Klanten identificeren leidt niet tot betere opsporing

Bart Custers

SAMENVATTING Om witwassen, terreurfondsen en fraude tegen te gaan, zijn financiële instellingen sinds kort verplicht hun klanten te identificeren. Op basis van de Wet Identificatie bij Dienstverlening (WID) worden grootschalige programma's voor klantidentificatie opgezet. Door het gebruik van procedures en standaarden is het echter eenvoudig voor criminelen om aan opsporing en vervolging te ontkomen.

1 Inleiding

Sinds kort is in Nederland de Wet Identificatie bij Dienstverlening (WID) ingevoerd. Deze wet verplicht Nederlandse financiële instellingen om de identiteit van hun klanten vast te stellen en vast te leggen, met als doel ongebruikelijke transacties gemakkelijker te kunnen melden. De WID geldt voor banken en verzekeraars, maar ook voor dienstverleners zoals advocaten, notarissen, belastingadviseurs en openbare accountants. Als gevolg hiervan hebben veel Nederlanders inmiddels een brief gehad om met hun paspoort of identificatiebewijs langs te komen bij de bank.

Het doel van de WID is het bestrijden van fraude, witwassen en terreurfondsen. In deze bijdrage zal ik uiteenzetten dat grootscheepse identificatieprogramma's niet bijdragen aan het bereiken van dit doel. Sterker nog, doordat ze de indruk geven dat er veel gedaan wordt, wordt nagelaten de nodige maatregelen te treffen om fraude, witwassen en terreurfondsen echt tegen te gaan. Om aan de regels te voldoen, wordt alles in procedures en standaarden gegoten. Standaardisatie in opsporingstechnieken maakt het echter eenvoudig voor criminelen om de dans te ontspringen. Het zou beter zijn om te werken met kleinschalige en flexibele teams die gericht kunnen opsporen.

In paragraaf 2 wordt de nieuwe Nederlandse en Amerikaanse wetgeving besproken die de aanleiding vormt voor klantidentificatie. Na de identificatie moeten de risico's van de klanten vastgesteld worden. De implementatie hiervan wordt uitgelegd in paragraaf 3. In paragraaf 4 wordt toegelicht dat de verplichte aanpak die de wetgeving voorschrijft niet tot het gewenste doel leidt vanwege de grootscheepse en voorspelbare aanpak. In paragraaf 5 wordt onderbouwd waarom het beter zou zijn om met kleine expertteams te werken. Door de aandacht meer op het doel (het opsporen van fraude, witwassen en terreurfondsen) te richten en minder op de procedures, kan veel tijd en geld bespaard worden. Tegelijkertijd zal de opsporing veel doeltreffender zijn. Deze conclusies worden in paragraaf 6 besproken.

Dr. ir. B.H.M. Custers is senior consultant bij Capgemini en postdoc onderzoeker aan de Universiteit van Tilburg. Zijn aandachtsgebieden zijn risicoprofilering en privacy, in het bijzonder op de terreinen van fraude, witwassen en terrorisme.

2 Nieuwe wetgeving

Als gevolg van terroristische aanslagen, boekhoudschandalen en toenemende witwaspraktijken wordt er steeds meer wet- en regelgeving opgesteld voor financiële instellingen. In dit kader kan onderscheid gemaakt worden tussen regelgeving die gericht is op de financiële soliditeit van ondernemingen (zoals Sarbanes-Oxley en Basel) en regelgeving die identiteitsfraude, witwassen en terreurfondsen tegengaat (zoals de WID en de Amerikaanse Patriot Act). Dit onderscheid betreft ook de belanghebbenden: het eerste soort regelgeving beschermt vooral de aandeelhouders van financiële instellingen, het tweede soort regelgeving heeft als achterliggend doel de maatschappij te beschermen tegen criminaliteit.

