

Toezicht expertisecentra
Trustkantoren en betaalinstellingen

Amsterdam
Postbus 98
1000 AB Amsterdam

Datum
24 maart 2011
Uw kenmerk

Ons kenmerk
2011/15664
Behandeld door
Dekker, L.A.M. (mw) RE CISA
Doorkiesnummer
020 524 1985
Bijlage(n)

Onderwerp

Circulaire van De Nederlandsche Bank NV (DNB) voor betaalinstellingen die money transfers verrichten, d.d. 24 maart 2011

Geachte

1. INLEIDING

Deze circulaire is bedoeld voor (buitenlandse) betaalinstellingen die money transfers uitvoeren in Nederland. Wij vragen u uw agenten en bijkantoren in Nederland te informeren over de inhoud van deze brief.

Het aanbieden van money transfers brengt hoge risico's met zich mee. Een betaalinstelling kan (ongewild) betrokken raken bij het witwassen van geld of bij de financiering van terrorisme. Het grote aantal transacties en de vele, wisselende opdrachtgevers verhogen dit risico.

Om misbruik van money transfers door criminelen te voorkomen, is het Financieel Expertise Centrum (FEC) begin 2010 het project 'Misbruik money transfers' gestart.¹ De FEC-partners hebben binnen dit project allerlei maatregelen voorgesteld.

In deze brief gaan we in op drie belangrijke maatregelen. DNB geeft u hiermee richtlijnen om te voorkomen dat uw betaalinstelling onbedoeld betrokken raakt bij het witwassen van geld of bij de financiering van terrorisme. DNB zal in haar toezicht op betaalinstellingen extra letten op deze maatregelen en toetsen hoe zij in de organisatie worden toegepast. Deze maatregelen vloeien voort uit artikel 3 en artikel 35 van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en hebben te maken met:

¹ Het FEC is een samenwerkingsverband van DNB, AFM, politie, Belastingdienst, FIOD, Openbaar Ministerie en AIVD. Het Ministerie van Veiligheid en Justitie en het Ministerie van Financiën nemen in het FEC deel als waarnemers. Meer informatie over het FEC vindt u op www.fec-partners.nl

- 1) het goed opleiden van medewerkers;
- 2) het uitvoeren van doeltreffende transactieanalyses;
- 3) het verbeteren van de datakwaliteit

In paragraaf 2 gaan we in op het onderdeel 'opleiding' en in paragraaf 3 op de onderdelen 'transactieanalyses' en 'datakwaliteit'.

2 OPLEIDING

Een betaalinstelling **moet**-op grond van artikel 35 van de Wwft-ervoor zorgen dat werknemers, voor zover relevant voor de uitoefening van hun taken, op de hoogte zijn van de bepalingen uit de Wwft en opleidingen krijgen waardoor zij ongebruikelijke transacties leren te herkennen.

DNB is ook van mening dat door een juiste scholing meer ongebruikelijke transacties herkend kunnen worden. Betaalinstellingen moeten daarom onderstaande richtlijnen volgen:

1. De instelling maakt voor elke medewerker een opleidingsplan-op-maat. In dit plan staan gegevens over nog te volgen en gevolgde opleidingen (Wanneer vonden zij plaats? Wat waren de resultaten?).
2. Voordat een nieuwe medewerker aan de slag kan gaan, moet hij of zij alle noodzakelijke opleidingen hebben gevolgd. Dit wordt in het opleidingsplan vastgelegd.
3. Iemand moet niet alleen op de hoogte zijn van de bepalingen uit de Wwft, maar dit ook blijven. Periodieke bijscholing is daarom nodig. Ook de planning en de afronding van deze bijscholing wordt in het opleidingsplan vastgelegd.
4. De betaalinstelling (de interne controle) toetst periodiek of aan bovenstaande voorwaarden is voldaan.

DNB is van mening dat met behulp van bovenstaande punten een instelling een goede invulling kan geven aan artikel 35 van de Wwft. Dit is niet de enige manier: het is aan de instelling om aan te tonen dat zij aan de richtlijn voldoet. Bijvoorbeeld door kasbaliemedewerkers feedback te geven naar aanleiding van resultaten van interne controles. Ook dit kan immers helpen om de kennis van medewerkers te vergroten. Om dit aan te tonen is een goede vastlegging onontbeerlijk.

3 TRANSACTIEANALYSES

Op grond van artikel 13 van de Wwft moet een instelling ter voorkoming van witwassen en financieren van terrorisme cliëntenonderzoek verrichten. Zo kunnen geldstromen beter in de gaten worden gehouden, zodat ongebruikelijke transacties sneller zijn te herkennen.

DNB vindt dat een aantal betaalinstellingen de transactieanalyses te beperkt uitvoert. Uit een steekproef van DNB blijkt dat een aanzienlijk deel van de transacties (20 tot 45 procent, afhankelijk van de vestigingslocatie) tot netwerken behoren die aanvullend onderzoek nodig hebben. Vaak worden deze transacties ten onrechte niet als ongebruikelijk aangemerkt. Als

gevolg hiervan kan een betaalinstelling:

- onvolledige (subjectieve) meldingen verrichten aan de FIU-NL;
- transacties toestaan die geweigerd hadden moeten worden, zodat zij betrokken kan raken bij witwassen;
- onvoldoende klantonderzoek verrichten ('Know your customer').

DNB verwacht van betaalinstellingen dat zij periodiek analyses uitvoeren om een beter beeld te krijgen van ongebruikelijke transacties. Zo kunnen zij beter passende maatregelen nemen. DNB vindt dat een betaalinstelling minimaal de analyses uit de volgende paragraaf moeten uitvoeren.

3.1 Standaard transactieanalyses

DNB zal bij haar toezichtbezoeken de uitkomsten willen bespreken van de transactieanalyses die de betaalinstellingen uitvoeren, en let daarbij op de onderstaande punten:

Send-transacties

- selectie op de zender vanuit Nederland;
- selectie op de ontvanger in het buitenland.

Receive-transacties

- selectie op de ontvanger in Nederland;
- selectie op de zender in het buitenland.

Wanneer moet u transactie uitvoeren:

- Op maandbasis: transacties van de laatste maand.
- Op kwartaalbasis: transacties over het laatste kwartaal.
- Op jaarbasis: transacties over het laatste jaar.

Deze selecties vansend-en receive-transacties kunnen helpen in een onderzoek naar verdachte money transfers. Bij kleine instellingen volstaat meestal een top-10 per categorie, en bij grote kantoren een top-50. De omvang van deze selectie blijft de eigen verantwoordelijkheid van een instelling.

DNB vindt het belangrijk om de belangrijkste (grote) Nederlandse en buitenlandse cliënten in beeld te krijgen en een nader cliëntenonderzoek uit te voeren. Een instelling moet nagaan of zij over voldoende informatie beschikt over de herkomst en bestemming van het geld. Als dit niet het geval is, of bij twijfel, moet een instelling passende maatregelen treffen. Denk bijvoorbeeld aan het instrueren van de kassiers om de cliënt bij een volgend bezoek te bevragen over de herkomst en de bestemming van het geld. Hierbij kan de kassier de cliënt verplichten documenten te laten zien, zoals een uittreksel van de Kamer van Koophandel of een factuur.

Als een zender of een ontvanger vanuit het buitenland grote bedragen verstuurt of ontvangt, zal het onderzoek zich meestal richten op de Nederlandse cliënten die met deze persoon zaken doen. Dit omdat betaalinstellingen in Nederland in de meeste gevallen geen achterliggende informatie kunnen krijgen van zenders en ontvangers in het buitenland.

Alle hierboven genoemde maatregelen beschouwt DNB als het minimumniveau. DNB verwacht dat een betaalinstelling, atbankelijk van het aantal transacties en het soort risico, aanvullend onderzoek uitvoert. Zoals onderzoeken over:

- specifieke gebieden c.q. landen (corridoronderzoeken);
- transacties op adressen van Nederlandse klanten (de adressen op hun bestaan controleren en op meervoudig gebruik van deze adressen);
- transacties juist onder de objectieve meldgrens (het zogenoemde smurfen);
- afzetpunten;
- de verhouding tussen send-/receive-transacties;
- transacties binnen Nederland dan wel Europa;
- doormeldingen;
- netwerkanalyses. Netwerkanalysetools kunnen bij middelgrote en grote betaalinstellingen van toegevoegde waarde zijn. Via deze applicaties kunnen op een eenvoudige manier netwerken van transacties in kaart worden gebracht om zo mogelijk misbruik aan te tonen.

DNB zal de uitkomsten van deze onderzoeken met de instelling bespreken en verwacht daarom ook dat instellingen transactieanalyses vastleggen zodat deze beschikbaar zijn als DNB hier om vraagt.

Leiden de uitkomsten van transactieanalyses tot grote hoeveelheden ongebruikelijke transacties? Neem dan contact op met uw contactpersoon bij de FIU-NL om te bespreken hoe u deze transacties moet melden.

3.2 Datakwaliteit

Een goede kwaliteit van (bron)data is een voorwaarde om transacties goed te kunnen monitoren en analyseren. Het is noodzakelijk dat de invoer van de klant- en transactiegegevens nauwkeurig, compleet en steeds op dezelfde manier gebeurt. DNB verwacht bijvoorbeeld dat instellingen de identiteitsdocumenten van klanten juist en volledig invoeren en dat zij aandacht besteden aan de datakwaliteit. Ook verwacht DNB dat betaalinstellingen een beeld hebben van de kwaliteit van hun brongegevens en van de verbeteringen die nog nodig zijn om op een doeltreffende manier transacties te kunnen analyseren.

Hieronder vindt u een aantal richtlijnen om de datakwaliteit te verbeteren:

- Landencode: gebruik ISO-landcodes (ISO 3166-1-alpha-2 zie: http://www.iso.org/iso/english_country_names_and_code_elements).
- Adres cliënt: vraag de klant naar de postcode en voer deze in op <http://www11.IJOSTcode.nl/> om de bijbehorende straatnaam te kopiëren en te plakken.
- Naam cliënt: voer de achternaam met hoofdletters en de voornaam(en) met kleine letters in. In het geval van transactieanalyses kunnen de achternaam en de voornaam(en) zo eenvoudig van elkaar worden onderscheiden.
- Transactiedatum: Voor de invoering van de send-/receive-datum raden wij u aan het volgende format te gebruiken: dd-mm-jlU. Bijvoorbeeld: 01-03-2011.

Datum
24 maart 2011
Bladnummer
5
Ons kenmerk
2011115664

4 TOTSLOT

Het monitoren van de geldstromen binnen de markt van money transfers acht DNB van groot belang in de strijd tegen het witwassen. Binnenkort zal DNB om die reden beginnen met het analyseren van de transactiegegevens van de markt. Op korte termijn zult u een brief ontvangen waarin u verzocht wordt de transactiegegevens over het eerste kwartaal van 2011 te rapporteren aan DNB.

Mocht u naar aanleiding van bovenstaande vragen hebben dan kunt u contact opnemen met de heer A.G. Sonnevile RA onder het in de aanhef vermelde telefoonnummer.