Gambling & Gaming
Good Practices Betaalinstellingen

DeNederlandscheBank
EUROSYSTEEM

Disclaimer

Deze good practice geeft niet-verplichtende aanbevelingen voor de toepassing van de Wft en de Wwft aan betaalinstellingen die merchants bedienen in de Gambling & Gaming sector. Met behulp van deze good practice draagt DNB haar opvattingen uit over de door haar geconstateerde of verwachte gedragingen in de beleidspraktijk, die naar haar oordeel een goede toepassing inhouden van de regels waarop deze good practice betrekking heeft.

Met deze good practice beoogt DNB te bereiken dat betaalinstellingen met merchants in de Gambling & Gaming sector het daarin gestelde, de eigen omstandigheden in aanmerking nemende, in hun afweging betrekken, zonder dat zij verplicht zijn dat te doen. De good practice geeft inzicht in de door DNB geconstateerde of te verwachten gedraging in de beleidspraktijk, is indicatief van aard en sluit daarmee niet uit dat voor instellingen een afwijkend, al dan niet strengere toepassing van de onderliggende regels geboden is. De afweging betreffende de toepassing berust bij deze instellingen zelf.

Inleiding

Met deze Good Practice wil De Nederlandsche Bank N.V. (DNB) betaalinstellingen[1] handvaten bieden voor de beheersing van risico's met betrekking tot verlenen van diensten aan aanbieders van kansspelen op afstand (online gokwebsites)[2] en/ of aanbieders van online gamewebsites (hierna tezamen: **Gambling & Gaming**).

DNB heeft in 2021 een thema-onderzoek uitgevoerd naar betaalinstellingen die betaaldiensten aanbieden aan merchants in de Gambling & Gaming sector. Hiertoe zijn een negental betaalinstellingen geselecteerd die merchants bedienen die actief zijn in de Gambling & Gaming sector. Het onderzoek heeft zich met name gericht op de beheersmaatregelen die betaalinstellingen treffen ten aanzien van de dienstverlening aan merchants in de Gambling & Gaming sector. Een aantal betaalinstellingen is vervolgens geselecteerd voor een verdiepend onderzoek (desk-based).

Risicobeheersing vergt altijd maatwerk. Dit geldt ook voor de risico's die gepaard gaan met Gambling & Gaming. De voorbeelden in deze Good Practice zullen vaak, maar niet altijd direct bruikbaar zijn voor elke instelling.

Relevante wet- en regelgeving

Betaalinstellingen dienen (onder meer) aan onderstaande wettelijke verplichtingen te voldoen die betrekking hebben op de beheersing van risico's op witwassen en financieren van terrorisme. Deze Good Practice ziet op een nadere (niet-bindende) invulling hiervan voor betaalinstellingen die merchants bedienen in de Gambling & Gaming sector.

- Integere en beheerste bedrijfsvoering (art. 3:10 Wet op het financieel toezicht (Wft) jo 3:17 Wft jo art. 10 en 17 Besluit prudentiële regels Wft (Bpr));
- Maatregelen om de risico's op witwassen en financieren van terrorisme vast te stellen en te beoordelen (door middel van de SIRA (art. 2b Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft));
- Gedragslijnen, procedures en maatregelen om de risico's op witwassen en financieren van terrorisme en de risico's die zijn geïdentificeerd in de meest recente versies van de supranationale risicobeoordeling (SNRA) en de nationale risicobeoordeling (NRA) te beperken en effectief te beheersen (artikel 2c Wwft);
- Cliëntenonderzoek (art. 3, 8 en 9 Wwft);
- Transactiemonitoring (art. 2a en art. 3, tweede lid, aanhef en onder d, van de Wwft);
- Melden ongebruikelijke transacties (art. 16 Wwft).

1 Deze Good Practice kan mogelijk ook relevant zijn voor overige betaaldienstverleners.
2 Per 1 oktober 2021 is een aanbieder van online kansspelen verplicht om op grond van artikel 31a van de Wet op de kansspelen een KOA-vergunning aan te vragen voor het aanbieden van diensten in Nederland. Een legale aanbieder staat onder toezicht van de Kansspelautoriteit.