De regelgeving voor het opsporen van fraude, witwassen en terreurfondsen kan onderscheiden

worden in twee verschillende benaderingen. In de eerste plaats is dat het melden van ongebruikelijke transacties (Wet MOT) en in de tweede plaats is dat het identificeren van je klanten (WID). Deze twee wetten proberen elkaar aan te vullen: als er een ongebruikelijke transactie plaatsvindt, moet snel te achterhalen zijn om welke klant het werkelijk gaat. Daarnaast heeft de identificatiewetgeving tot doel om risicovolle klanten te mijden, nog voordat zich incidenten hebben voorgedaan. Naar aanleiding van de introductie van de WID richt deze bijdrage zich op de identificatiewetgeving; voor meer informatie over de Wet MOT, wordt hier verwezen naar Faber en Van Nunen (2004).

Al voordat de WID in werking trad, waren veel financiële instellingen op basis van Amerikaanse wetgeving verplicht hun klanten te identificeren. Met name op basis van de Amerikaanse Bank Secrecy Act (BSA) en de Patriot Act zijn banken verplicht te achterhalen met wie ze zaken doen. Van elke klant moet een risicoprofiel worden opgesteld en bij onaanvaardbare risico's kan er worden ingegrepen, bijvoorbeeld door klanten te weigeren of de autoriteiten in te lichten. Dit proces staat bekend als Know Your Customer (KYC).

Hoewel de Amerikaanse wetgeving niet wereldwijd geldt, wordt wel geëist dat financiële instellingen in de Verenigde Staten hun KYC-beleid wereldwijd implementeren. Omdat voor veel internationale banken het opschorten van hun activiteiten in de Verenigde Staten geen overweging is, worden op deze manier indirect ook KYC-verplichtingen opgelegd aan andere landen. Hoewel het intrekken van een bankvergunning de ultieme sanctie is van een toezichthouder, kunnen ook boetes worden opgelegd. Dat dit een reëel risico is, mag blijken uit het feit dat in 2005 een grote Nederlandse bank een boete van miljoenen dollars kreeg vanwege verboden transacties met Iran en Libië (Simpson, 2005).

Sinds kort zijn in Nederland delen van KYC-wetgeving ingevoerd in de nieuwe Wet Identificatie bij Dienstverlening. De WID verplicht Nederlandse financiële instellingen om de identiteit van hun klanten vast te leggen, met als doel ongebruikelijke transacties gemakkelijker te kunnen melden om zodoende fraude, witwassen en terreurfondsen te bestrijden. De WID geldt voor banken en verzekeraars, maar ook voor dienstverleners zoals advocaten, notarissen, belastingadviseurs en openbare accountants.

3 Risicoanalyses

Het implementeren van een KYC/WID-beleid betekent dat er risicoprofielen moeten komen van alle bestaande en nieuwe klanten. Daarvoor moeten allerlei karakteristieken van de klant in kaart gebracht worden, met bijbehorend bewijsmateriaal. Het verzamelen van klanteigenschappen kan via de klant zelf, maar ook via allerlei externe partijen, zoals Kamers van Koophandel, aandelenbeurzen en toezichthouders. Aan die karakteristieken wordt vervolgens door een weging een risico toegekend, een soort rapportcijfer voor betrouwbaarheid. Deze betrouwbaarheid is afhankelijk van zowel de inhoud van de documentatie (een postbusonderneming kan bijvoorbeeld duiden op een gebrek aan transparantie) als de herkomst van de informatie (de toezichthouders in Rusland staan bijvoorbeeld bekend als minder betrouwbaar dan de toezichthouders in Duitsland).

De klanteigenschappen waaraan gedacht kan worden, zijn onder meer personalia, kredietwaardigheid, aantal en typen rekeningen, feiten van fraude/criminaliteit uit het verleden, et cetera. Bewijsvoering gaat gewoonlijk door middel van kopieën van paspoorten en andere documenten, zoals verklaringen van goed gedrag. Omdat het verzamelen van kopieën van paspoorten voorheen niet verplicht was, roepen verschillende banken hun klanten nu op om nogmaals langs te komen met hun identificatiebewijs.

Bij rechtspersonen zijn de klanteigenschappen enigszins anders, zoals markt/handelsactiviteiten en namen van directeuren, aandeelhouders en eigenaren. Daarnaast is van belang of de rechtspersoon ingeschreven staat bij (of onder toezicht staat van) een aandelenbeurs, een Kamer van Koophandel, een financiële autoriteit of een lokale overheid. Bewijsvoering gaat meestal met uitreksels van handelsregisters, documenten van toezichthouders, jaarverslagen met accountantsverklaring, oprichtingsaktes, et cetera.

De uiteindelijke weging van de risico's hangt af van welke eigenschappen als risicovol worden gezien. Vaak zijn dat eigenschappen die eerdere gevallen van fraude, witwassen of terreurfondsen met elkaar gemeen hebben en eigenschappen die transparantie belemmeren. Enkele eigenschappen die als risicovol worden gezien, zijn bijvoorbeeld:

- *De locatie van klant*: landen als Irak, Somalië of Noord-Korea worden als zeer risicovol gezien, omdat er weinig of geen toezicht is op natuurlijke personen en rechtspersonen. Hetzelfde geldt, hoewel in mindere mate, voor landen als Rusland en India. Daarnaast zijn er landen waarmee de Amerikaanse overheid handel verbiedt. Hierbij valt te denken aan Cuba en Iran.[1]
- *Handelsactiviteiten*: bepaalde handelsactiviteiten zijn gevoelig voor witwaspraktijken en terreurfondsen. Voorbeelden hiervan zijn casino's, wisselkantoren en

diamanthandels. Doordat in deze branches veel contant geld omgaat, is de transparantie soms beperkt.

- *Bedrijfsvorm*: zogeheten postbusbedrijven zijn louter papieren constructies waar geen bedrijfsactiviteiten plaatsvinden. Vaak zijn ze opgericht om belastingtechnische redenen. Deze constructies kunnen ondoorzichtig zijn als vastgesteld moet worden wie de directeuren of eigenaren zijn. Ook voor bepaalde Nederlandse rechtsvormen is het toezicht gebrekkig. Voor bijvoorbeeld het oprichten van stichtingen is de "verklaring van geen bezwaar" niet vereist, terwijl er steeds meer signalen zijn dat bepaalde stichtingen terreurfondsen doorsluizen. Daarnaast kunnen buitenlandse bestuurders soms moeilijk getraceerd worden op basis van enkel een naam en adres.
- *Aanwezigheid op zwarte lijsten:* als directeuren, aandeelhouders of eigenaren voorkomen op zwarte lijsten kan dit een verhoogd risico betekenen. In geval van rechtspersonen kan ook een bedrijfsnaam op een zwarte lijst voorkomen. Van belang is om onderscheid te maken tussen lijsten die een verhoogd risico aangeven en lijsten die transacties verbieden met bepaalde klanten. Soms worden lijsten met een verhoogd risico ook wel aangeduid als 'grijze lijsten' om ze te onderscheiden van de 'echte' zwarte lijsten die een verbod inhouden.

Het laatstgenoemde punt, zwarte lijsten, verdient wellicht nadere toelichting. Zowel de Verenigde Staten als de Europese Unie hebben verscheidene zwarte lijsten. Zo is er bijvoorbeeld de OFAC-list van het Office of Foreign Assets Control (OFAC) van het US Department of the Treasury. Op de OFAC-list[2] staan meer dan 5000 personen die als terroristen en/of criminelen worden aangemerkt door de Amerikaanse overheid en waarmee bedrijven geen zaken mogen doen. Andere lijsten waar op gecontroleerd kan worden zijn bijvoorbeeld de FBI ('most wanted') list, de EU-lijst met terroristische organisaties, de Australische DFAT-lijst, de Bank of England-lijst, lijsten van Europol en talloze andere lijsten. Naast lijsten met verdachten van terrorisme en criminaliteit kan ook koppeling plaatsvinden met andere lijsten, zoals lijsten met betrekking tot kredietwaardigheid (in Nederland geregistreerd bij het Bureau Kredietregistratie, BKR).

Naast risicoverhogende eigenschappen zijn er ook risicoverlagende eigenschappen. Meestal gaat het dan om toezicht door onafhankelijke partijen. Bij rechtspersonen kan een beursnotering betekenen dat de betreffende beurs eisen stelt aan transparantie en soliditeit van de onderneming. In verschillende landen is een inschrijving bij de Kamer van Koophandel verplicht en onderhevig aan zorgvuldigheidseisen. Voor financiële markten is er vaak specifiek toezicht, denk bijvoorbeeld aan de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB). Ook klanten die onder de (semi-)overheid vallen zijn meestal onderhevig aan verscherpt toezicht. Uiteraard worden bovengenoemde eigenschappen alleen als risicoverlagend beschouwd in landen waar men de overheid en toezichthoudende instanties betrouwbaar acht.

4 Voorspelbare aanpak

In de praktijk betekent het uitvoeren van de hierboven beschreven regelgeving dat vrijwel alle aandacht uitgaat naar het opstellen van risicoprofielen van onschuldige klanten. Immers, in slechts een zeer klein aantal gevallen (veel minder dan 1 procent) is er werkelijk sprake fraude, witwassen of terreurfondsen. Desalniettemin schrijft de regelgeving voor dat van alle klanten een risicoprofiel moet worden opgesteld. Daarmee verschuift de nadruk naar de wijze van de bedrijfsvoering in plaats van naar het resultaat van de zoektochten. De beoordeling door toezichthouders of aan de regelgeving is voldaan, vindt plaats op basis van de procedures en systemen die een financiële instelling heeft geïmplementeerd. Het zou beter zijn geweest te beoordelen of gevallen van fraude, witwassen en terreurfondsen daarmee daadwerkelijk worden opgespoord. Hieronder zal ik beschrijven waarom dat maar moeilijk lukt, maar allereerst is het van belang om even stil te staan bij de rol van de wetgever en vooral de toezichthouders.

Doordat de toezichthouders zich willen bemoeien met de wijze waarop de regelgeving moet worden geïmplementeerd, wordt de rolverdeling tussen de financiële instellingen en de toezichthouders vertroebeld. Wanneer de toezichthouders, zoals De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM), mede bepalen hoe de uitvoering bij financiële instellingen eruit moet komen te zien, kunnen er problemen ontstaan bij het handhaven van het toezicht. Immers, wanneer de beoordeling laat zien dat er onvoldoende is gedaan bij een bank, is de toezichthouder daar medeverantwoordelijk voor. Het was voor de wetgever en de toezichthouders en (hun onafhankelijke positie) beter geweest om zich alleen bezig te houden met resultaatsverplichtingen. Door te beoordelen of fraude, witwassen en terreurfondsen werkelijk geïdentificeerd en aangepakt worden, ligt de nadruk op het resultaat en niet zozeer op de hoeveelheid geïnvesteerde tijd en geld. Nu wordt door een verplichting van de WID en KYC-aanpak het doel van de wetge-

ving uit het oog verloren. Daarmee gaat een hoop tijd en geld verloren, omdat het niet gericht is op de groep klanten die opgespoord zou moeten worden.
Bij grote (wereldwijde) financiële instellingen gaat het al snel om honderdduizenden klanten. Gezien de kosten en de grote hoeveelheden werk die daarmee gepaard gaan, is er een onvermijdelijke neiging tot standaardisatie. Procedures lijken nodig om het verzamelen van grote hoeveelheden gegevens te stroomlijnen. Daar staat echter tegenover dat standaarden en procedures zich vooral richten op de bulk van het werk, terwijl het opsporen van verdachte fondsen zich vooral zou moeten richten op uitzonderingen. Door een grootscheepse en voorspelbare aanpak ontstaat het risico dat je degenen naar wie je op zoek bent over het hoofd ziet. Daarnaast is er het risico dat degenen die niet willen opvallen al ruim van tevoren hun strategie kunnen aanpassen op de bestaande risicoprofilering en zodoende eenvoudig de dans ontspringen.

5 Kleine teams

Wat moet er dan gebeuren? Daadwerkelijk doelgericht fraude, witwassen en terreurfondsen opsporen kan het beste met kleine, flexibele teams. In plaats van de huidige grootschalige aanpak, zijn juist teams met veel knowhow nodig. Hieronder zal ik twee redenen aanvoeren ter verdediging van dit standpunt.
De eerste reden is dat criminelen zich graag verbergen achter ingewikkelde juridische constructies die niet opvallen in de massale aanpak. De tweede reden is dat de huidige controle vaak een papieren controle is, die zich richt op documenten en niet op personen. Als je personen wilt opsporen, moet je documenten als middel, maar niet als doel beschouwen.
Criminelen verbergen zich nu al achter ingewikkelde juridische constructies om niet op te vallen. Iemand met een crimineel verleden die op zwarte lijsten voorkomt, zal willen verbergen dat hij betrokken is bij een bepaalde onderneming, omdat dat zou opvallen in de programma's voor klantidentificatie. Daarom is het bij zakelijke klanten de bedoeling na te gaan welke natuurlijke personen erachter zitten. Hierbij kan gedacht worden aan de directeuren van een onderneming, maar ook aan de aandeelhouders. Soms zijn de aandeelhouders andere bedrijven, maar als dat niet enkel papieren constructies zijn, zitten in de moederbedrijven ook weer directeuren en aandeelhouders. Van alle personen die zeggenschap hebben over een bedrijf wil je kunnen nagaan of ze iets met terrorisme of fraude van doen hebben.
Het is echter moeilijk na te gaan welke personen achter een bedrijf zitten. Bij veel internationale ondernemingen zit een moederbedrijf in een ander land dan het dochterbedrijf. Dat betekent dat een zoektocht via andere bronnen (zoals lokale toezichthouders en Kamers van Koophandel) moet plaatsvinden, mogelijk in een andere taal en met andere regels. Veel bedrijven zitten om belastingtechnische redenen in landen met een streng bankgeheim (zoals Luxemburg en Zwitserland) of in landen met een gunstig, maar ondoorzichtig belastingklimaat (zoals de Kaaimaneilanden, de Kanaaleilanden en de Maagdeneilanden).
Complexe constructies en zoektochten zoals hierboven beschreven kunnen niet worden gevangen in gestandaardiseerde opsporingsprocedures. Gezien de benodigde knowhow en flexibiliteit zouden kleinschalige teams veel gerichter te werk kunnen gaan.
Kleine, hoogwaardige teams kunnen ook voorkomen dat de identificatie vooral een papieren controle is. Immers, hoewel de programma's voor klantidentificatie er vooral op zijn gericht om verdachte personen te vinden, vindt de huidige profilering plaats op basis van documenten. Dit is een indirecte vorm van controle, want in plaats van de integriteit van een persoon te controleren, wordt nu de integriteit van een document gecontroleerd. Hierbij kunnen twee dingen misgaan: er kan geknoeid worden met de integriteit van het document of er kan geknoeid worden met de link tussen het document en de persoon die erbij hoort.
Het eerste probleem, knoeien met documenten, komt regelmatig voor bij internationale criminaliteit en terrorisme. Personen gebruiken meerdere paspoorten en aliassen. Documenten worden van moeilijk te vervalsen kenmerken voorzien, zoals grafische trucjes, watermerken, hologrammen en zegels. Het onderscheiden van echte en valse documenten vereist wel dat controleurs voortdurend getraind worden in deze steeds complexer wordende kenmerken.
Het tweede probleem, knoeien met de link tussen persoon en document, komt ook steeds vaker voor. Dit is een van de redenen dat paspoorten tegenwoordig van biometrie worden voorzien. Door lichaamskenmerken van een persoon in een identiteitsdocument te verwerken wordt de link tussen persoon en document verstevigd. Zo wordt het moeilijk voor mensen om zich te verschuilen achter documenten.

6 Conclusie

Veel gegevens verzamelen over klanten en fondsen betekent niet automatisch dat ook de fraude, witwassen en terreurfondsen blootgelegd worden. Gewoonlijk wordt minder dan één op de duizend

klanten verdacht van witwassen, fraude of het financieren van terreur, zodat we kunnen spreken van het zoeken naar een speld in een hooiberg. De regelgeving schrijft een generieke aanpak voor, waarbij alle klanten en fondsen gescreend worden. Dit betekent dus veel werk waarbij relatief weinig gevonden wordt. In plaats van zoveel tijd, werk en geld te stoppen in het profileren van iedereen, verdient het aanbeveling veel gerichter te zoeken naar opvallende patronen en kenmerken.

Bij de huidige generieke aanpak van risicoprofilering zullen kwaadwillenden snel doorhebben wat ze moeten doen om niet op te vallen. Er zullen een aantal mensen door de mand vallen, maar als blijkt waardoor, zullen anderen proberen de risicovolle eigenschappen te verbergen. Opsporing is immers een kat-en-muisspel waarbij spelers proberen om elkaar te slim af te zijn. Nu is het opstellen van risicoprofielen een statisch gebeuren: eenmaal vastgestelde risico's worden niet meer geëvalueerd. Het zou echter beter zijn om de risico's voortdurend te blijven monitoren, omdat risico's steeds veranderen. Om dat spel te winnen past een ad hoc benadering met creativiteit en flexibiliteit beter dan een generieke en voorspelbare aanpak.

In plaats van een gestandaardiseerde aanpak en procedures is het beter om kleine hoogwaardige teams gericht te laten zoeken. Daarbij kunnen zoekprofielen worden opgesteld aan de hand van verdachte of risicovolle eigenschappen. Daarbij worden gevallen van fraude, witwassen of terreurfondsen uit het verleden onderzocht op gemeenschappelijke eigenschappen. Dit gebeurt ten opzichte van een controlegroep, deze eigenschappen dienen discriminatoir te zijn: de eigenschappen dienen afwezig te zijn bij gevallen waar aantoonbaar geen sprake was van fraude, witwassen of terreurfondsen. Merk op dat dit voor terreurfondsen enigszins lastig kan zijn, omdat daarvan tot op heden nog relatief weinig gevallen bekend zijn. Zulke zoekprofielen, gecombineerd met de juiste expertise (op het gebied van opsporing en vervolging maar ook specifiek op het gebied van fraude, terreur en witwassen), kunnen vervolgens aanleiding zijn om verdachte klanten nader te bekijken. In tegenstelling tot het richten van aandacht op alle klanten, wordt daarmee de focus gelegd op een klein percentage klanten dat werkelijk relevant is als het gaat om terreurfondsen, witwassen en fraude. ■

Literatuur

Comptroller's Handbook (2000), *Bank Secrecy Act/Anti-Money Laundering,* Comptroller of the Currency, Administrator of National Banks, US Department of the Treasury.

Custers. B.H.M. (2005), Pak terreurgeld aan, maar doe het goed, *Trouw,* 3 maart 2005, p. 11.

Dorresteijn, A.F.M., en R.H. van het Kaar (2003), *De juridische organisatie van de onderneming,* Deventer: Kluwer.

Faber, W., en A.A.A. Nunen (2004), *Uit onverdachte bron; evaluatie van de keten ongebruikelijke transacties,* WODC Onderzoek en Beleid, Den Haag: Boom Juridische Uitgevers.

Piatetsky-Shapiro, G., en W.J. Frawley (1993), *Knowledge Discovery in Databases,* Menlo Park, California: AAAI Press/The MIT Press.

Simpson, G. R. (2005), How Top Dutch Bank Plunged Into World of Shadowy Money, *Wall Street Journal,* 30th of December 2005, p. A1.

Noten

1 Voor een overzicht van de huidige sancties die de Verenigde Staten opleggen aan verschillende landen, zie: http://www.ustreas.gov/offices/enforcement/ofac/programs/

2 Voor recente versies van de lijst zie: http://www.ustreas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf