Opsporing terreurfo

Het onder meer door Amerikaanse wetgeving verplichte *Know Your Customer*-beleid van financiële instellingen is door zijn generieke benadering niet alleen inefficiënt maar ook ineffectief. Doelgericht zoeken naar verdachte klanten met behulp van risicoprofielen zou meer opleveren dan dit gezoek in een hooiberg.

BART CUSTERS*

Standaarden en procedures richten zich op de bulk van het werk, terwijl opsporen van verdachte fondsen zich zou moeten richten op uitzonderingen.

Sinds de aanslagen van 11 september 2001 is men op tal van fronten bezig het internationaal terrorisme te bestrijden. Ook het opsporen van terrorismefondsen heeft hierbij een hoge vlucht genomen. In het kader van nieuwe (voornamelijk Amerikaanse) wetgeving zijn financiële instellingen 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 gehele proces staat bekend als Know Your Customer (KYC), waarvan delen in Nederland zijn ingevoerd in de Wet identificatie bij dienstverlening (WID). KYC en WID verplichten onder meer banken, verzekeraars, notarissen en openbare accountants om hun klanten te identificeren en ongebruikelijke transacties te melden, teneinde witwaspraktijken en terreurfondsen op te sporen.

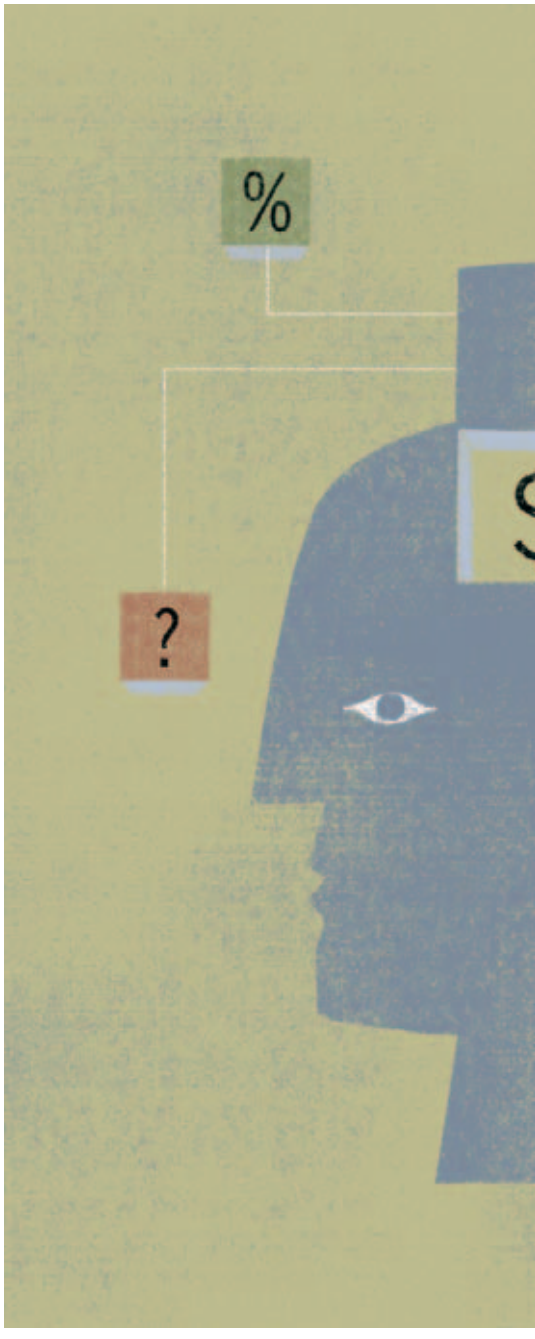

FOTO: CORBIS

Patriot Act

Een Know Your Customer-beleid is erop gericht een klanten identificatieprogramma in te stellen zoals dat verplicht is onder de Amerikaanse Bank Secrecy Act (BSA) en de Patriot Act. Die eerste wet dateert van 1970 en verplicht financiële instellingen medewerking te verlenen aan overheidsinstanties die witwaspraktijken opsporen. Het gaat dan vooral om het melden van omvangrijke of ongebruikelijke transacties en van activiteiten die duiden op witwassen, belastingontduiking of criminele activiteiten. De Patriot Act dateert van oktober 2001, vlak na de aanslagen op het World Trade Center en het Pentagon. Deze wet verruimt de bevoegdheden van Amerikaanse opsporingsdiensten aanzienlijk en voorziet daarnaast in aanpassingen in regelgeving op het gebied van immigratie, paspoortvereisten en witwaspraktijken.

Wereldwijde werking

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. Het intrekken van een bankvergunning is daarbij de ultieme sanctie, maar ook kunnen

ndsen **kan slimmer**

boetes worden opgelegd. Dat dit een reëel risico is, mag blijken uit het feit dat in 2005 een grote Nederlandse bank (ABN AMRO, red.) een boete van miljoenen dollars kreeg vanwege verboden transacties met Iran en Libië.

De Amerikaanse wetgeving legt indirect ook KYC-verplichtingen op aan andere landen.

Grote internationale banken weten niet altijd hoeveel klanten ze werkelijk hebben.

Risicoanalyses: alle klanten

In de praktijk betekent het implementeren van een KYC-beleid voor een financiële instelling dat er risicoanalyses moeten komen van alle bestaande en nieuwe klanten. Gewoonlijk bestaat dit uit het in kaart brengen van een aantal karakteristieken van de klant, bijbehorend bewijsmateriaal hierover verzamelen en, tenslotte, aan het geheel door een weging een oordeel toekennen.

Bij klanteigenschappen kan onder meer worden gedacht aan personalia, kredietwaardigheid, aantal en typen rekeningen, feiten van fraude/criminaliteit uit het verleden. De bewijsvoering bestaat gewoonlijk uit kopieën van paspoorten en andere documenten, zoals verklaringen van goed gedrag.

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, Kamer van Koophandel, financiële autoriteit of een lokale overheid. Uitreksels van handelsregisters, documenten van toezichthouders, jaarverslagen met accountantsverklaring, oprichtingsaktes en dergelijke, zorgen in dit geval voor de bewijsvoering.

Risicovolle factoren

Het vaststellen van het risico is uiteindelijk een weging van deze karakteristieken. Verscheidene eigenschappen worden als risicovol gezien:

- *Locatie*: landen als Irak, Somalië of Noord-Korea gelden als zeer risicovol, omdat er weinig of geen toezicht is op natuurlijke en rechtspersonen. Hetzelfde geldt, in mindere mate, voor landen als Rusland en India. Daarnaast zijn er landen waarmee de Amerikaanse overheid handel verbiedt, zoals Cuba en Iran.
- *Handelsactiviteiten*: bepaalde handelsactiviteiten zijn gevoelig voor witwaspraktijken en terreurfondsen. Voorbeelden zijn casino's, wisselkantoren en diamanthandels.
- *Bedrijfsvorm*: zogeheten postbusbedrijven - papieren constructies waar geen bedrijfsactiviteiten plaatsvinden - zijn vaak opgericht om belastingtechnische redenen. Deze constructies kunnen ondoorzichtig zijn als vastgesteld moet worden wie de directeuren of eigenaren zijn.
- *Aanwezigheid op zwarte lijsten*: als directeuren, aandeelhouders of eigenaren voorkomen op zwarte lijsten kan dit een verhoogd risico betekenen of leiden tot een verbod van een transactie. Er zijn talloze zwarte lijsten, waaronder die van de Amerikaanse Office of Foreign Assets Control (OFAC), de FBI (*most wanted*) en Europol, de EU-lijst met terroristische organisaties. Ook koppeling met kredietwaardigheidlijsten is mogelijk (in Nederland bij het Bureau Kredietregistratie).

Risicoverlagend

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

Op basis van de weging van alle factoren komt men tot een risicoschatting van een klant,

Gewoonlijk wordt minder dan één op de duizend klanten verdacht van witwassen, fraude of het financieren van terreur.

een soort rapportcijfer. Een verhoogd risico kan reden zijn om een klant beter in de gaten te houden of - bij een onacceptabel hoog risico - er niet langer zaken mee te doen.

Problemen in uitvoering

In de praktijk is het uitvoeren van de hiervoor beschreven regelgeving weerbarstig. Vooral de generieke benadering maakt een KYC-beleid al snel onvoldoende effectief en efficiënt - waarbij niet doelgericht wordt gezocht naar verdachte klanten. Hier onder volgt een aantal concrete problemen.

Onduidelijke scope

Grote internationale banken weten niet altijd hoeveel klanten ze werkelijk hebben. Omdat ze vaak zijn gegroeid via overnames en fusies, hebben ze vaak verschillende klantenbestanden die niet eenvoudig kunnen worden samengevoegd. Het kan gaan om tientallen informatiesystemen met in totaal honderdduizenden of zelfs miljoenen klanten. Klanten staan dan gefragmenteerd geregistreerd, waarbij er bovendien veel overlap aanwezig kan zijn.

Identificatieproblemen

Wanneer weet je of je de juiste persoon voor je hebt? Als in het ene bestand een mevrouw De Vries wordt genoemd, en in het andere bestand een mevrouw Jansen-De Vries, is niet duidelijk of het om dezelfde persoon gaat. Is het adres hetzelfde, dan is aannemelijk dat mevrouw De Vries in de tussentijd getrouwd is, maar dat staat niet zonder meer vast. De waarschijnlijkheid neemt echter toe, naarmate meer karakteristieken (bijvoorbeeld geboortedatum, telefoonnummer, sofinummer) hetzelfde zijn. Met behulp van technische methoden kan op basis van overlap in gegevens, met bepaalde waarschijnlijkheid worden vastgesteld of het in zulke gevallen om dezelfde identiteit gaat. Bijvoorbeeld met Entity Analytics Solutions (EAS) van IBM, dat onder meer wordt gebruikt door de Amerikaanse veiligheidsdiensten.

Personen achter organisaties

Uiteindelijk is het de bedoeling om bij zakelijke klanten na te gaan welke natuurlijke personen er achter zitten, directeuren, maar ook aandeelhouders. Soms zijn de aandeelhouders andere bedrijven, maar als dat niet louter papieren constructies zijn, zitten in de moederbedrijven ook weer directeuren en aandeelhouders.
Bij veel internationale ondernemingen zit een moederbedrijf echter in een ander land.
Dat betekent een zoektocht via andere bronnen (zoals lokale toezichthouders en kamers van koophandel), mogelijk in een andere taal en met andere regels, bijvoorbeeld een streng bankgeheim (zoals Luxemburg en Zwitserland) of een gunstig maar ondoorzichtig belastingklimaat (zoals de Kaaimaneilanden, Kanaaleilanden en Maagdeneilanden).

Standaardisatie

Bij grote (wereldwijde) financiële instellingen gaat het bij het opstellen van risicoprofielen al snel om honderdduizenden klanten. Gezien de kosten is er daarbij een onvermijdelijke neiging tot standaardisatie en procedures om het verzamelen van grote hoeveelheden gegevens te stroomlijnen. Standaarden en procedures richten zich echter vooral op de bulk van het werk, terwijl het opsporen van verdachte fondsen zich juist vooral zou moeten richten op uitzonderingen. Een grootscheepse en voorspelbare aanpak schept het risico dat je degenen naar wie je op zoek bent over het hoofd ziet. Daarnaast kunnen degenen die niet willen opvallen, al ruim van tevoren hun strategie aanpassen op de bestaande risicoprofilering en zodoende makkelijk de dans ontspringen.

Controle op documenten, niet op personen

Hoewel een KYC-beleid erop is gericht verdachte personen te vinden, vindt de huidige profilering plaats op basis van documenten. Dit is een indirecte vorm van controle. Hierbij kunnen twee dingen misgaan: er kan worden geknoeid met de integriteit van het document, of met de link tussen het document en de persoon die erbij hoort. Knoeien met documenten komt regelmatig voor bij internationale criminaliteit en terrorisme. Personen gebruiken meerdere paspoorten en aliassen. Knoeien met de link tussen persoon en document, komt ook steeds vaker voor. Dit is een van de redenen waarom paspoorten tegenwoordig van biometrie worden voorzien. Door lichaamskenmerken in een identiteitsdocument te verwerken wordt de link tussen persoon en document verstevigd.

Speld in hooiberg

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 door Know Your Customer-regelgeving voorgeschreven generieke aanpak, waarbij alle klanten en fondsen worden gescreend, betekent dus veel werk waarbij relatief weinig wordt gevonden.
In plaats van zoveel tijd, werk en geld te stoppen in het profileren van iedereen, zou het beter zijn gerichter te zoeken naar opvallende patronen en kenmerken. Alleen al door slim te zoeken wordt het opsporen van terreurfondsen efficiënter.
Een gerichte aanpak zal ook effectiever zijn omdat kwaadwillenden zullen proberen hun risicovolle eigenschappen te verbergen.
Opsporing is een kat-en-muisspel waarbij spelers proberen elkaar te slim af te zijn. Om dat spel te winnen past een ad hoc benadering met creativiteit en flexibiliteit beter dan de huidige generieke en voorspelbare aanpak.

Om het kat-en-muisspel te winnen past een ad hoc benadering met creativiteit en flexibiliteit beter.

Zoekprofielen

Wat zou er dan moeten gebeuren? Het verdient aanbeveling eerst zoekprofielen op te stellen aan de hand van verdachte of risicovolle eigenschappen. Risicovolle eigenschappen kunnen bijvoorbeeld blijken uit eerdere casussen waarin terreurfondsen werden aangetroffen. Met die profielen kan vervolgens worden bekeken welke klanten verdacht lijken. Deze verdachten en personen om hen heen kunnen vervolgens aan een nader onderzoek worden onderworpen.
Door de vraag te stellen 'wie kent wie?' kunnen netwerken van personen in kaart worden gebracht.
In tegenstelling tot het richten van aandacht op alle klanten, wordt daarmee de focus gelegd op een klein percentage klanten. Precies het deel van de klanten dat werkelijk relevant is als het gaat om terreurfondsen. ■

Noot

* Bart Custers is consultant bij Capgemini en gespecialiseerd in risicoprofilering. Hij schreef hierover het boek *The Power of Knowledge* en adviseerde onder meer een grote bank bij het uitwerken van de procedures voor risicoprofilering en het opzetten van een expertisecentrum op te zetten.