consistent en consequent monitoren van transacties kunnen dit soort situaties voorkomen en vormen daarmee een waardevolle bijdrage aan het vroegtijdig signaleren, opsporen en vervolgen van strafbare feiten.

**Voorbeeld 3: twee banken, twee risicoschattingen**

Begin dit jaar valt een opmerkelijke bijschrijving op de rekening van een cliënt de bank op. Waar normaliter de betaalrekening wordt gevoed door de inkomsten uit een onderneming, worden ditmaal enkele honderdduizenden euro's onder de vermelding 'lening' bijgeschreven. De ontvangen gelden worden d.m.v. een spoedbetaling overgeboekt naar het rekeningnummer van een notaris. Dit doet de bank vermoeden dat de cliënt een huis gekocht met middelen uit een ongebruikelijke bron. De transactie wordt door de FIU verdacht verklaard en er wordt een witwasonderzoek gestart. Dit leidt enkele maanden later tot het doorzoeken van meerdere panden, waarbij beslag wordt gelegd op onroerend goed, auto's, horloges, bitcoins, contant geld en drugs. Een van de panden blijkt ingericht te zijn als distributiecentrum voor drugs. Vrijwel gelijktijdig met de doorzoekingen doet een andere bank een melding bij de FIU. Het betreft de bank van de medeverdachte, welke in ruim twee jaar tijd enkele honderdduizenden euro's contant op eigen rekening stort. Dit wordt vervolgens overgeboekt als lening voor het aan te kopen pand. De bank merkt op dat er gebruik wordt gemaakt van grote coupures, de cliënt de herkomst

5 Kruithof, K., e.a. (2016) *Internet-facilitated drugs trade, An analysis of the size, scope and role of the Netherlands*, WODC, Ministerie van Veiligheid en Justitie, p. 18.

6 www.fatf-gafi.org/publications/?hf=10&b=10&s=desc(fatf_releasedate)

van de gelden niet kan of wil onderbouwen en niet meer reageert op verzoeken tot contact van de bank.
Bron: lc.nl

De witwasconstructie uit de bovenstaande casus kent twee kanten. Zo zien we enerzijds een opmerkelijke transactie ten behoeve van de aankoop van vastgoed onder het mom van een 'lening' en anderzijds zien we de contante stortingen om de vastgoedtransactie te financieren. De 'poortwachtersfunctie' van de banken komt hierbij nadrukkelijk tot uiting bij de eerste fase van het witwasproces, namelijk het plaatsen van crimineel geld in het bancaire systeem.[7] Het blijkt echter dat hoewel beide banken uit het voorbeeld dezelfde poortwachtersfunctie vervullen, deze klaarblijkelijk anders wordt ingevuld. De melding betreffende de contante stortingen volgt pas vele maanden later na het starten van het strafrechtelijk onderzoek en het vorderen van de rekeningen van de verdachten. Aan de kant van de opsporing roept dit de vraag op of de informatiepositie van de bank toereikend is. Echter, beide banken nemen hetzelfde girale verkeer waar. Daarnaast lijkt, afgaande op de inhoud van de melding, er achteraf voldoende grond te zijn geweest om in een eerder stadium een aantal meldingen van ongebruikelijke transacties aan FIU te doen. Wij zien dat reactief nader onderzoek plaatsvindt met een geclusterde melding tot gevolg, waarbij waardevolle details van de 'losse' transacties niet meer uit de enkele verdachte transactie af te leiden zijn. Hierdoor kon waardevolle informatie voorafgaand aan het doorzoeken van de woningen niet meegenomen worden. Dit doet dan ook de vraag rijzen wat de interne richtlijnen van de betreffende banken zijn voor het starten van nader onderzoek naar het transactiepatroon van bepaalde clienten en welke parameters zij hanteren ten behoeve van het vroegtijdig signaleren van risico's.

**Voorbeeld 4: Alerte kantoormedewerker**

In de zomer van 2015 vindt een gesprek plaats bij een bank. De eigenaar van een bedrijf meldt zich bij de balie van een bankfiliaal om een aantal rekeningen te openen. De eigenaar stelt onlangs een goede verkoop te hebben gedaan en in het bezit te zijn enkele miljoenen aan contanten in verschillende valuta's. De kantoormedewerker antwoordt hierop dat de bank hier geen medewerking aan kan verlenen. Naast het blokkeren van de transactie besluit de bank een onderzoek in te stellen naar de nieuwe klant. Het blijkt dat het bedrag vervolgens niet op de geopende rekeningen wordt gestort, maar dat er wel verschillende schimmige transacties plaatsvinden. Daarnaast blijkt dat de eigenaar in verschillende open bronnen naar voren

7 Dean, G., Fahsing, I. & Gottschalk, P. (2010) *Organizes crime: Policing illegal business entrepreneurialism*, Oford: Oxford University Press 2010.

komt als verdachte in internationale drugsonderzoeken. De bank acht de situatie zeer ongebruikelijk en besluit de transactie te melden bij de FIU.
Bron: Google.nl

Bij de bovenstaande 'voorgenomen' oftewel niet uitgevoerde transactie wordt voorafgaand aan de transactie een risicoschatting gemaakt door de bank. Zo blijkt dat de bank de risico indicatoren, zoals het gebruik van verschillende valuta's, contant geld en het ontbreken van een economisch verklaarbare herkomst, meeweegt bij de dienstverlening aan de cliënt. Dit getuigt van kennis van de bekende witwastypologieën zoals gesteld en laat zien dat hier sprake is van alertheid en training van het personeel. Daarnaast wordt na het blokkeren van de transactie een cliëntenonderzoek ingesteld, waarbij de eigen systemen en de open (internet) bronnen worden geraadpleegd. Dit resulteert in het aanmerken van de voorgenomen transactie en het rekeningverloop als ongebruikelijk bij de FIU. De dienstverlening wordt echter wel voortgezet.

## 5. Conclusies en aanbevelingen

Door bestaande en beschikbare informatie, zoals de VT's, proactief, consistent en consequent te analyseren en te benutten, ontstaat er zicht op personen, bedrijven en criminele infrastructuren die vanuit een traditionele invalshoek onder de radar blijven. Tijdens dit traject zijn er tevens inzichten ontstaan waaruit de positie van de banken als poortwachter bij de aanpak van georganiseerde criminaliteit nadrukkelijk blijkt.

Vanuit deze kennis worden een aantal aanbevelingen gedaan gericht voor adequate en tijdige risicoprofilering en voor het kritischer bezien van de onderliggende dienstverlening door banken aan cliënten, die betrokken zijn bij door de bank gemelde ongebruikelijke transacties. Deze aanbevelingen hebben tot doel om vanuit de gezamenlijke aanpak van georganiseerde criminaliteit te voorkomen dat financiële instellingen bewust of onbewust meewerken aan witwasconstructies.

### Adequate, tijdige risicoprofilering

Aan de kant van de opsporing zijn meldingen een belangrijke 'grondstof'. Wij worden nogal eens geconfronteerd met meldingen waaruit afwijkingen blijken ten opzichte van 'reguliere' cliënten. Hoewel de meldingen uiteindelijk als ongebruikelijk worden bestempeld, zijn dit dikwijls meldingen die 'geclusterd' zijn, die over een lange periode en relatief laat na de aanvankelijke transacties worden gemeld. Dit leidt ertoe dat de informatie door tussenkomst van de FIU later bij de opsporingsdiensten en/of andere ketenpartners terecht komt en daarmee leidt tot minder snel optreden. Dit doet dan ook de vraag

rijzen wat de interne richtlijnen van de betreffende instellingen zijn voor het starten van een nader onderzoek en welke parameters zij hanteren ten behoeve van het vroegtijdig signaleren van risico's. Door op een systematische wijze risico's te analyseren met behulp van betere systeemanalyses en 'big data' kan men komen tot een slimmere en snellere manier van risicoprofilering, tot op cliënt- en transactieniveau. Kortom, het is zaak dat financiële instellingen blijven investeren in adequate (digitale) infrastructuur en capaciteit vrijmaken om systemen op dermate wijze in te richten dat de data van voldoende kwaliteit zijn om risicoanalyse plaats te laten vinden. Mogelijkerwijs kunnen nieuwe technieken zoals de inzet van 'advanced analytics' en 'artificial intelligence' bijstaan in het analyseren van grote hoeveelheden data.

### Verschil in de risicoprofilering

De analyse van VT's brengt verschillen in risicoprofilering bij de banken aan het licht. Zo blijkt uit de casuïstiek dat banken hetzelfde girale verkeer waarnemen, maar er verschil zit in de inhoud, periode en tijdigheid van de meldingen bij de FIU – ook waar het gaat om dezelfde casus. Voor de opsporing is dit een lastig dilemma, aangezien de instellingen dezelfde poortwachtersfunctie vervullen en moeten voldoen aan dezelfde bepalingen van de Wwft. Het lijkt er vooralsnog op dat – en dan zeggen we het voorzichtig – de financiële instelling niet in alle gevallen tot een adequate, tijdige risicoprofilering komt. Dit doet dan ook de vraag rijzen wat de mogelijke verschillen zijn tussen interne richtlijnen van de financiële instellingen voor het starten van nader onderzoek en welke parameters zij hanteren ten behoeve van het vroegtijdig signaleren van risico's. Hoe zijn deze verschillen onderbouwd (deze contextuele kennis kan ook voor opspoorders relevant zijn in hún beoordeling) en op welke wijze is een adequate en homogene risicoprofilering in te stellen?

### Voortzetting dienstverlening

Uit het feit dat er transacties gemeld worden blijkt dat er risicoschattingen plaatsvinden ten aanzien van de dienstverlening aan cliënt. Daarnaast wordt nadere onderzoeken ingesteld, waarbij de eigen systemen en de open (internet)bronnen worden geraadpleegd, met als resultaat dat transacties als ongebruikelijk worden gemeld bij de FIU. Het valt echter op dat na het melden van de transacties de dienstverlening vaak pas na een relatief lange periode wordt stopgezet of in sommige gevallen wordt voorgezet, terwijl er alle aanleiding lijkt te zijn om de dienstverlening per direct stop te zetten. Hoewel dit te maken kan hebben met de geheimhoudingsplicht van de banken, lijkt het soms onevenredig lang te duren. Hierdoor is niet uit te sluiten dat de betrokken instelling, in ieder geval tijdelijk, mogelijkerwijs witwasconstructies en/of de financiering van terrorisme faciliteert. De instelling loopt hiermee zeer hoge (zo niet onacceptabele) risico's, die raken aan het Wetboek van Strafrecht (schuldwitwassen). Het verdient dan ook de aanbeveling om zowel intern als extern, met bijvoorbeeld de toezichthouder of andere

overheidspartners, dit soort casuïstiek vaker te bespreken en zo tot passende interne en externe maatregelen te komen.

### Reactieve houding meldingsplichtige instellingen

Naast adequate, tijdige risicoprofilering, de verschillen daarin en de voortzetting van de dienstverlening zien we opvallende zaken met betrekking tot het moment wanneer instellingen melden. Zo blijkt uit de behandelde casuïstiek dat de betreffende banken niet altijd melden op basis van de risicoprofilering, maar als reactie op het vorderen van rekeningen in het kader van een opsporingsonderzoek. Hoewel dit niet altijd te voorkomen valt, aangezien opsporingsdiensten doorgaans over andere informatie dan banken beschikken, valt tevens uit de meldingen op te maken dat er vaak wel al risico-indicaties beschikbaar waren die in een eerder stadium hadden kunnen leiden tot een melding ongebruikelijke transactie. Daarnaast wordt in sommige meldingen gesproken over het plaatsen van clienten op 'hoog risico' voor een half jaar in afwachting van de verdacht verklaring van de voorgaande ongebruikelijk gemelde transactie alvorens aanvullend onderzoek te doen. Naast het feit dat dit de rollen van de bank en FIU omdraait bij het vroegtijdig signaleren van witwassignalen, zorgt deze reactieve houding tevens voor vertraging in het meldproces. Het verdient dan ook de aanbeveling om risicovolle transacties consequent en consistent te analyseren.

### Training, gebruik typologieën en ontwikkelingen bij de risicoschatting

DNB stelt vast dat banken opleidingen en trainingen over de Wwft hebben opgenomen in jaarlijkse trainingsprogramma's en verwacht hierbij dat de inhoud van zo'n programma zodoende is opgesteld dat de bankmedewerkers zich bewust worden van witwas- en terrorismefinancieringsrisico's. Deze programma's dienen tevens toegespitst te zijn op de functies, werkzaamheden en het niveau van de doelgroep: van bestuur en senior management tot junior medewerker. Daarnaast stelt DNB dat bij het opstellen van het trainingsprogramma er gebruik wordt gemaakt van casuïstiek vanuit het eigen transactiemonitoringsproces en van de casuïstiek die de FIU[8] iedere twee weken publiceert. Het verdient dan ook de aanbeveling om waar nodig de nieuwe ontwikkelingen en typologieën uit te leren binnen de organisaties. Het actief delen van casuïstiek en nieuwe ontwikkelingen op het gebied van witwassen tussen publiek/private organisaties is hierbij behulpzaam.

8 De Nederlandsche Bank N.V. (2017) *Post-Event transactie-monitoringsproces bij banken, Guidance*, De Nederlandsche Bank, p. 42.

De rapporten van de Financial Action Taskforce (FATF)[9] zijn hiervan een voorbeeld. De FATF beoordeelt onder andere of de anti-witwasmaatregelen in een land voldoende worden nageleefd en in hoeverre er actief wordt gewerkt aan het ontwikkelen van de witwasbestrijding. Ook brengt de FATF 'typology-reports' uit. Dit zijn rapporten waarin veelvoorkomende methoden en trends van witwassen en terrorismefinanciering worden vastgesteld en beschreven.

Zo heeft het fenomeen bitcoins ertoe geleid dat in augustus 2017 een aantal typologieën zijn vastgesteld van witwassen met betrekking tot virtuele valuta. Deze typologieën zijn in combinatie met het klantprofiel zeer waardevol voor de risicoschatting en kunnen wellicht leiden tot het melden van een ongebruikelijke transactie in een vroeg stadium en interne maatregelen bij de bank. Het verdient dan ook de aanbeveling om typologieën, ontwikkelingen frequenter uit te venten. Daarnaast zouden deze trainingsprogramma's bindend moeten zijn voor de opleidingsprogramma's van de banken. Training en onderwijs met betrekking tot relevante ontwikkelingen op het terrein van witwassen en georganiseerde criminaliteit, met inbegrip van de witwastypologieën, zijn hierbij een absolute must en is wellicht enkel doeltreffend indien er een landelijk trainings- en opleidingsprogramma beschikbaar wordt gesteld.

## Tot slot

Op basis van de door ons uitgevoerde analyse zijn een aantal verbeterpunten te benoemen in het proces van detectie, onderzoek en melden van ongebruikelijke transacties door de banken. Wij zijn er van overtuigd dat door het in samenwerking met financiële instellingen, toezichthouders en de overheid verbeteren van deze punten het voorkomen en bestrijden van witwassen en terrorismefinanciering een stevige impuls kan krijgen.

9 Jenne, B.C.G. & van Doorn, J.E.E. (2009) 'Aanvullend cliëntenonderzoek in de Wwft', *Jaarboek Compliance 2009*, P. 236.

**Literatuurverwijzingen**


- Dean, G., Fahsing, I. & Gottschalk, P. (2010) *Organizes crime: Policing illegal business entrepreneurialism*, Oford: Oxford University Press 2010.
- De Nederlandsche Bank N.V. (2017) *Post-Event transactie-monitoringsproces bij banken, Guidance,* De Nederlansche Bank, geraadpleegd van www.toezicht.dnb.nl/binaries/50-236416.pdf.
- FATF Guidance (2013) *National Money laundering and terrorist financing risk assessment, Financial Action Task Force*, geraadpleegd van www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.
- Financial Intelligence Unit - Nederland (2017) FIU-Nederland, *Jaaroverzicht 2016,* geraadpleegd van www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/fiu_jaaroverzicht_2016.pdf.
- Jenne, B.C.G. & van Doorn, J.E.E. (2009) Aanvullend cliëntenonderzoek in de Wwft, *Jaarboek Compliance 2009,* geraadpleegd van www.compliance-instituut.nl/wp-content/uploads/Aanvullend-clientenonderzoek-in-de-Wwft.pdf.
- Kruisbergen, E.W., van de Bunt, H.G., Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland, Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*, O&B 306.
- Kruithof, K., Aldridge J., Décary-Hétu, D., Sim, M., Dujso, E. & Hoorens, S. (2016) *Internet-facilitated drugs trade, An analysis of the size, scope and role of the Netherlands*, WODC, Ministerie van Veiligheid en Justitie, geraadpleegd van www.wodc.nl/binaries/2671-volledige-tekst_tcm28-124626.pdf.
- Tops , P. & Tromp J., (2016) *De achterkant van Nederland, hoe onder- en bovenwereld verstrengeld raken*, Balans Uitgeverij.