Inhoud

Integriteitsrisico's bij Gambling & Gaming

Gambling brengt een verhoogd inherent risico met zich mee op witwassen en financiering van terrorisme.[3] Voorbeelden van risico's die verband houden met de aard van de dienstverlening zijn onder andere een veelvoud aan transacties, de hoogte van de transacties en de omloopsnelheid van het geld. Ook bij gaming bestaat het risico op witwassen. Het Anti Money Laundering Centre heeft een aantal voorbeelden genoemd ten aanzien van het risico op witwassen[4] bij Gambling & Gaming.[5]

Gambling

Bij Gambling bestaat het risico op witwassen. De herkomst van geld kan gemaskeerd worden, door illegaal geld als inleg te gebruiken en via een gokplatform wit te wassen. Elementen van online Gambling die dit mogelijk maken zijn bijvoorbeeld:

- Het gebruik van anonieme betaalmethoden (credit- en debet kaarten, prepaidkaarten, cheques en cryptocurrencies) waarmee de inleg op de speelaccounts gevoed wordt (enkel bij illegale aanbieders).
- Geld gaat van een betaalrekening naar de spelersrekening (speelaccount).[6] Vervolgens wordt het geld ingezet waarna eventueel speelwinst volgt. Deze winst wordt uitbetaald op de speelrekening (speelaccount). Vervolgens kan dat weer worden uitbetaald op een betaalrekening. In de methode die zojuist is beschreven, is er vanuit gegaan dat de speler zeer beperkt of zelfs helemaal niet speelt met zijn gelden.
- Spelers kunnen onderlinge afspraken maken waarbij één speler opzettelijk verliest ten bate van de andere speler. Het geld wordt dan uitbetaald op het account van de winnende speler.
- Een speelaccount kan worden gebruikt voor betaling van illegale transacties. Bijvoorbeeld door een player to player transfer waarbij geld wordt verplaatst van het ene speelaccount naar het andere speler account zonder daadwerkelijk te spelen. De verkoper laat zich vervolgens uitbetalen van zijn speelaccount naar zijn betaalrekening (dit betreffen geen gokwinsten, maar bijvoorbeeld opbrengsten van verkoop van goederen) (enkel bij illegale aanbieders).
- Een speelaccount kan bij een aanbieder worden gebruikt om gelden op te slaan en zo te verbergen voor de autoriteiten.

3 EBA/GL/2021/02, 1 maart 2021, GL 9.6, 10.4, 12.5.
4 Loterijen vormen een laag witwasrisico. https://www.rijksoverheid.nl/documenten/kamerstukken/2021/01/27/bijlage-1-vervolgonderzoek-naar-risicos-witwassen-en-terrorismefinanciering-bij-aanbieders-in-de-kansspelsector-die-vrijgesteld-worden-van-de-verplichtingen-van-de-wwft.
5 https://www.amlc.nl/online-gokken-als-witwasmethodiek/ https://www.amlc.nl/online-games-en-witwassen/.
6 Fraude met spelerstegoeden geven tevens mogelijk aanleiding voor een kansspelaanbieder om een incident te melden ingevolge de de Beleidsregels van de raad van bestuur van de Kansspelautoriteit inzake informatieplicht van vergunninghouders.

Gaming

Ook bij Gaming bestaat het risico op witwassen. Vanwege de grote hoeveelheden geld die omgaan in de online Gaming wereld kan de markt aantrekkelijk zijn voor criminelen. Bij online Gaming is het tijdverdrijf belangrijker dan het verdienen van geld. In de online games spelen "waarden" een belangrijke rol. Waarden kunnen bijvoorbeeld toegang geven tot een hoger level of men kan hiermee aankopen doen van spelonderdelen. Deze waarden worden onder andere verdiend in de game door opdrachten uit te voeren of ze aan te kopen. Deze waarden kunnen ook non-convertible virtual currencies worden genoemd.[7]

- Er bestaan verschillende online ruilplatforms (Real Money Trading) waar spelwaarden onderling kunnen worden geruild of kunnen worden aangekocht of verkocht in ruil voor geld.
- Verkoop van spelwaarden vindt steeds vaker plaats via anonieme betaalmethoden.
- Meerdere manieren zijn mogelijk om geld wit te wassen of gelden te ontvreemden. Criminelen kunnen bijvoorbeeld toegang verkrijgen tot een computer en de game door bijvoorbeeld phishing en het hacken van de PC. Hierdoor verkrijgen ze toegang tot een spel en de gegevens van de speler.
  - De bankrekening van de speler die gekoppeld is aan het speelaccount kan worden leeggehaald door aankopen te doen (speelwaarden voor een game en deze door te verkopen aan ruilplatforms).
  - De rekening kan worden gebruikt voor het doorstorten van illegale gelden. Daarnaast kunnen criminelen speelwaarden dupliceren en deze herhaaldelijk door verkopen of zelf games ontwikkelen en exploiteren.

7 https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Risico's Gambling & Gaming voor betaalinstellingen

Aangezien de geldstromen van Gambling & Gaming merchants over de rekeningen van betaalinstellingen lopen, wordt van betaalinstellingen verwacht dat zij de bijbehorende risico's adequaat beheersen. De betaalinstelling fungeert als poortwachter.

In het themaonderzoek is zowel de Gambling sector als de Gaming sector onderzocht. In de praktijk komen deze sectoren namelijk vaak samen voor. Zo kunnen Gaming merchants elementen van Gambling bevatten (kansspelelement). In zulke gevallen doen zich andere risico's voor dan wanneer het enkel Gaming betreft. Het hieraan gerelateerde cliëntenonderzoek en transactiemonitoring zal voor Gambling & Gaming merchants ook andere elementen kunnen vereisen en zal hierop moeten worden aangepast. DNB benadrukt in dit verband dat van betaalinstellingen wordt verwacht dat zij bij het analyseren van hun merchants een duidelijk onderscheid maken tussen Gambling en Gaming merchants en deze als zodanig rapporteren in de jaarlijkse Integriteitsrisicoanalyse (IRAP).

SIRA

Op grond van artikel 2b Wwft moeten betaalinstellingen maatregelen nemen om hun risico's op witwassen en financieren van terrorisme vast te stellen en te beoordelen. In dat kader wordt van betaalinstellingen die klanten bedienen in de Gaming & Gambling sector verwacht dat ze in de Systematische Integriteitsrisico analyse (SIRA) de risico's die samenhangen met deze sectoren inzichtelijk maken, bijvoorbeeld door scenario's op te nemen die de risico's die kenmerkend zijn voor deze sector adresseren. Hierbij kan worden gedacht aan:

- AML / CTF scenario's met betrekking tot risico's gelieerd aan de dienstverlening van de hoog risico sector Gambling & Gaming;

Voorbeelden van scenario's

- De betaalinstelling kan niet of onvoldoende vaststellen of uitbetalingen van de Gambling merchant de thresholds overschrijden die zijn vastgesteld.
- Het risico dat virtuele items in het spel worden aangekocht met illegaal geld. Deze virtuele items kunnen een economische waarde hebben buiten het spel.

- AML / CTF scenario's met betrekking tot risico's gelieerd aan dienstverlening aan merchants in hoog risico landen en/of met complexe structuren (gezien het feit dat dit vaker voorkomt bij Gambling & Gaming merchants);

- AML / CTF scenario's met betrekking tot risico's gelieerd aan betaalstromen en betaalmethoden;

Voorbeelden van scenario's

- De pay-in door klanten in de Gambling sector staat niet in verhouding tot de pay-out aan klanten waardoor het risico bestaat dat er wordt witgewassen.

- Gebruik van verschillende (anonieme) betaalmethoden verhoogt het risico op witwassen in de Gambling & Gaming sector.

- Scenario's met betrekking tot risico's gelieerd aan de regulering van merchants;

Voorbeelden van scenario's

- De betaalinstelling verleent diensten/ producten aan Gambling merchants die niet beschikken over een vergunning in het land waar zij haar activiteiten verrichten waardoor het risico bestaat dat de diensten/ producten voor een ander doel worden gebruikt.[8]
- De betaalinstelling levert diensten/ producten aan Gambling merchants die deze diensten gebruiken voor criminele doeleinden of kinderen als doelgroep bedienen.

Voor guidance van DNB omtrent de SIRA verwijst DNB naar: De Integriteitsrisicoanalyse- meer waar dat moet, minder waar dat kan (ook beschikbaar in het Engels).

8 Op https://kansspelautoriteit.nl/veilig-spelen/veilig-online-gokken/ kan worden gecontroleerd welke partijen een vergunning van de Ksa hebben voor aanbod in Nederland (inclusief merknamen waarmee ze opereren).

Beleid en Cliëntenonderzoek

Ingevolge artikel 2c Wwft hebben betaalinstellingen beleid opgesteld voor de beheersing van risico's op witwassen en financieren van terrorisme. Voor de uitwerking van dit beleid met betrekking tot Gaming & Gambling merchants kunnen onderstaande aandachtpunten worden opgenomen die zien op de uitvoering van het cliëntenonderzoek in gevolge artikel 3, 8 en 9 Wwft.

Voor guidance van DNB omtrent het cliëntenonderzoek verwijst DNB naar: Leidraad Wwft en Sw (ook beschikbaar in het Engels).

Good practices:

Een betaalinstelling heeft een Gambling - Gaming Policy. In de policy kunnen onder meer de volgende elementen worden betrokken:

- Waar de merchant actief is (in welke landen worden de online-Gambling en Gaming diensten aangeboden) en voor welk beoogd doel de betaalproducten worden gebruikt. Daarmee stelt de betaalinstelling vast of de betaalproducten enkel worden gebruikt voor de Gambling en Gaming afzetmarkt.
- De instelling verricht (nader) onderzoek indien vermoedens bestaan dat de merchant illegaal (zonder vergunning) Gambling activiteiten aanbiedt. Zo kan de instelling uitsluiten dat de dienstverlening niet wordt misbruikt voor het illegaal aanbieden van online-gokdiensten. Bij wijzigingen in de regulering (zoals intrekking van de vergunning, einddatum van de vergunning etc.) handelt de betaalinstelling adequaat en blokkeert de instelling onder andere de pay-in en pay-out betalingen.
- De Gambling-vergunning wordt (periodiek) opgevraagd en gevalideerd aan de hand van bijvoorbeeld de vergunningen registers. Aan de hand van de Gambling-vergunning wordt gecontroleerd of de landen waar de kansspelen worden aangeboden binnen de geografische reikwijdte van de Gambling-vergunning vallen. Tevens wordt gecontroleerd of de kansspelen die worden aangeboden (via de website, app etc.) binnen de reikwijdte van de Gambling-vergunning vallen.
- Het AML/CTF-beleid en procedures van de merchant worden opgevraagd. De instelling controleert of de merchant beheersmaatregelen treft om ML/ TF risico's te beheersen. Zie hiervoor ook de Leidraad Wwft van de KSA - De Wwft in de kansspelsector.
- Audits/controles worden uitgevoerd op de merchant om compliance met de Wwft te waarborgen.
- Een jaarlijkse periodieke review wordt uitgevoerd op Gambling & Gaming merchants (afhankelijk van de toegekende risico-classificatie).
- Goedkeuring van hoger management bij de cliëntacceptatie en na iedere review bij Gambling & Gaming merchants.

Transactiemonitoring

Van betaalinstellingen die klanten hebben in de Gambling & Gaming sector wordt ingevolge artikel art. 2a en art. 3, tweede lid, aanhef en onder d, van de Wwft verwacht dat zij adequaat de transacties van deze merchants monitoren. Daarbij kan gebruik gemaakt worden van het toepassen van gespecificeerde business rules voor transacties van merchants actief in Gambling & Gaming. Hiervoor is het van belang dat merchants in de Gambling & Gaming sector de juiste risicoclassificatie en Merchant Category code krijgen. Indien dit niet het geval is worden merchants tegen onjuiste business rules (thresholds) afgezet, waardoor ongebruikelijke transacties niet worden opgemerkt.[9]

Good practices:

Voor Gambling en Gaming merchants kunnen bepaalde thresholds worden ingesteld ter uitvoering van transactiemonitoring. Deze thresholds kunnen zien op de onderstaande voorbeelden:

- De hoogte van de bedragen en de frequentie voor pay-in en/of pay-out (specificeer thresholds). Bijvoorbeeld een enkele transactie van een Gambling merchant, van €15.000,- of meer binnen 24 uur. Een ander voorbeeld kan zijn dat op het niveau van de merchant een verandering in transactiegedrag wordt opgemerkt door een threshold in te stellen waarbij de transactie een bepaald percentage (nader door betaalinstelling te bepalen) hoger is dan het gemiddelde over de vorige 6 maanden.
- De controle tussen pay-in en pay-out. Bijvoorbeeld, het monitoren van een uitbetaling van een payer (de klant van de merchant) ter vergelijking met de inleg van dezelfde payer (indien de mogelijkheid bestaat thresholds vast te stellen op het niveau van de payer). Indien de inleg met een bepaald vastgesteld percentage (nader te bepalen door betaalinstelling) afwijkt van de uitbetaling wordt de transactie nader onderzocht.
- De betaalmethode voor pay-in en/of pay-out. Bijvoorbeeld, het nader onderzoeken van een transactie bij een bepaalde threshold (nader te bepalen door betaalinstelling) bij gebruik van een anonieme betaalmethode.
- Naast het gebruik van thresholds kunnen andere business rules worden opgesteld. Hierbij kan gedacht worden aan onderstaande voorbeelden:
  - De controle op het gebruik van zakelijke rekeningen (rechtspersoon) voor pay-ins en pay-outs.
  - IP adres controleren. Bijvoorbeeld betalingen van- en naar eenzelfde IP adres of betalingen waarbij het land van de 'shopper' afwijkt van het land waar het IP-adres afkomstig van is.
  - Betrokkenheid hoog risico landen. Bijvoorbeeld de controle op inkomende transacties vanuit hoog risico landen.

9 Indien betaaldienstverleners worden geconfronteerd met fraude bij de aanschaf van spelerstegoeden kan tevens mogelijk sprake zijn van witwassen en/of financiering van terrorisme. De betaaldienstverlener dient dergelijke ongebruikelijke transacties te melden bij FIU-NL

- Controle transactie (pay-in/ pay-out) op illegaal gokken. Bijvoorbeeld het blokkeren van transacties van de zender en naar de ontvanger in landen waar merchants geen vergunning hebben voor Gambling activiteiten of waar deze diensten verboden zijn.

Voor guidance van DNB omtrent transactiemonitoring verwijzen we naar: Post-event transactiemonitoringsproces bij betaaldienstverleners (ook beschikbaar in het Engels).

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl