KYC–CDD POLICY

www.finabanknv.com
customercare@finabanknv.com

FinaBank

INHOUDSOPGAVE

LIJST VAN AFKORTINGEN EN BEGRIPPEN

AML/CFT	: Anti-Moneylaundering/Counter Financing of Terrorism
Bank	: Finabank N.V. en haar rechtsopvolgers
CBvS	: Centrale Bank van Suriname
CDD	: Customer Due Diligence
Derde partij	: een persoon die geen klant is van de bank
DNFBP's	: Non-Designated Financial Businesses and Professions / Aangewezen Niet-Financiële Ondernemingen en Beroepen
EDD	: Enhanced Due Diligence
FATF	: Financial Action Task Force
FIU Suriname	: Financial Intelligence Unit Suriname
FCM	: Financial Crime Mitigation
FoD	: Afdelingen van de bank die geclassificeerd worden als de First Line of Defense, zoals Retail Banking, Platinum Banking, Business Banking, Treasury, Restructuring & Recovery, Customer Service, Cash Department.
FX-transacties	: Foreign Exchange Transacties
IAD	: Internal Audit Departement
Identificatiedocument	: het document waarmee een natuurlijke persoon zich bij de bank identificeert.
Incidentele klant	: een derde partij die een rechtshandeling bij de bank pleegt of laat plegen zonder dat hij in de boeken van de bank is opgenomen als klant.
Incidentele transactie	: een transactie die gepleegd wordt door, namens of ten behoeve van een derde partij op incidentele basis.
Klant	: degene met wie de bank een zakelijke relatie is aangegaan voor de afname van een dienst of product.
KYC	: Know Your Customer / Ken Uw Klant
KYCC	: Know Your Customers Client
ML/FT	: Money laundering/Financing of Terrorism
MOT	: Wet Melding Ongebruikelijke Transacties
OII	: Office of Institutional Integrity

Over-The-Counter transactie	: financiële transactie die direct tussen een derde partij en de bank afgesloten wordt buiten de boeken van de bank, hetgeen bekend staat als 'trading'.
PSA	: Personen van Surinaamse Afkomst
Prospect klant	: een natuurlijke persoon of een rechtspersoon die een aanvraag of verzoek heeft ingediend om klant van de bank te worden.
RBA	: Risk Based Approach/ Risico Gebaseerde Benadering
RvC	: Raad van Commissarissen
SoD	: Afdelingen van de bank die geclassificeerd worden als de Second Line of Defense, zoals RMD en OII
UBO	: Ultimate Beneficial Owner/ Uiteindelijke Begunstigde
Verbonden personen	: medewerkers en daaraan gelijkgestelden, directieleden, leden van de Raad van Commissarissen.
WID	: Wet Identificatieplicht Dienstverleners
WTK	: Wet Toezicht Bank- en Kredietwezen 2011
Zakelijke relatie	: een relatie die door een natuurlijke persoon of een rechtspersoon is aangegaan met de bank.

1. FINABANK IN DE ROL VAN DE POORTWACHTER

1.1 Inleiding

Finabank hecht hoge waarde aan het naleven van integriteitsnormen en het voorkomen van integriteitsrisico's. Als poortwachter van het financiële stelsel speelt de bank een belangrijke rol bij het opsporen en voorkomen van onder meer witwaspraktijken, terrorismefinanciering, corruptie en fraude. De bank heeft daarom controles ingevoerd om te voorkomen dat onze klanten en onze bank (onbewust) financieel economische criminele activiteiten ondersteunen. Een van de belangrijke controles houdt verband met het goed leren kennen de klant en zijn bedrijfsactiviteiten. Deze beheersmaatregel biedt de bank de mogelijkheid om de 'Klantintegriteit' vast te stellen. Een begrip dat ook herkenbaar is met de term 'Ken Uw Klant' of 'Customer Due Diligence', hierna afgekort als KYC/CDD.

In Suriname zijn de regels met betrekking tot KYC/CDD onder meer vastgelegd in de Wet ter voorkoming en bestrijding van Money laundering en Terrorismefinanciering en de Wet Toezicht Bank- en Kredietwezen 2011. Naast de Surinaamse wet- en regelgeving moet Finabank zich vanwege haar (samenwerkings)relaties met buitenlandse partijen ook houden aan verschillende internationale anti-witwas-, antiterrorismefinanciering- en sanctieregelgeving. Om aan deze eisen te voldoen voeren wij gedegen onderzoek uit naar klanten waar wij een (zakelijke) relatie mee aangaan alsook naar de vertegenwoordigers en de uiteindelijk belanghebbenden.

1.2 Doel

Dit beleid is gericht op het nauwkeurig uitvoeren van de KYC/CDD om de klantintegriteit vast te stellen en daardoor mogelijke integriteitsrisico's te identificeren en de bank daartegen te waarborgen door die te voorkomen of indien mogelijk die te beheersen middels mitigatiemaatregelen, zodat de bank behoed wordt van schade in de meest ruime zin.

1.3 Reikwijdte

Dit beleid is van toepassing op alle personen die aan Finabank verbonden zijn: de zogenaamde verbonden personen. Alle verbonden personen zijn verplicht zich te onderwerpen aan dit KYC/CDD beleid en te allen tijde integer te handelen bij de uitvoering van KYC/CDD om zodoende integriteitsrisico's voor de bank tegen te gaan.

1.4 Doelgroep

De KYC/CDD wordt uitgevoerd op alle natuurlijke personen en rechtspersonen die op welke wijze of in welke vorm dan ook zaken met de bank doet:

- bij een natuurlijke persoon: op de klant/prospect klant, zijn wettelijke vertegenwoordiger, zijn gevolmachtigde of een derde partij die zelfstandig een incidentele transactie pleegt;
- bij een rechtspersoon: op de klant/prospect klant, haar statutaire vertegenwoordigers, haar gevolmachtigden (procuratiehouders), haar ultimate beneficial owners (zowel directe als indirecte) tot en met op het niveau van natuurlijke personen.

2. RISK BASED APPROACH (RISICOGEBASEERDE AANPAK)

2.1 Algemeen

De bank laat de omvang van haar risicoanalyse of risicobeoordeling bij de uitvoering van KYC/CDD bepalen door een op risico gebaseerde benadering (RBA), hetgeen inhoudt:

1. dat de door de bank te treffen maatregelen ter voorkoming of vermindering van onder meer witwassen en financiering van terrorisme in overeenstemming zijn met de geconstateerde risico's;
2. dat de maatregelen de bank in staat moeten stellen om besluiten te nemen over de meest doeltreffende inzet van eigen middelen;
3. dat de bank zich voorziet in procedures voor het vaststellen, beoordelen, bewaken, beheren en beperken van onder meer witwassen en terrorismefinanciering;
4. dat de bank bij grotere risico's versterkte maatregelen neemt om die risico's te beheersen en te beperken en dat dienovereenkomstig bij afname van de risico's vereenvoudigde maatregelen kan nemen voorzover er geen sprake is van enig vermoeden van witwassen of financiering van terrorisme.

Kortom, op basis van een "risk based approach" ziet de bank erop toe dat het gewicht of sterkte van de maatregelen evenredig is aan de omvang van de risico's. Hoe groter de risico's, hoe strenger of robuuster de maatregelen

2. 2 Beoordeling van ML/FT-risico's

De bank onderneemt passende maatregelen om de risico's op onder meer witwassen en financiering van terrorisme te bepalen en te beoordelen. Deze maatregelen hebben onder meerbetrekking op de volgende risicodragers:

a. clienten: het beoordelen van clienten middels het uitvoeren van KYC/CDD, en bij hoog risico middels het uitvoeren van EDD. Een gedegen analyse voor het goed kennen van deklant, met name zijn activiteiten of business, zijn verwachtingen;
b. landen of geografische gebieden: het onderzoeken van de risicocategorie van het land of het geografisch gebied waarin een client gevestigd is, haar filialen of zakenpartners heeft, en naar welk land een client transacties wilt verrichten, zoals gepubliceerd door toonaangevende internationale organisaties;
c. producten en diensten: het beoordelen van de risico's die aan producten en diensten kunnen kleven die door een client is aangevraagd of welke aan een client zijn verleend. Daarbij onderzoekt de bank onder meer of het product of de dienst past bij die client. Heeft hij het product of de dienst nodig en waarvoor wordt het gebruikt;
d. transacties: het beoordelen van de transacties van een client al dan niet met onderliggende documenten en de toetsing daarvan met het transactieprofiel;
e. leveringskanalen (delivery channels): het beoordelen van de risico's bij het gebruik van de delivery channels door een client. Deze delivery channels omvatten filialen, geldautomaten (ATM's), betaalterminals, POS-apparaten, mobile banking, wallets, internetbankieren (e-banking).

De bank zorgt ervoor dat:

- zij in voldoende mate weet welke integriteitsrisico's zij met de klant kan lopen na het analyseren van de risk drivers en welke beheersmaatregelen zij beschikt.
- deze beoordelingen worden gedocumenteerd om hun grondslag te kunnen tonen;
- deze beoordelingen periodiek worden geactualiseerd;
- zij adequate mechanismen beschikt voor de verstrekking van informatie aan de bevoegde autoriteiten (OM) en toezichthouders (FIU Suriname, CBvS) voorzover de bank daartoe gehouden is bij wet of richtlijn, of daarvoor door een bevoegde autoriteit een verzoek wordt gedaan;
- bij de beoordeling alle relevante risicofactoren voor het bepalen van het totale risiconiveau en het passende niveau van aanpak worden beoordeeld;
- de omvang van haar maatregelen afhankelijk wordt gesteld van de aard en de omvang van het risico ten aanzien van de verschillende factoren, bijvoorbeeld: bij laag risico wordt volstaan met KYC/CDD, terwijl bij hoog risico een EDD aan te pas komt.

2.3 Risicofactoren/ Risk drivers

De bank heeft een client risk score card vastgesteld op basis waarvan risicocategorieën voor klanten worden vastgesteld. De bank classificeert haar klanten in risicocategorieën op basis van de resultaten van de toetsing van de klant op door de bank geïdentificeerde risicofactoren, zodat de bank adequate mitigerende maatregelen kan nemen. De risicocategorieën, zoals die uit de client risk score card voortvloeien, zijn: laag, gemiddeld, hoog en onacceptabel. De risicofactoren worden steeds onderbouwd met onderliggende documenten. De risicofactoren oftewel de risk drivers worden hieronder opgesomd, zonder enige beperking of limitatie, met enkele meest voorkomende situaties waarin de bank EDD uitvoert:

1. Clientgebonden risicofactoren zoals:
    a. niet-ingezetene klanten, of niet in Suriname gevestigd;
    b. client gaat veel om met cash geld (cash intensive business);
    c. ongewoon of buitensporig complex eigendomsstructuur strookt niet met de aard van de ondernemingsactiviteit;
    d. gevolmachtigde aandeelhouder;
    e. Bedrijven met aandelen aan toonder (bearer shares) of warrants aan toonder (bearer share warrants);
    f. verbergen van persoonlijke activa middels gebruikmaking van een rechtspersoonof juridische constructie;
    g. zakelijke relatie vindt in ongewone omstandigheden plaats;
    h. een politiek prominente personen (PEP) en PEP associates;
    i. op naam gestelde aandelen worden ten behoeve van een derde gehouden;
    j. bij natuurlijke personen, rechtspersonen, en daarmee vergelijkbare entiteiten die afkomstig zijn uit landen of jurisdicties die niet of onvoldoende voldoen aan de internationaal gangbare normen op het gebied van de voorkoming en bestrijding van money laundering en terrorismefinanciering;

k. indien het particulier vermogensbeheer betreft ten behoeve van vermogende natuurlijke personen;
l. bij rechtspersonen of juridische constructies die bedoeld zijn voor het onderbrengen van persoonlijke vermogens;
m. Stichtingen en liefdadigheidsinstellingen (bv, non-profit organisatie (NPO's) en andere niet-gouvernementele organisaties, die als onderdeel van haar werkzaamheden financiële middelen ontvangt, verstrekt, subsidieert, verzamelt, overmaakt en/of winsten beoogt;
n. bij natuurlijke personen, rechtspersonen en juridische constructies met een bad press;
o. gesanctioneerde personen;
p. De eigendomsstructuur van het bedrijf lijkt ongebruikelijk of overdreven complex gezien de aard van de zaken van het bedrijf;
q. Rechtspersonen of juridische constructies die vehikels zijn voor het aanhouden van persoonlijke activa;
r. Off-shore bedrijven en Shell of Shelf companies
s. Bedrijven actief in sectoren met een hoog risico (goudhandel, edele metalen, kansspelen, juwelen, houthandel, geldwisselkantoren, professionele beroepsgroepen, commercieel vastgoed, tweedehandsauto's);
t. Correspondentbanken.
u. Rationale achter het openen van een rekening of het aangaan van de relatie;
v. Omvang of doel van de te verwachten transacties;
w. Intensiteit en duur van de cliëntrelatie;
x. Algemene kennis van de achtergrond van de cliënten (welke sector, is cliënt een PEP).

2. Risicofactoren gebonden aan land of regio zoals:
   a. gesanctioneerde landen of landen waarvoor embargo gelden;
   b. landen die niet over adequate AML/CFT systemen beschikken;
   c. landen met aanzienlijk niveaus van corruptie of andere criminele activiteiten;
   d. landen met actieve terroristische organisaties;
   e. landen die terrorisme financieren;
   f. landen die door FATF of een vergelijkbare organisaties/ instituten worden aangemerkt als risicolanden.

3. Product- of dienstgebonden risicofactoren zoals:
   a. private banking: financiële dienstverlening van de bank aan welgestelde particulieren (platinum banking);
   b. bij het aangaan van correspondentbankrelaties;
   c. producten en diensten die misbruikt kunnen worden voor witwaspraktijken;
   d. ML risico's verbonden aan nieuwe technologieën zoals Virtuele valuta (Virtual Asset Service Providers).

4. Risicofactoren gebonden aan transactie- of leveringskanaal zoals:
    a. anonieme transacties;
    b. transacties met cash geld;
    c. betalingen worden ontvangen van onbekende of niet-gelieerde derden.

2.4 Risicobeheersing en risicobeperking

Voor het doeltreffend beheersen en beperken van ML/FT-risico's heeft de bank ervoor gezorgd dat:

- zij bij de uitvoering van KYC/CDD dit beleid volgt. Evenzo bij het analyseren en beoordelen van ML/FT risico's;
- zij processen en procedures, alsmede werkinstructies beschikt;
- zij controlemechanismen in place heeft, waaronder doch niet beperkt tot een controlerende IAD, rapportages en rapportagelijnen, FCM, Internal Watchlist, WorldCheck;
- zij werkt aan educatie en cultuurverandering.

3. KNOW YOUR CUSTOMER/CUSTOMER DUE DILIGENCE

3.1 Omschrijving van KYC/CDD

KYC staat voor Know Your Customer, hetgeen letterlijk betekent: "ken je klant". De Engelse term "due diligence" betekent letterlijk "gepaste zorgvuldigheid". Met gepaste zorgvuldigheid beoordelen van de klant op integriteitsrisico's wordt Customer Due Diligence genoemd, afgekort CDD. De uitvoering van KYC/CDD staat ook wel bekend als het clientenonderzoek.

Het clientenonderzoek (KYC-CDD) kent drie (3) levels van CDD. De trigger voor het bepalen van het CDD-onderzoek zijn de risicofactoren die afhankelijk zijn van het verwachte risico dat de (potentiële) klant met zich meebrengt. Deze wordt naar aanleiding van de risicoclassificatie uitgebreid. Onderstaand de mate van due diligence per risicoclassificatie:

1. Vereenvoudigd CDD (Simplified EDD): kan worden toegepast indien de cliënt een laag risico meebrengt dat de bank ongewild betrokken wordt bij het faciliteren van witwas transacties of terrorismefinanciering.
2. Standaard CDD: Dit geldt voor cliënten bij wie er sprake is van een matig ML/TF risico. De facto zijn dit alle cliënten die geen laag of hoog risico meebrengen voor de bank dat hij betrokken wordt bij ML of TF. Bij deze level van onderzoek wordt de bank instaat gesteld om:
    a. de klant te identificeren
    b. diens identiteit te verifiëren
    c. de UBO te identificeren en diens identiteit te verifiëren
    d. het doel en beoogde aard van de zakelijke relatie vast te stellen
    e. de zakelijke relatie en zijn transacties te monitoren, eventueel onderzoek naar de bron van de middelen die bij de relatie of de transactie gebruikt worden
    f. vast te stellen of de natuurlijke persoon die de klant vertegenwoordigt daartoe bevoegd is en deze persoon te identificeren en diens identiteit te verifiëren.

3. Uitgebreide CDD (Enhanced Due Diligence): Indien op basis van bij de klant aanwezige risico-indicatoren wordt vastgesteld dat een inherent hoger risico bestaat op money laudering of terrorisme financiering, dienen acties ondernomen te worden, die passen bij de uitgebreide CDD (meer hierover in paragraaf 3.10.1).

Om de risicoclassificatie te bepalen is er een CRR-tool ontwikkeld. Die zal bijdragen aan de risk rating van de klant. De score zal mede bepalen in welke level van CDD de assessment zal plaatsvinden. Echter indien er redenen bestaan om extra onderzoek te verrichten is dat mogelijk. Bij uitgebreide CDD (Enhanced Due diligence) is altijd goedkeuring van OII vereist.

3.2 Het clientenonderzoek

Het clientenonderzoek is het proces waarbij de bank op basis van onderzoek met redelijke zekerheid moet kunnen vaststellen dat zij haar klant kent en dat eventuele risico's die gepaard gaan met het aangaan of voortzetten van de relatie met de klant beheersbaar zijn. Als poortwachter is het voor de bank van groot belang om het clientenonderzoek uit te voeren om te weten met wie zij zaken doet of zal doen, welke integriteitsrisico's daarbij (kunnen) kleven en of die beheersbaar zijn of tot een aanvaardbaar niveau gereduceerd danwel gemitigeerd kunnen worden.

Het clientenonderzoek door Finabank omvat de volgende maatregelen:

a. het identificeren van de klant en verifiëren van de identiteit van die klant met behulp van betrouwbare, onderliggende documenten, gegevens of informatie, zoals nader beschreven in de WMTF. Het toepassen van due diligence op de klant en zijn onderneming/business;
b. het identificeren van de UBO en het nemen van redelijke maatregelen om zijn identiteit te verifiëren ter overtuiging daarvan. Indien de UBO een rechtspersoon en/of juridische constructie betreft, wordt onderzoek gedaan naar de eigendomsverhoudingen en zeggenschapsstructuur van de klant. De UBO moet de naam van zijn nominator bekendmaken;
c. het begrijpen en, in voorkomende gevallen, het verkrijgen van informatie over het doel en de beoogde aard van de zakelijke relatie. Het analyseren van de risk drivers;
d. het uitvoeren van voortgezet clientenonderzoek (KYC/CDD/EDD) met betrekking tot de zakelijke relatie en controle op verrichtingen in de loop van die relatie om ervoor te zorgen dat de transacties worden uitgevoerd in overeenstemming met het klantprofiel (de kennis over de klant, zijn bedrijf en het risicoprofiel, inclusief de bron van inkomsten, de herkomst van geldmiddelen;
e. het verzamelen en vast leggen van essentiële clientgegevens;
f. het screenen van cliënten tegen de sanctie, negatieve media en PEP-lijsten;

g. het beoordelen van het risicoprofiel van client middels de CRR tool en het verwachte transactie gedrag op de bankrekening;
h. doorlopende transactie monitoring;
i. het melden van ongebruikelijke transacties aan de FIU-SU;
j. het opslaan van clientgegevens op een veilige manier.

De bank bepaalt aan de hand van de geldende eisen onder de punten (a) tot en met (d) de grondigheid van het onderzoek aan de hand van risico-inschatting. Onderzocht wordt ook in hoeverre de geïdentificeerde risico's mitigeerbaar en beheersbaar zijn en welke controles er daarvoor aanwezig zijn.

Zolang aan dat onderzoek niet is voldaan, ziet de bank, voor zover het betreft nieuwe klanten,
pertinent af van:
- het openen van de rekening;
- het aangaan van zakenrelaties;
- het uitvoeren van een transactie.

In het geval van een bestaande klant stelt de bank een redelijk termijn vast voor het verlenen van medewerking voor de uitvoering van het incidentele clientenonderzoek. Indien de klant daartoe geen medewerking verleent of de bank door toedoen van de klant dat clientenonderzoek niet (adequaat) kan uitvoeren, zal de bank de volgende maatregelen treffen:
- het beëindigen van de zakenrelatie (de-risking);
- het maken van een melding (van een verdachte transactie) naar het FIU Suriname.

3.3 Momentum van clientenonderzoek

De bank voert clientenonderzoek uit op de volgende momenten:
a. vóór of bij het aangaan van zakelijke relaties;
b. vóór of tijdens het afsluiten of uitvoeren van transacties voor een incidentele client;
c. wanneer er een vermoeden van witwassen of financiering van terrorisme of het begaan van een daaraan onderliggende delict bestaat; of
d. wanneer de bank twijfels heeft over de juistheid (waarheidsgetrouwheid) of de toereikendheid (adequaatheid) van de eerder verkregen gegevens betreffende de identiteit of informatie van de cliënt;
e. voortdurende controle op de zakelijke relatie, teneinde te verzekeren dat deze overeenkomen met de kennis die de dienstverlener heeft van de cliënt en diens risicoprofiel.
f. bij het verrichten van incidentele transacties boven de ingevolge het Besluit Indicatoren Ongebruikelijke Transacties van toepassing zijnde drempel;
g. bij het verrichten van elektronische geldovermakingen;
h. zodra de bank op basis van feiten en omstandigheden het nodig oordeelt, waaronder doch niet beperkt tot bad press.

De bank blijft zelfs na identificatie van de cliënt CDD-maatregelen toepassen en onderzoekt alle transacties die verricht zijn gedurende de loop van de zakenrelatie nauwkeurig, teneinde er zeker van te zijn dat de verrichte transacties in overeenstemming zijn met de informatie waarover de bank beschikt met betrekking tot de klant, het risicoprofiel en de herkomst van de fondsen van de klant.

De bank past deze CDD-maatregelen toe op zowel nieuwe als op bestaande klanten, waarbij de reikwijdte van deze maatregelen op grond van de risicogevoeligheid, het type cliënt, de zakenrelatie of de transactie wordt bepaald.

3.4 Vaststelling van de identiteit

Binnen het kader van het clientenonderzoek is met betrekking tot de vaststelling van de identiteit van de klant, prospect of een derde partij de uitvoering van de volgende processen verplicht:

1. Identificatie: het vaststellen van de identiteit;
2. Verificatie: het zich overtuigen van de identiteit middels het plegen van verificatie.

Deze processen worden uitgevoerd conform de wettelijke voorschriften en richtlijnen.

3.4.1 Identificatie van natuurlijke persoon

Voor de identificatie van een natuurlijke persoon vereist de bank de volgende identificatiedocumenten:

a. geldige Surinaamse identiteitskaart;
b. geldig paspoort;
c. geldig Surinaams rijbewijs;
d. geldige PSA-kaart.

3.4.1.1 Bewijs van indiening en vervallen identificatiebewijs

In Suriname komt weleens geregeld voor dat vanwege diverse redenen burgers niet tijdig kunnen beschikken over hun identificatiedocument, zoals door gebrek aan vervaardigingsmateriaal, langdurige wachttijden, tijdelijke sluiting van uitgevende kantoren. Klanten beschikken vaak wel over een bewijs van indiening van hun aanvraag voor het verkrijgen van hun respectieve identificatiedocument.

Een bewijs van indiening dat door een klant overgelegd wordt tezamen met een vervallen identificatiedocument waarop de klant duidelijk herkenbaar is, wordt door de bank geaccepteerd voor het uitvoeren van KYC/CDD doeleinde. Van dat bewijs en het vervallen identificatiedocument wordt een kopie in het dossier van de klant gevoegd. Nadat de klant zijn identificatiedocument van de daartoe bevoegde uitgevende instantie heeft ontvangen, dient hij dat aan de bank te overleggen waarvan een (scan)kopie in het klantdossier wordt toegevoegd en de klantfile in de core banking system bijgewerkt.

3.4.1.2 Klanten met vreemde nationaliteit

Klanten die een vreemde nationaliteit bezitten, identificeren zich bij de bank met hun geldige paspoort en/of PSA-kaart. Indien een vreemdeling met vestigingsvergunning in het bezit is van een "Surinaams identiteitskaart voor vreemdelingen", is het die vreemdeling toegestaan om zich met die identiteitskaart te identificeren bij de bank. Als onderdeel van de KYC/CDD dienen klanten met een vreemde nationaliteit, met uitzondering van de houder van een PSA-kaart, ook het bewijs van hun legaal verblijf in Suriname te overleggen. Dat bewijs kan het volgende zijn:

a. Bij kortverblijf: het paspoort met de stempels van de immigratie;
b. Bij verblijf voor bepaalde tijd: de verblijfsvergunning of de PSA-kaart;
c. Bij verblijf voor onbepaalde tijd: de vestigingsvergunning.

3.4.1.3 Handelingsonbekwaamheid
Indien een persoon van rechtswege handelingsonbekwaam is, volstaat de bank met het vaststellen van de identiteit van diens wettelijke vertegenwoordiger. Dit is ook voorgeschreven in het Burgerlijk Wetboek van Suriname.

3.5 Verificatie van de identiteit

3.5.1 Algemeen
Wettelijk is de bank verplicht om al het nodige te doen ter verkrijging van informatie ter vaststelling van de identiteit van de klant ten behoeve van wie diensten worden verleend. Kortom, de identiteit van de klant dient te worden geverifieerd. De verificatie doet de bank aan de hand van het overgelegde identificatiedocument. In geval van twijfel vraagt de bank een additioneel (identificatie) document op.

Met informatie ter vaststelling van de NAW wordt onder meer bedoeld: naam, adres, woonplaats, telefoonnummer, geboortedatum, geboorteplaats, nationaliteit, beroep en eventueel de werkgever van de cliënt; tevens worden vastgelegd de aard, het nummer, de datum en de plaats van uitgifte van de documenten aan de hand waarvan de identiteit is vastgesteld.

3.5.2 Verificatie achteraf
Wanneer omstandigheden zulks vereisen, voltooit de bank de verificatie binnen één maand na de totstandkoming van de zakelijke relatie, indien de risico's voor witwassen of financiering van terrorisme e.a. zijn ingedamd en dit essentieel is om de normale gang van zaken niet te verstoren.

In dit geval kan de bank, afhankelijk van de type dienst of product, beperkingen stellen van het aantal transacties, de typen en/of de omvang van de transacties die kunnen worden verricht. De bank zal ook als maatregel grote en complexe transacties bewaken.

3.6 Identificatie van rechtspersonen en juridische constructies
De bank onderscheidt rechtspersonen en juridische constructies in de volgende categorieën:
1. Surinaamse rechtspersonen;
2. Buitenlandse rechtspersonen:
   a. In Suriname mede gevestigd,
   b. In Suriname niet gevestigd;
3. Surinaamse juridische constructies
4. Buitenlandse juridische constructies.

In deze policy wordt de nadruk gelegd op de Surinaamse rechtspersonen en juridische constructies zonder uitsluiting van buitenlandse rechtspersonen en juridische constructies.

De Surinaamse rechtspersonen worden onderverdeeld in:
I. Publiekrechtelijke rechtspersonen:
   a. de Staat Suriname oftewel de Republiek Suriname;
   b. rechtspersonen sui generis (o.a. in de vorm van stichting, naamloze vennootschap);
   c. Staatsbedrijven ex Landsbedrijvenverordening 1971.

II. Privaatrechtelijke rechtspersonen:
   a. naamloze vennootschap (nv);
   b. coöperatieve vereniging;
   c. onderlinge waarborgmaatschappij;
   d. stichting;
   e. vereniging (met of zonder zedelijkheid).

De Surinaamse juridische constructies zijn:
a. eenmanszaak;
b. naamloze vennootschap i.o.;
c. vennotschap onder firma;
d. commanditaire vennootschap;
e. maatschap.

De identificatie van deze rechtspersonen en juridische constructies geschiedt met de ocumenten, zoals vermeld in deze policy.

3.7 Reguliere klanten en bijzondere categorie klanten

In het kader van de risicogebaseerde benadering bij voornamelijk de processen onboarding en monitoring, maakt de bank in haar klantenbestand een onderscheid tussen reguliere klanten en bijzondere categorie klanten, en wel als volgt:
a. reguliere klanten: alle klanten die niet behoren tot de bijzondere categorie klanten;
b. bijzondere categorie klanten: klanten die gerekend worden tot de DNFBP's:
   1. Kredietcoöperaties;
   2. Trustmaatschappijen;
   3. Makelaars;
   4. Beroeps- of bedrijfsmatige handelaren in goud, juwelen en andere edele metalen en edelstenen (ontginning, opkoop, verkoop);
   5. Advocaten;
   6. Notarissen en kandidaat-notarissen;
   7. Andere onafhankelijke beoefenaars van juridische beroepen;
   8. Accountants;
   9. Administratiekantoren;
   10. Beroeps- of bedrijfsmatige handelaren in of bemiddelaars bij aan- en verkoop van onroerende goederen, voertuigen, schepen, luchtvaartuigen,kunstvoorwerpen, antiquiteiten, en de rechten waaraan deze zaken zijn onderworpen;
   11. Beheersmaatschappijen;
   12. Handelaren van motorrijtuigen (importeur en verkoper);
   13. Vastgoedbedrijven (nota bene: aannemers zijn geen vastgoedbedrijven);
   14. Belastingconsulenten of belastingadviseurs of vergelijkbare beroepsbeoefenaar;
   15. Deurwaarders;
   16. Consultants;
   17. PEP's;
   18. NPO's;
   19. Taxateurs;
   20. Inklaarders.
   21. Stichtingen
   22. Houthandel
   23. Reisbureaus

De bank merkt de bijzondere categorie klanten aan als high risk klanten en onderwerpt hen zowel bij de onboarding als gedurende de relatie aan EDD.

3.8 Onacceptabele klanten

De bank merkt de volgende klanten aan als onacceptabele klanten:

1. Shell Banks;
2. Hawala's en vergelijkbare constructies;
3. Landen, natuurlijke personen, rechtspersonen en overige juridische constructies die vermeld staan op internationale sanctielijsten, waaronder doch niet beperkt tot FATF, EU, VN, OFAC sanctielijsten;
4. Cryptodienstverleners en deelnemers van cryptodiensten (virtual assets);
5. Piramidespelen en vergelijkbare spelen;
6. Klanten met aandelen aan toonder of warrants aan toonder;
7. Klanten met complexe vennootschapsstructuren waarbij de UBO niet of moeilijk vast te stellen is, of waaraan de klant niet of beperkt medewerking verleent;
8. Natuurlijke personen en rechtspersonen die voorkomen op een nationale, regionale of internationale sanctielijst (Finabank zal een melding doen bij CBvS);
9. Money or Value Transfer Services (geldovermakingskantoren);
10. Wisselkantoren (cambio's) en valutahandelaren;
11. Geldschieters;
12. Casino's;
13. Aanbieders van kansspelen (loterijen en hazardspelen);
14. Cannabis.
15. Juridische structuren ontworpen om economisch eigendom te verbergen (via offshore constructies);
16. Het niet kunnen identificeren van UBO('s) van de rechtspersoon;
17. Problemen met verificatie van de identiteit van de bestuurders van de rechtspersoon;
18. Het niet kunnen identificeren van de oorsprong van het vermogen / onaanvaardbare herkomst van middelen;
19. Cliënten die anoniem wensen te blijven of fictieve identiteitsgegevens verstrekken;
20. Natuurlijke personen en rechtspersonen die woonachtig of gedomicilieerd zijn in of burgers zijn van gesanctioneerde landen;
21. Politieke partijen.

3.9 Transactieprofiel en transactiegedrag

Voor de bepaling van het risicoprofiel van een klant maakt de bank een transactieprofiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een klant of klantengroep. Door dit transactieprofiel stelt de bank zich in staat om in voldoende mate te monitoren dat de transacties die tijdens de duur van de relatie verricht worden, overeenkomen met de kennis die de instelling heeft van de klant en diens risicoprofiel.Door het verwachte transactiegedrag van de cliënt in beeld te toetst de bank of de door de klant uitgevoerde transacties afwijking vertoont met het transactieprofiel.

Het transactieprofiel bij rechtspersonen en andere juridische constructies die in het algemeen bekend staan onder de term

'zakelijke klanten', wordt gevormd door diens maandelijkse omzet en bedrijfsactiviteiten, terwijl het transactieprofiel bij natuurlijke personen, meer bekend als particulieren, wordt gevormd door de hoogte van zijn inkomen en de bron/herkomst daarvan.

Het transactieprofiel wordt door de FoD vastgesteld op basis van de intake met de klant en waar mogelijk onderbouwd met onderliggende documenten. Bij het samenstellen van het transactieprofiel en bij de screening van transacties wordt onder meer gelet op:

- wie is de klant;
- wat doet de klant (activiteiten);
- wat is de omzet/inkomsten (revenue streams);
- passen de transacties binnen het transactieprofiel met inachtneming van een vastgestelde marge van tolerantie.

Gedurende de duur van de klantrelatie toetst de FoD periodiek of de cliënt nog steeds aan het risicoprofiel voldoet en of het transactiepatroon overeenkomstig de verwachtingen is. De frequentie en de intensiteit van de reviews heeft de bank afgestemd op de risicoclassificatie van de klant. Wanneer het transactiegedrag van een klant afwijkt van zijn transactieprofiel, onderwerpt de bank de klant en zijn transacties aan een onderzoek. Daarbij wordt de klant gehoord en in de gelegenheid gesteld om die afwijking te onderbouwen. Met name bij de revisie kan het transactieprofiel worden bijgesteld wanneer blijkt dat het verouderd is ten opzichte van de werkelijke situatie van de klant. Eveneens, wanneer de OII onder meer in het kader van de uitvoering van transactiemonitoring en continuous monitoring constateert dat het transactiegedrag van de klant niet overeenkomstig zijn transactieprofiel is, ziet zij erop toe dat de FoD een revisie uitvoert.

3.10 Enhanced Due Diligence en KYCC

3.10.1 Algemeen

In deze paragraaf ligt de focus op de EDD. De EDD houdt een verscherpte clientenonderzoek in dat door de bank wordt verricht indien en naar gelang een zakelijke relatie of transactie naar haar aard een hoger risico (high risk) op witwassen of financiering van terrorisme vertegenwoordigt. De bank voert het verscherpte clientenonderzoek zowel voorafgaand aan de zakelijke relatie of de transactie, als gedurende de zakelijke relatie.

De bank voert, zonder zich te beperken tot de onderstaande situaties, de EDD uit in de volgende gevallen waarin altijd sprake is van een hoger risico:

a. wanneer het betreft een zakelijke relatie of transactie met een hoger risico op witwassen of financieren van terrorisme;
b. wanneer de klant – of de UBO van de klant – woonachtig of gevestigd is, dan wel zijn zetel heeft, in een land dat is aangewezen als een hoog risico land of gebied;
c. wanneer de klant – of de UBO van de klant – een PEP is;
d. in het geval van een correspondentrelatie.

Evenals bij de uitvoering van een standaard clientenonderzoek wordt ook bij de uitvoering van de EDD alle risicofactoren in relatie tot de klant getoetst. De risicofactoren staan ook bekend als risicodragers oftewel risk drivers.

3.10.2 EDD maatregelen

De bank treft de volgende niet-limitatief opgesomde maatregelen voor zakelijke relaties met verhoogd risico (high risk):

a. het inwinnen van aanvullende informatie over de klant en voor zover toepasselijk van de gevolmachtigde of begunstigde (beroep, de omvang van de activa, informatie uit openbare register en databestanden en van internet, enz.), en het regelmatiger bijwerken van de identificatiegegevens van de cliënt en de uiteindelijke begunstigde;
b. het inwinnen van aanvullende informatie over de beoogde aard van de zakelijke relatie;
c. het inwinnen van informatie over de bron van inkomsten/ gelden of het vermogen van de cliënt.
d. het inwinnen van informatie over de redenen voor de beoogde of verrichte transacties;
e. het verkrijgen van goedkeuring van de directie voor het aangaan of voortzetten van de zakelijke relatie met PEP's.
f. verscherping van het toezicht op de zakelijke relatie door het aanpassen van het aantal en de timing van de controles en de selectie van transactiepatronen die een uitvoeriger onderzoek vereisen.
g. vereisen dat de eerste betaling wordt verricht via een rekening op naam van de cliënt bij een bank die onderworpen is aan soortgelijke cliënt onderzoeksnormen.

3.10.3 Situaties voor EDD

Het EDD onderzoek wordt door de bank uitgevoerd zodra de bank een hogere risico bij een
zakelijke relatie of transactie constateert of vermoedt. In ieder voert de bank het EDD onderzoek
wanneer een van de volgende situaties van toepassing is:

a. indien een cliënt geen ingezetene van Suriname is, of niet in Suriname gevestigd is;
b. indien een cliënt niet fysiek aanwezig is voor identificatie;
c. indien het particulier vermogensbeheer betreft ten behoeve van vermogende natuurlijke personen;
d. bij rechtspersonen of entiteiten die bedoeld zijn voor het onderbrengen van persoonlijke vermogens;
e. bij vennootschappen en daarmee vergelijkbare entiteiten waarvan de aandelen aan toonder
f. zijn gesteld of indien de op naam gestelde aandelen ten behoeve van een derde worden gehouden;
g. bij natuurlijke personen, rechtspersonen, en daarmee vergelijkbare entiteiten die afkomstig
h. zijn uit landen of jurisdicties die niet of niet geheel voldoen aan de internationaal gangbare normen op het gebied van het voorkomen en bestrijden van witwassen en financiering van terrorisme;

i. bij politiek prominente personen (PEP);
j. bij het bestaan van bad press over de klant;
k. bij het aangaan van correspondent bankrelaties.

3.10.4 KYCC

Een belangrijk onderdeel van de EDD is de KYCC hetgeen bij het uitvoeren van EDD door de bank toegepast kan worden waar zulks nodig mocht blijken om een 360 graden onderzoek te verrichten op een klant. In de financiële wereld staat de afkorting 'KYCC' voor het volgende:

- Know Your Client's Clients;
- Know Your Customer's Customers;
- Know Your Entity;
- Know Your Employee;
- Know Your Client's Correspondents.

Alle drie begrippen monden uit in hetzelfde doel en beogen om die reden hetzelfde resultaat. In deze policy zullen deze begrippen verder worden aangeduid met de afkorting "KYCC".

Het KYCC-principe legt in incidentele gevallen een extra verantwoordelijkheid op de bank om niet alleen haar eigen klanten te kennen door deze te onderwerpen aan een KYC/CDD toets, doch ook de cliënten en relaties van die klanten. Alhoewel de KYCC vaak gepaard met een EDD onderzoek, kan dit reeds bij de onboarding van de klant worden uitgevoerd door de FoD.

Bij het uitvoeren van EDD dienen de cliënten en relaties van de klanten van de bank zich ook te worden onderworpen aan de KYC-CDD toets. Hoewel het primair tot de verantwoordelijkheid van de klant van de bank behoort om informatie over zijn cliënten en relaties aan te leveren bij de bank, ontslaat die verantwoordelijkheid de bank niet om zélf ook op zoek te gaan naar informatie over deze cliënten en relaties: de zogenaamde "indirecte relaties".

De bank acht het noodzakelijk om in het kader van de AML/CFT-regels en best practices te weten met wie zijn klanten zaken doen. Bij de samenstelling van het KYCC-profiel, dienen de gegevens door de medewerkers van de FoD te worden vastgelegd. Deze gegevens worden geadministreerd en opgeslagen in het klantdossier.

3.11 Gebruik van afgeleide KYC/CDD

Alhoewel het tot de verantwoordelijkheid van de bank behoort om zelf clientenonderzoek uit te voeren, kan de bank een klant die geïntroduceerd wordt door een in Suriname gevestigde financiële dienstverlener of door een in Suriname gevestigde niet-financiële dienstverlener zich verlaten op het door die dienstverlener verrichte clientenonderzoek (hierna: "Afgeleide KYC/CDD"). Dit kan de bank doen voor zover het door die dienstverlener verrichte clientenonderzoek de elementen van de wettelijke identificatieplicht omvat.

Het vertrouwen op en het accepteren van de afgeleide KYC geschiedt uitsluitend wanneer de bank:

a. zich ervan heeft vergewist dat kopieën van alle gegevens en inlichtingen over het verrichte clientenonderzoek door die derde op verzoek van de bank onverwijld aan haar beschikbaar kunnen worden gesteld;

b. zich ervan heeft vergewist dat de derde over procedures en maatregelen beschikt die de derde in staat stelt om een clientenonderzoek uit te voeren en de gegevens en inlichtingen die als gevolg van dat clientenonderzoek zijn verkregen, te bewaren.

3.12 Intermediairs

Intermediairs zijn personen – natuurlijke personen of rechtspersonen – die door een financiële instelling, m.n. door een bank gecontracteerd kunnen worden om bepaalde elementen of taken met betrekking tot de uitvoering van clientenonderzoek voor rekening en risico van die bank uit te voeren.

Alhoewel het wettelijk toegestaan is om het clientenonderzoek en het beheer van gegevens uit te besteden aan een intermediair, gaat Finabank geen relaties aan met intermediairs of maakt geen gebruik van een intermediair voor het uitvoeren van de KYC/CDD gerelateerde taken.

3.13 Bron van inkomsten en herkomst van middelen

3.13.1 Verschil tussen bron van inkomsten en herkomst van middelen

Bij het identificeren van de bron van inkomsten en de herkomst van middelen van onze klanten, is belangrijk om als bank integriteitsrisico's tegen te gaan. Het zijn twee belangrijke doch verschillende begrippen, namelijk:

a. De bron van inkomsten ("van waar/waaruit") betreft:
   i. door de specifieke activiteit van onze klant waarmee zijn inkomen verkregen is;
   ii. met een bepaald volume;
   iii. in een bepaald valutasoort;
   iv. over een bepaald periode.
b. Herkomst van middelen ("van wie") betreft
   i. door NAW-gegevens van de klant of diens werkgever van wie het inkomen verkregen is;
   ii. met een bepaald volume;
   iii. in een bepaald valutasoort.

Finabank stelt de volgende voor haar acceptabele manieren vast waarop de bron van inkomsten of herkomst van middelen kan worden aangetoond:

1. het accepteren van een schriftelijke verklaring, ondertekend en afgegeven door de klant, waarin een verklaring van de bron/herkomst goed is verklaard; en/of
2. het accepteren van een onderliggend document, afgegeven door de klant.

Onderliggende documenten waarmee de herkomst van de middelen kan worden onderbouwd zijn zonder enige limitatie: kwitanties, facturen, bonnen, debiteurenlijsten. Bij chartale transacties (stortingen) door de bijzondere categorie klanten vereist de bank dat zij onderliggende documenten aanleveren (zoals een lijst met klanten) conform het zogenoemde 'Know Your Customer's Customer (KYCC)' principe, gezien deze bijzondere klanten internationaal bekend staan als vehikels voor witwaspraktijken en financiering van terrorisme.

Indien een klant de herkomst van de middelen conform deze policy niet met documenten kan bewijzen, verleent de bank hem geen diensten. Met name zal bij de kassa's van de bank geen transacties (stortingen) aan deze klant worden toegestaan of verleend.

Een klant die zijn bron van inkomsten heeft aangetoond door middel van een acceptabel onderliggend document in een bepaald valutasoort (bijvoorbeeld omdat de jaarrekening of salarisslip in die valutasoort luidt), maar tevens heeft aangegeven middels een andere acceptabele verklaring dat hij zijn inkomsten in meerdere valutasoorten ontvangt, is die onderbouwing c.q. documenten voor de bank acceptabel.

3.14 Doorlopend clientenonderzoek door FOD

Voor het effectief tegengaan van ML/FT controleert de relatiebeheerders bij elke fysieke klantencontact, of het klantprofiel (o.a. naw-gegevens, bron van inkomsten en transacties op de bankrekeningen) voldoet aan het bankbeleid. De klant ondergaat daarbij een integriteitstoets en wordt zonodig de klant bijgesteld of gereviseerd. De FoD van de bank constateert of voert dit uit. Bij constatering van ongebruikelijke transacties of bij vermoeden daartoe, wordt daarvan terstond melding gemaakt aan de OII. De klant wordt door de FoD terzake gehoord en zonodig gevraagd om additionele documenten danwel bewijsmiddelen aan te leveren. Indien en voor over de overgelegde documenten door de klant het vermeende ongebruikelijke transacties erklaren of aannemelijk maken, kan dat leiden tot het bijwerken c.q. bijstellen van het klantprofiel en het klantdossier.

Eveneens is het van belang voor de bank om de klantfile waarvan het klantprofiel een inherent onderdeel vormt, periodiek te reviseren. Mede daarvoor categoriseert de bank haar klanten in risicocategorieën low, medium, high, onacceptable. Op grond van deze risicocategorieën voert de bank periodiek doorlopend clientenonderzoek uit, zoals weergegeven in de onderstaande tabel:

Categorie	Omschrijving	Frequentie clientenonderzoek
Low	Op basis van score in client score card	Minimaal om de 5 jaren
Medium	Op basis van score in client score card	Minimaal om de 3 jaren
High	Op basis van score in client score card	Minimaal jaarlijks

Een trigger voor het updaten of reviseren van het klantprofiel kan ook komen vanuit:

a. transactiemonitoring;
b. klantcontact;
c. continuous monitoring.

Zodra de bank constateert dat het klantprofiel is gewijzigd, gaat zij gelijk over tot uitvoering van hernieuwde clientenonderzoek.

3.15 Updaten van klantdossiers

Ten einde ML/FT tegen te gaan is het noodzakelijk dat de relatiebeheerder continu, bij iedere update, nagaat of het profiel van de klant (o.a. NAW, bron van inkomsten en transacties op de bankrekeningen) voldoet aan het beleid van de bank. Het is noodzakelijk om continu na te gaan of de integriteit van de klant in lijn is met het beleid van de bank. Ook hier wordt de verantwoordelijkheid van de FoD benadrukt. Dit dient te geschieden in het kader van de continue revisie van het klantprofiel. Indien er ongebruikelijke transacties door de eerste lijn wordt geconstateerd, wordt dit ter stond gemeld aan de OII.

3.16 First line of defense (FoD) en Second line of defense (SoD)

Het naleven en het monitoren van AML/CFT maatregelen en procedures behoren tot de verantwoordelijkheid van de gehele bank. De FoD doet de eerste integriteitsscreening (KYC/CDD), onder meer bij:

a. on-boarding;
b. revisie en;
c. bij iedere transactie m.b.t. het transactiegedrag in relatie tot het vastgesteldetransactieprofiel.

Vervolgens is de SoD, met name de OII, verantwoordelijk voor de kwaliteitscontrole door OII op verzoeken van de door de FoD aangeleverde verzoeken m.b.t. uitgevoerde KYC bij de onboarding, revisie en transacties voor hoog risico relaties en transacties. Hiervoor wordt voorafgaand aan de relatie, bij de verwerking van transacties en doorlopende bij het periodieke klantonderzoek onderzoek verricht naar of een klant op een sanctielijst staat en geen transacties uitvoert die verboden zijn door de toegepaste en gehandhaafde economische sancties en embargo's. De screening van high risk klanten houdt een pre-screening in op de onboarding, terwijl de screening van medium en low risk klanten een post-screening betreft. Bij de mediumen low-risk klanten zal er op steekproefsgewijs controle plaatsvinden.

3.17 Machtigingen

Ten einde misbruik van bankproducten waaronder bankrekeningen te voorkomen, dienen gemachtigden en/of procuratiehouders op bankrekeningen een gedegen screening te doorlopen.

Indien een klant een derde op zijn rekening wil machtigen en/of toevoegen, onderzoekt de bank de relatie tussen de klant en die derde. Indien uit dat onderzoek van de bank blijkt van een onzuivere relatie, wordt het verzoek van de klant niet gehonoreerd.

Indien het een zuivere relatie blijkt, voegt de bank de gemachtigde niet toe aan de rekening zolang zij de gemachtigde niet heeft gescreend (KYC/CDD/EDD). Dit geldt eveneens voor toevoeging van additionele personen bij andere bankproducten waaronder doch niet beperkt tot mededebiteur, additionele creditcard houder.

4. TRANSACTIEMONITORING

4.1 Algemeen

Volgens de Wet MOT is de bank onder meer verplicht om een voortdurende controle uit te oefenen op haar zakelijke relaties. Ook moet zij de transacties van haar zakelijke relaties monitoren en bij ontdekking van of bij het vermoeden van een ongebruikelijke transactie zo snel mogelijk daarvan melding doen aan de FIU Suriname. Derhalve is transactiemonitoring een essentiële maatregel om integriteitsrisico's te beheersen. Kortom, het doel van de transactiemonitoring is om de integriteitsrisico's tijdig te ontdekken en die te mitigeren en te beheersen. Voorzover die niet gemitigeerd kunnen worden, worden ze geëlimineerd.

Bij de transactiemonitoring ligt de focus van de bank op:

- Transactiescreening: onder meer screening tegen sanctielijsten, interne watchlist, high risk landenlijst, afwijking;
- Fraude detectie: onder meer detectie van afwijkingen, link analyses, regels.
- Detectie van typologieën van ML/FT.

Voor de transactiemonitoring dient de core banking system mede als een informatiebron met betrekking tot inkomsten van een klant.

Het cliëntenonderzoek is onderdeel van het transactiemonitoringsproces, aangezien de bank daardoor kennis van de cliënt heeft verkregen, waaronder het doel en de beoogde aard van de zakelijke relatie met de cliënt (het type cliënt, het type dienstverlening aan de cliënt en het risicoprofiel van de cliënt). Met die kennis is de bank in staat om risico gebaseerd te beoordelen of bij de door de cliënt uitgevoerde transacties sprake is van ongebruikelijke patronen, die kunnen duiden op witwassen of terrorismefinanciering. Voor de monitoring van transacties van klanten beschikt de bank over een speciaal daarvoor gebouwd elektronisch systeem, de Financial Crime Mitigation (FCM) genaamd. De FCM is ingesteld op twee typen screenings, te weten:

a. real-time screening: de transacties die hierbij in de queue komen worden realtime gescreend met de World-Check database;
b. batch alert screening: hierbij worden transacties gescreend tegen de in FCM ingebouwde scenario's oftewel rules.

Bij de screening wordt het transactieprofiel gebruikt om na te gaan met welke risico's de bank te maken kan krijgen waaronder meer terrorismefinanciering, money laundering, smurfing, fraude/corruptie. Bij gescreende transacties waarbij red flags zijn geconstateerd, worden door de OII diepgaand onderzoek verricht, terzake een besluit te nemen over de acceptatie van die transacties.

De scenario's, voorkomende in de FCM zullen tot stand komen uit een SIRA, uitgevoerd door de OII en RMD, met inachtneming van de wettelijke vereisten die gelden voor transactiemonitoring.

4.2 FCM

De bank verdeelt de transactiemonitoring onderin:

1. Pre-transactiemonitoring;
2. Post-event transactiemonitoring.

4.2.1 Doel

De FCM is een transactiemonitoring tool waarin zowel transactiescreening en transactiemonitoring plaatsvinden. Het doel van de FCM is om mogelijke ongebruikelijke transacties te detecteren, te onderzoeken/screenen en daardoor de integriteitsrisico's voor de bank te mitigeren c.q. elimineren.

4.2.2 Pre-screening

De pre-screening is gebaseerd op real-time screening alvorens een transactie wordt uitgevoerd. Deze screening vindt plaats op de diverse risicolijsten die voorkomen in de World-Check database en in de Internal Watchlist. De pre-screening vindt alleen plaats op de internationale wire transfer (overmakingen) en wordt risk-based uitgevoerd om voornamelijk de risico's jegens de correspondent banken te mitigeren.

4.2.3 Post-screening en de FCM scenario's

De post-screening vindt plaats middels de FCM-module Batch Alert. Voor de monitoring van de Batch Alerts screening zijn er aan de hand van scenario's rules in FCM gebouwd die betrekking hebbende op het transactiegedrag van klanten. Deze screening houdt een post-screening in van de transacties die de vorige dag reeds uitgevoerd zijn via de delivery channels. De uitgevoerde transacties die gehit hebben tegen één of meer scenario's, worden gesorteerd in de daarvoor bestemde queue. Deze transacties worden door de OII onderzocht en voor zover nodig maatregelen getroffen waaronder het ongedaan maken van de transactie, het uitvoeren van hernieuwde (verscherpte) clientenonderzoek, verrichten van melding aan FIU Suriname.

De scenario's zijn gebaseerd op wettelijke regelingen en de door de bank uitgevoerde SIRA. Deze scenario's worden jaarlijks door de OII geëvalueerd en het resultaat daarvan wordt gerapporteerd aan de RCC en RC. Voor zover OII onregelmatigheden of onvolkomenheden ontdekt of waarneemt met betrekking tot het adequaat functioneren van de rules brengt zij advies uit en doet voorstellen aan de RCC en RC tot wijziging c.q. aanpassing van de rules.

5. CONTINUOUS MONITORING

5.1 Algemeen

Het uitvoeren van een voortdurende controle op de zakelijke relatie en diens transacties behoort tot een van de belangrijke verplichtingen van de bank. Deze voortdurende controle staat bekend onder de term "continuous monitoring". De continuous monitoring dient als een van de belangrijke maatregelen die de bank neemt ter bestrijding van witwassen en financiering van terrorisme. Zowel de FoD als de OII zijn hiervoor verantwoordelijk. Bij het uitvoeren van de continuous monitoring maakt de bank onderscheid in:

a. periodic review: periodiek past de bank review toe op haar klanten.

b. event-driven review: deze wordt ondermeer toegepast bij signalen, hits, incidenten, afname van nieuwe producten en diensten.

5.2 De rol van de FoD

De FoD is verantwoordelijk voor het geregeld monitoren van de zakelijke relatie waaronder de optredende veranderingen in de Customer Master (CM), waaronder het klantprofiel. Dit kan plaatsvinden door veranderingen in de bedrijfsactiviteiten, doeluitbreiding of doelbeperking, aandelenoverdracht, wijziging van bestuurders en toezichthouders, veranderingen van werkgever, toename of afname van omzet enzovoorts. Na de verrichte review c.q. update van de CM wordt het dossier in de klantfile mede geüpdatet en waarnodig wordt OII van de review c.q. update in kennis gesteld. De FoD zorgt te allen tijde ervoor dat de CM en het dossier van de klant in overeenstemming zijn.

Eveneens zorgt de FoD voor het monitoren van de verrichte transacties met het transactieprofiel van de klant met de beschikbaar gestelde systeem, en bij geconstateerde afwijkingen wordt een review c.q. update gepleegd en waarnodig de OII daarvan in kennis gesteld. Zo nodig, doet de FoD melding aan de OII van geconstateerde ongebruikelijk transacties of een vermoeden daartoe.

5.3 De rol van OII

De OII is belast met het monitoren van de risico's bij cliënten gedurende de zakenrelatie. Bij deze monitoring worden reviews uitgevoerd op de volgende wijze:

- event-driven review;
- periodic review.

De event-driven review voert zij uit:

a. na verkregen melding van de FoD over een door deze laatste uitgevoerde review. Dit review houdt in het reviewen van de door de FoD geupdated CM en het klantdossier en het valideren daarvan.
b. na verkregen melding van het proces "Transactie Monitoring" van de OII die tijdens het uitvoeren van werkzaamheden met betrekking tot financial crime identification op basis van alerts c.q. red flags onregelmatigheden of misstanden zoals crime detection waarneemt of constateert. In dat geval draagt het proces Transactie Monitoring het onderzoek over aan hetproces Continuous Monitoring. Deze laatste draagt zorg voor de paper trail en diepgaand onderzoek terzake.
c. na verkregen melding van het proces "Reporting" die tijdens het samenstellen van rapportages ten behoeve van de CBvS en/ of FIU Suriname onregelmatigheden of misstanden waarneemt of constateert. Alle beschikbare documenten worden overgedragen aan het proces Continuous Monitoring voor financial crime investigation.

De periodic review behoort eveneens tot een van de belangrijke taken van het proces Continuous Monitoring. Dit houdt in het op periodieke basis uitvoeren van de volgende controles:

1. Review van klantprofiel;
    a. De bank zorgt ervoor dat de gegevens die zij tijdens het cliëntenonderzoek heeft verzameld over onder meer de klant en zijn bedrijf actueel worden gehouden.
    b. Het reviewen houdt een periodieke beoordeling in of een client nog steeds in de juiste risicocategorie is ingedeeld.
    c. Bij de review wordt de risicogebaseerde benadering gehanteerd hetgeen inhoudt dat de frequentie en de intensiteit van de review samenhangt met de risicocategorie waarin de klant is ingedeeld.
2. Review van transacties;
    a. De bank controleert of de transacties van de klant een ongebruikelijk karakter hebben. Het gaat hierbij om transacties die van het normale en verwachte transactiepatroon van de klant afwijken.
    b. De bank beoordeelt de transacties die door of ten behoeve van of ten gunste van de klant zijn verricht.
    c. Het doen van een melding aan de FIU Suriname in de gevallen waarbij de bank een (voorgenomen) ongebruikelijke transactie signaleert
3. Review van klantdossier;
    a. het completeren van het klant dossier met actuele documenten betreffende de klant en zijn bedrijf.
    b. het (doen) bewaren van de klantdossiers met inachtneming van de bewaartermijn zoals aangegeven in deze policy.
4. Review van US Persons;
    De bank controleert jaarlijks het dossier van de US Person teneinde de FATCA rapportages aan de IRS te verrichten.
5. Review op banksystemen.
    a. het doen van review over het adequaat functioneren van de banksystemen en het doen van voorstellen dan wel het uitbrengen van advies ter aanpassing van de banksystemen.

6. POLITICALLY EXPOSED PERSON

6.1 Omschrijving van PEP

Een politically exposed person oftewel een politiek prominente persoon (PEP) wordt door de bank omschreven als een persoon die in Suriname of in het buitenland een vooraanstaande publieke functie bekleedt of heeft bekleed, alsmede diens directe familieleden en naaste geassocieerden van een dergelijke persoon.

6.2 PEP categorieën

Vanwege hun positie en invloed, wordt erkend dat veel PEP's zich in posities bevinden die mogelijk kunnen worden misbruikt voor het plegen van witwasdelicten (ML) en aanverwante basisdelicten (predicate offenses), met inbegrip van corruptie en omkoping, evenals het uitvoeren van activiteiten die verband houden met terrorismefinanciering (TF).

PEP's worden onderscheiden in vijf categorieën:

1. Buitenlandse PEP: individuen aan wie prominente openbare/ overheidsfuncties zijn toevertrouwd door een vreemd land, waaronder doch niet beperkt tot staatshoofden of hoofde van de overheid, hoge politici, hogere overheidsfunctionarissen, gerechtelijke of militaire ambtenaren, senior bestuursleden van staatsbedrijven, belangrijke functionarissen van politieke partijen.
2. Binnenlandse PEP: individuen aan wie prominente openbare/ overheidsfuncties zijn toevertrouwd in Suriname, waaronder doch niet beperkt tot staatshoofden of hoofde van de overheid, hoge politici, hogere overheidsfunctionarissen, gerechtelijke of militaire ambtenaren, senior bestuursleden van staatsbedrijven, belangrijke functionarissen van politieke partijen.
3. PEP van Internationale Organisaties: personen aan wie een belangrijke of een prominente functie is toevertrouwd door een internationale organisatie. Dit verwijst naar onder meer leden van het hoger management of personen die met gelijkwaardige functies zijn toevertrouwd, d.w.z. directeuren, adjunct-directeuren en bestuursleden of gelijkwaardige functies.
4. Familieleden van PEP: zijn individuen die ofwel direct gerelateerd zijn aan een PEP (bloedverwantschap) of door huwelijk of soortgelijke (burgerlijke) vormen van partnerschap.
5. Naasten van PEP / Close Associates: zijn ook individuen die nauw verbonden zijn meteen PEP, sociaal of professioneel.

6.3 Algemene maatregelen t.a.v. PEP's

De bank treft de navolgende maatregelen voor de acceptatie en behoud van PEP's:

a. De bank classificeert PEP's als high risk en voert te allen tijde EDD uit alvorens een PEP wordt geaccepteerd als klant.
b. Een zakelijke relatie met een PEP wordt in beginsel aangegaan na verkregen goedkeuring van de RCC conform het besluitvormingsproces zoals beschreven in de RCC Charter. Echter indien na een risk based approach gebleken is dat de PEP laag risico's met zich meebrengt kan de goedkeuring plaatsvinden door OII. Een voorbeeld van de PEP met een lage risico zijn zij die slechts het toegekende salaris giraal binnenkrijgen vanuit de werkrekeningen van de overheidsinstantie alwaar zij werkzaam zijn en blijven ze aangemerkt als high risk voor monitoringsdoeleinden.
c. Alle PEP's – nieuwe als bestaande – worden in de klantfile voorzien van een PEP-code / high risk code.
d. Bij het uitvoeren van due diligence onderzoekt de bank of de natuurlijke persoon (prospect) of de bestuurder en/of UBO van een rechtspersoon of een andere juridische constructie PEP is.
e. Indien bij de revisie of bij monitoring blijkt dat natuurlijke personen of de bestuurders en/of UBO's van rechtspersonen of andere juridische constructies van bestaande klanten een PEP is, wordt het voorgelegd aan de RCC voor besluitvorming of de relatie met die klant wordt gecontinueerd of beëindigd. In het geval van een besluit tot continuering van de klantrelatie, wordt de klantfile van die klant voorzien van een PEP-code / high risk code.

f. Voor een binnenlandse PEP die tegelijkertijd ook een buitenlandse PEP is vanwege een andere prominente publieke functie in een ander land, gelden de eisen van de buitenlandse PEP.
g. De bank gaat geen zakelijke relatie aan of handhaaft geen zakelijke relatie als zij weet of vermoedt dat de tegoeden verkregen zijn uit corruptie of misbruik van overheidsmiddelen, onverminderd de verplichting die de bank heeft volgens het strafrecht of andere wetten of richtlijnen.
h. De bank verzamelt voldoende informatie van een nieuwe cliënt en raadpleegt openbaar beschikbare informatie om vast te stellen of een cliënt als een PEP moet worden aangemerkt.
i. De bank is bewust dat het aangaan of onderhouden van zakelijke relaties met familieleden en partners (close associates) van PEP's de reputatie van de bank op dezelfde wijze kan schaden als die met de PEP zelf. Vandaar dat de bank dezelfde maatregelen toepast bij deze groepen als bij de PEP.
j. De bank onderzoekt de herkomst van de tegoeden van een PEP voordat zij overgaat tot het accepteren van een PEP.
k. Naast de gebruikelijke CDD-maatregelen beschikt de bank over een risico beheersingssysteem welke de gradatie van iedere PEP vaststelt die de bank blootstelt aan risico's.

6.4 Specifieke maatregelen t.a.v. PEP's

De bank treft onder meer de volgende specifieke maatregelen ten aanzien van PEP's:

1. De bank heeft procedures in place voor de vaststelling van de bron van het vermogen van cliënten en uiteindelijk belanghebbenden die als PEP zijn aangemerkt.
2. Iedere PEP wordt door de bank als high risk beschouwd en als zodanig aangemerkt en voert de bank doorlopende controle uit op de zakelijke relatie.
3. De risico's die PEP's met zich meebrengen kunnen per risicofactor (klant, product of dienst, land en industrie) verschillen. De bank zal daarom de identificatie, het monitoren en het beheren van de rekeningen en transacties van de PEP's op basis van risk-based approach uitvoeren.
4. De vaststelling van het klantprofiel van de PEP's waarin onder meer het doel van de rekening, de inkomstenbronnen waaruit de rekening gevoed zal worden, de hoogte van de maandelijkse stortingen worden door de bank nauwkeurig vastgelegd.
5. De bank voert risk-assessments uit op de zakelijke relatie waarbij de nadruk ligt op de volgende aspecten:
   a. de functie en verantwoordelijkheid van de persoon, aard en hoogte van zijn inkomsten (salaris of honorarium);
   b. de mate en aard van zijn bevoegdheid of invloed over overheidsactiviteiten of over andere functionarissen;
   c. de mate van toegang tot significante overheidsbezittingen en fondsen;
   d. financiële informaties en beroepsachtergrond;
   e. de sector waarin hij opereert;
   f. de geografische ligging van zijn kantoren of zaken;
   g. de toegang tot en beheer of invloed op overheids- of corporate-rekeningen;

h. de mate van betrokkenheid van de tussenpersonen, leveranciers, vendors en agenten in de industrie of de sector waarin de PEP actief is;
i. het oneigenlijk gebruik van corporate vehicles en andere juridische entiteiten om eigendom, bezittingen of vermogen te verduisteren.

6. Het regelmatig monitoren van diverse risicofactoren, zoals de producten en diensten waarvan de PEP gebruik maakt, de frequentie van gebruik, de grootte en complexiteit vande transacties.
7. Het uitoefenen van doorlopend toezicht op de zakelijke relatie.

6.5 Aanvullende maatregelen t.a.v. binnenlandse PEP's

Bestuurders van een rechtspersoon die een hoog bestuurlijk ambt (regeringsambt) aanvaarden, worden niet onboard. Dit is van toepassing op de rechtspersonen. Indien blijkt dat de klant reeds bestaande klant is wordt geadviseerd dat de bestuurder afstand doet van zijn bestuursfunctie in die rechtspersoon en dient het klantprofiel herbeoordeeld te worden. Indien de klant zulks weigert wordt de klantrelatie beëindigd.

Bovenstaande maatregel geldt alleen voor prospects en bestaande klanten die een hoog bestuurlijk ambt (regeringsambt) aanvaarden vallende onder de uitvoerende, wetgevende en rechterlijke macht. Met hoog bestuurlijk ambt wordt bedoeld personen in de volgende functies:

1. Personen met functies in de Nationale Assemblee en de Regering. Onder deze macht vallen o.a. de volksvertegenwoordigers met name DNA leden, Ressort leden.
2. De President, Staatshoofd, de Vice President en Ministers.
3. Rechters en overige leden van het hof van Justitie, de Procureur-Generaal,Functionarissen met een hoog bestuurlijke ambt bij het Openbaar Ministerie en Leden van het Constitutioneel Hof.

6.6 Speciale aandacht t.a.v. relaties met PEP's

Wanneer uit de customer due diligence blijkt dat het betrefteen directe familielid of naaste medewerker van een PEPdient de geldbron afkomstig van de PEP en of de geld- en vermogensbronnen van de PEP bepaald en gedocumenteerd te worden. Bij constatering van Bad press (Negatief nieuws/nadelige media Screening) van de PEP die de rekening financiert, kan worden vastgesteld of de PEP opzettelijk heeft geprobeerd hun betrokkenheid bij de financiering van de rekening te verhullen. Relaties met PEP's kunnen verhoogde risico's met zich meebrengen vanwege de mogelijkheid dat personen die dergelijke functies bekleden hun macht en invloed kunnen misbruiken voor persoonlijk gewin of voordeel, of voor persoonlijk gewin of voordeel van naaste familieleden en naaste medewerkers.

Dergelijke personen kunnen ook hun familie of naaste medewerkers gebruiken om fondsen of activa te verbergen die verduisterd zijn als gevolg van misbruik van hun officiële functie als gevolg van omkoping en corruptie. Daarnaast kunnen ze ook proberen hun macht en invloed te gebruiken om vertegenwoordiging en/of toegang tot of controle over juridische entiteiten voor soortgelijke doeleinden te verkrijgen.

6.7 Reikwijdte voor het categoriseren als PEP's

De Wet Identificatieplicht Dienstverleners geeft aan dat directe familieleden en naaste geassocieerden van een dergelijke persoon (de PEP) ook tot PEP gerekend worden. Echter is er geen definitie gegeven wat er verstaan moet worden onder directe familieleden. De FATF Recommendations 12 geeft ook geen definitie qua reikwijdte om familieleden als PEP te categoriseren, maar geven wel indicatoren aan om een besluit te kunnen nemen. Volgens FATF dient risico gebaseerd gekeken te worden naar de relatie tussen de PEP en de persoon, alsook de cultuur van het land (Suriname).

Het gaat om de mogelijke invloed die de persoon kan hebben op de PEP, vanwege de familieband. Er dient dus risico gebaseerd o.b.v. de gegeven indicatoren, de band met de PEP bekeken te worden om de persoon ook als PEP te categoriseren. Primair zal de focus gelegd worden op de eerstegraads familieleden zoals: partner, ouders (ook adoptie- en stiefouders), schoonouders, kinderen (ook adoptie- en stiefkinderen), schoondochters- en schoonzonen. Indien in het kader van de risk-based approach het noodzakelijk is verder te gaan dan de eerstegraads familieleden.

6.8 Weigering of de-risking van PEP's

Indien uit onderzoek of uit betrouwbare bronnen blijkt dat het vermogen (geld en goederen) van de PEP's mogelijk zijn verkregen uit onder meer corruptie of misbruik van overheidsmiddelen, zal de bank de aanvraag tot het aangaan van een klantrelatie weigeren, of een bestaande zakelijke relatie beëindigen.

6.9 Verlies van PEP-status

Wanneer een klant die door de bank aangemerkt was als een PEP of een rechtspersoon wiens UBO aangemerkt was als PEP, niet langer met een prominente openbare functie is belast of bekleedt, wordt tot een jaar nadat hij opgehouden heeft de vooraanstaande openbare functie te bekleden, als een politiek prominente persoon aangemerkt. Na dat jaar zal de bank bij de afhandeling van zijn PEP-status zich baseren op een risicobeoordeling. Deze regeling is van overeenkomstige toepassing op directe familieleden en naaste geassocieerden van de PEP.

7. CORRESPONDENT BANKING EN SAMENWERKING TUSSEN BANKEN

7.1 Algemeen

Voor de werking van deze policy wordt onder correspondent banking oftewel correspondentbankieren verstaan een overeenkomst tussen twee banken waarbij de ene bank (correspondent) rekeningen en/of deposito's aanhoudt die eigendom zijn van de andere bank (respondent) en betalings- en andere diensten verleent aan die respondenten bank.

Onder correspondent bankrelatie wordt verstaan een vaste relatie tussen een bank in Suriname en een buiten Suriname gevestigde bank voor de afwikkeling van transacties of de uitvoering van opdrachten ten behoeve van de klanten van de bank.

7.2 Het aangaan van grensoverschrijdende samenwerking

7.2.1 Finabank als respondent bank

Voor het adequaat verlenen van internationale betalingen, kan voor de bank noodzakelijk blijken om overeenkomsten aan te gaan met banken in het buitenland voor het tot stand brengen van een samenwerking. Deze samenwerking wordt ook wel aangeduid met de term "grensoverschrijdende samenwerking".

Het adequaat onderhouden van deze relatie is voor de bank van groot belang. De bank heeft voor dat doeleinde ervoor verkozen om OII als centraal punt aan te wijzen in de communicatie c.q. correspondentie over AML/CFT vraagstukken of aangelegenheden met de correspondent bank. De FoD is verantwoordelijk om erop toe te zien dat alle vragen of onderzoekingen (investigations) vanuit de internationale banken waarmee de bank een samenwerking heeft worden doorgeleid naar de OII voor verdere afhandeling.

Alvorens Finabank als respondent bank een grensoverschrijdende samenwerking aangaat, zal zij de volgende maatregelen nemen:

1. het uitvoeren van KYC/CDD of een verscherpt clientenonderzoek (EDD) op de correspondent bank. Dit wordt uitgevoerd door OII. Daarbij zorgt de bank ervoor dat zij voldoende informatie over de correspondent bank verzamelt om:
    a. een volledig beeld te krijgen van de aard van haar bedrijfsactiviteiten;
    b. de reputatie van de correspondent bank vast te stellen;
    c. de kwaliteit van het toezicht dat op die bank wordt uitgeoefend vast te stellen;
    d. informatie over eventuele onderzoeken ter zake van witwassen en financiering van terrorisme of uit hoofde van toezicht genomen maatregelen te achterhalen.
2. het beoordelen van de procedures en maatregelen ter voorkoming van witwassen en financiering van terrorisme van de correspondent bank en vergewist zich ervan dat deze adequaat en doeltreffend zijn.
3. het schriftelijk vastleggen van de verantwoordelijkheden van beide banken op het gebied van de voorkoming en bestrijding van witwassen en financiering van terrorisme in een overeenkomst die door beide partijen rechtsgeldig wordt ondertekend.
4. het verkrijgen van toestemming van de RCC voor het aangaan van de relatie met de correspondent bank.

7.2.2 Verscherpt cliëntenonderzoek

Finabank ziet erop toe dat ook na het sluiten van de overeenkomst tot samenwerking met de grensoverschrijdende bank jaarlijks een verscherpt cliëntenonderzoek wordt uitgevoerd.

7.2.3 Finabank als correspondent bank

Wanneer Finabank in de hoedanigheid van correspondent bank een relatie aangaat met een respondent bank, ziet zij erop toe dat zij zowel voorafgaand aan de zakelijke relatie of de transactie, als gedurende de zakelijke relatie, en wel halfjaarlijks, een verscherpt cliënten onderzoek verricht op de respondent bank.

Zij ziet voornamelijk erop toe dat de respondent banken geen relaties onderhouden met Shell Banks of hun rekeningen bij Finabank laten gebruiken door Shell Banks.

In Suriname is met de introductie van SNEPS door de CBvS niet langer sprake van een één op één relatie tussen banken in Suriname voor wat het interbancair betalingsverkeer betreft. Met SNEPS vindt een interbancaire clearing via de CBvS plaats, hetgeen inhoudt dat de clearing en settlement via de CBvS plaatsvindt.

Op de giro- of spaarrekeningen die lokale banken bij Finabank openen, vallen onder de categorie "cliëntenrekeningen" waarop de voorwaarden van de bank van toepassing zijn. De bank staat niet toe dat deze rekeningen rechtstreeks gebruikt worden door klanten van die banken.

7.3 Correspondent bankrelatie met Shell Banks

Een Shell Bank is een bank die is opgericht in een land waar ze niet fysiek aanwezig is, niet wordt gereguleerd door de toezichthouder (centrale bank) en mogelijk niet tot een gereguleerde financiële groep behoort.

Finabank gaat geen correspondent bankrelatie aan met een Shell Bank, noch onderhoudt zij enige relatie met een Shell Bank. Zij vergewist zich ook ervan dat de grensoverschrijdende bank met wie zij een correspondent bankrelatie aangaat of onderhoudt, hun rekeningen niet laten gebruiken door Shell Banks.

In geval uit haar onderzoek blijkt dat de grensoverschrijdende bank dit wel doet, beëindigt zij de correspondent bankrelatie onverwijld en doet daarvan melding aan de FIU Suriname.

7.4 Transitrekeningen/ Payable-through-accounts

Voor de werking van deze policy wordt onder transitrekening verstaan een bankrekening die door een respondent bank bij een correspondent bank wordt aangehouden waartoe derde partijen rechtstreeks toegang hebben voor de uitvoering van transacties ten behoeve van zichzelf. De derde partijen kunnen zijn cliënten van de respondent bank die op die rekening debiteringen of crediteringen kunnen plegen zonder tussenkomst van de correspondent bank. De transitrekening wordt door Finabank gecategoriseerd als een high risk rekening. Derhalve staat Finabank niet toe dat haar rekeningen bij correspondent banken als transitrekeningen worden gebruikt door haar klanten. Eveneens laat de bank in beginsel niet toe dat haar General Ledger Accounts (GL-accounts) door klanten rechtstreeks gebruikt worden voor het plegen van transacties. Stortingen op de GL-accounts door klanten kunnen slechts plaatsvinden met toestemming van de bank.

8. ONGEBRUIKELIJKE TRANSACTIES

8.1 Algemeen

Ingevolge de Wet MOT is de bank verplicht ongebruikelijke transacties op basis van objectieve en/of subjectieve indicatoren te melden aan FIU Suriname. Deze indicatoren vinden hun grondslag in het Besluit Indicatoren Ongebruikelijke Transacties. De meldingsplicht berust bij de OII.

8.2 Objectieve indicatoren

De objectieve indicatoren die tot meldingsplicht leiden zijn onder meer:

1. Alle contante of girale transacties (inclusief het verzilveren van cheques) met een waarde vanaf USD 10,000.00 of de tegenwaarde in een andere valutasoort.
2. Transacties met landen, organisaties of personen, die op zwarte lijsten of sanctielijsten voorkomen.
3. Transacties, die in verband kunnen worden gebracht met mogelijke witwassen of terroristische misdrijven.
4. Contante transacties met een waarde van USD 10,000.00 of meer waarbij contante omwisseling in een ander valuta of van kleine naar grote coupures plaatsvindt.
5. Transacties met (rechts-)personen, die zijn gevestigd in landen of jurisdicties die zijn aangewezen als landen of jurisdicties, die niet of onvoldoende voldoen aan internationaal gangbare normen op het gebied van AML/CFT.
6. Alle verdachte zaken, die op basis van observaties of anderszins, uit het banksysteem blijken en duiden op witwassen, financiering van terrorisme of enig ander strafbaar feit.
7. Alle gevallen van identiteitsfraude.
8. Bij onverklaarbare afwijkingen met het klantprofiel.

8.3 Subjectieve indicatoren

De subjectieve indicatoren die tot meldingsplicht leiden zijn onder meer:

1. wanneer de bank aanleiding ziet tot of indicaties heeft te veronderstellen dat de transacties verband kunnen houden met witwassen of financiering van terrorisme;
2. wanneer het cliëntenonderzoek de door de wet voorgeschreven gegevens niet heeft opgeleverd;
3. wanneer een bestaande klantrelatie wordt beëindigd omdat niet alle door de wet voorgeschreven gegevens is verkregen;
4. wanneer er een onverklaarbare discrepantie tussen geld- en goederenstroom bestaat. Een cliënt behaalt ongebruikelijk hoge omzetten en/of winsten waarvan niet duidelijk is met welke activiteiten deze verdiend zijn;
5. wanneer een transactie waarbij een cliënt betrokken is, leidt tot een resultaat dat duidelijk hoger of lager is dan werd verwacht; of er is een ongebruikelijk hoog resultaat vergeleken met vergelijkbare ondernemingen in de branche van de cliënt, met name wanneer de omzet voor een belangrijk deel uit contante verkopen bestaat;
6. wanneer een transactie waarbij een klant betrokken is, geschiedt onder duidelijk slechtere voorwaarden dan redelijkerwijs te verwachten is, zonder dat er een acceptabele verklaringis waarom er niet voor een betere structurering gekozen is;
7. wanneer de herkomst van de gelden niet te verklaren of te verifiëren is.

8.4 Melding aan FIU Suriname - schending geheimhoudingsplicht

De Directie en medewerkers van Finabank die te goeder trouw inlichtingen verstrekken aan de FIU Suriname op grond van de WMFT, zijn gevrijwaard van strafrechtelijke en civielrechtelijke aansprakelijk voor de schending van een verbod op onthulling van informatie uit hoofde van een overeenkomst of een wettelijke of bestuurlijke bepaling.

8.5 Verbod op Tipping-off

De bank, haar Directie en medewerkers houden zich strikt aan de wettelijke verbodsbepaling met betrekking tot tipping off. Ze doen geen mededeling aan de betrokken klant of aan derde persoon over wie de bank een melding heeft gedaan of voornemens is te doen aan de FIU Suriname, dat overeenkomstig de Wet MOT inlichtingen zijn verstrekt aan de FIU Suriname. Eveneens onthouden zij zich van enige mededeling aan klant of de derde partij dat er een onderzoek naar money laundering, terrorismefinanciering en belastingontduikingsactiviteiten wordt uitgevoerd, tenzij de FIU Suriname anders verlangt.

9. TRANSACTIES MET WISSELKANTOREN EN VALUTAVERKOPERS

Indien en voorzover de bank vanwege slechte financieel-economische situatie in het land genoodzaakt wordt zaken te doen met cambio's en personen die valuta verhandelen, zal zij de transacties tot stand brengen met inachtneming van de volgende niet limitatief opgesomde beheersmaatregelen om zodoende integriteitsrisico's te mitigeren.

1. De bank voert een verscherpt clientenonderzoek (EDD) uit op iedere cambio c.q. valutahandelaar waarmee zij zaken doet of gaat doen, terwijl het dossier beschikbaar en up-to-date wordt gehouden. Onderdelen van dit EDD zijn:
   a. Controle van onder meer de volgende documenten ter identificatie van de cambio c.q. valutahandelaar:
      - KKF-uittreksel
      - Statuten
      - Jaarrekening, opgemaakt door een Finabank erkende accountant.
   b. Onderzoek op bad press (searches in beschikbare nationale en internationale bronnen).
   c. Identificatie van bestuurders, RvC en UBO's ongeacht de hoeveelheid aandelen.
   d. Definitieve ontvangstbevestigingen van gedane meldingen aan FIU Suriname.
   e. Toetsing aan de toepasselijke vereisten van de Wet Toezicht Geldtransactiekantoren, Wet Identificatieplicht Dienstverleners en Wet Melding Ongebruikelijke Transacties.
   f. Een ondertekende kopie van de Finabank versie van de Wolfsberg Questionnaire voor cambio's.
2. Zesmaandelijks wordt een review van de status van de cambio gedaan door Treasury met ondersteuning c.q. begeleiding van de OII en het verslag met bevindingen en conclusiesvoorgelegd aan de RCC.
3. De transacties worden over-the-counter gedaan (OCT-transacties). Deze behoren tot de incidentele transacties. De bank accepteert hierbij slechts de transactie en niet de derde partij.
4. Bij de totstandkoming van transacties dient de herkomst van de middelen of de bron van inkomsten onderbouwd te worden verklaard waaronder doch niet beperkt tot een overzicht met de namen van de klanten van wie de cambio de gelden heeft gekocht c.q. gewisseld: KYCC-uitvoering. Het format van het overzicht kan door de bank worden bepaald met inachtneming van de vereisten in o.a. de Wet Identificatieplicht

Dienstverleners. De cambio is niet toegestaan om overzichten van andere cambio's te overleggen.

5. Bij fx-transacties dienen de onderliggende documenten ter onderbouwing van de herkomst eerst door de Treasury onder toepassing van dit beleid te worden gescreend alvorens de fx-transactie wordt goedgekeurd en/of uitgevoerd.
6. Het doen van zaken met cambio's c.q. valutahandelaren is de verantwoordelijkheid van de Treasury, terwijl de OII deze monitoort.
7. Bij het plegen van transacties bij de kassa's van de bank waarbij de klant als herkomst van de middelen aangeeft dat hij die verkregen heeft middels een wisseltransactie of omzetting bij een cambio, vereist de bank in dat geval in het kader van KYC/CDD dat de klant naast de vereiste documentatie ook overlegt de kwitantie van de omzetting welke hij verkregen heeft van de cambio. Daarnaast zal de klant de herkomst van de middelen die hij bij de cambio heeft gewisseld ook aan te tonen, tenzij het een girale transactie van de klant vanuit Finabank naar de cambio betreft.

10. "NON-FACE TO FACE" ZAKELIJKE RELATIES OF TRANSACTIES

De bank maakt onderscheid tussen face-to-face zakelijke relaties/transacties en non-face-toface zakelijke relaties / transacties. Onder face-to-face zakelijke relaties / transacties wordt in deze policy verstaan een zakelijke relatie / transactie die aangegaan/uitgevoerd is waarbij voldaan is aan twee cruciale elementen van KYC, namelijk het zien en het spreken van de klant. Hieronder vallen ook het aangaan van zakelijke relaties of het plegen van transacties waarbij de KYC terzake middels encrypted video-conferences heeft plaatsgehad.

Voor de werking van deze policy wordt onder non-face-to-face zakelijke relaties / transacties verstaan een zakelijke relatie / transactie die aangegaan/uitgevoerd is zonder dat er sprake is van het voldoen aan de twee cruciale elementen van KYC, zien en spreken van de klant.

10.1 Non-face to face zakelijke relatie (NFTF KYC)

Voor de werking van deze policy wordt onder NFTF KYC verstaan het proces waarbij de bank due diligence uitvoert op een klant zonder hem face-to-face gezien en gesproken te hebben. Vanwege het risico bij de onboarding van een klant die niet 'bekend' is, vereist de bank van haar FoD dat zij cliëntenonderzoeksmaatregelen uitvoeren die minstens zo streng zijn als de maatregelen die zouden moeten worden genomen als er persoonlijk contact zou zijn om het risico dat door NFTF wordt genomen, te minimaliseren.

De voornaamste problemen/ risico's bij NFTF KYC:

1. Toetsing van de klantidentificatie en verificatie.
2. Toetsing van de echtheid van de handtekening van de klant of diens vertegenwoordigers.
3. Controle van documenten op echtheid.
4. Onvolledige KYC waardoor het klantprofiel niet volledig kan worden vastgesteld vanwege het ontbreken van een contextueel gesprek waaruit middels vragen en doorvragen belangrijke

informatie over de klant of diens bedrijf in de ruimste zin wordt verkregen.

10.1.1 Risicomitigatie maatregelen

De bank heeft risico gebaseerde maatregelen genomen om de risico's van NFTF KYC te beheersen c.q. te mitigeren waaronder:

1. het vaststellen van procedure ter uitvoering van NFTF KYC.
2. identificatie en verificatie van nieuwe klanten:
    a. het screenen van aangeleverde documenten op echtheid en/of echtheidskenmerken.
    b. het controleren van handtekeningen met aangeleverde identificatiedocumenten.
    c. de nieuwe klant dient zelf de afzender te zijn van alle documenten of informatie.
    d. acceptatiecriteria voor gescande kopieën van identificatiedocumenten (in full colour en hoge resolutie);
    e. video-opname van specifieke gezichtsherkenning waarbij cliënt ID naast het gezicht houdt;
    f. Indien de cliënt al bankiert: vereiste van afgeleide identificatie: eerste overboeking van een rekening bij een andere bank waarop adequaat AML/CFT toezicht wordt uitgeoefend;
    g. Goedkeuring van het hoger leidinggevend personeel.
3. identificatie en verificatie van digitale handtekeningen voor bestaande relaties:
    a. het screenen van aangeleverde documenten op echtheid en/of echtheidskenmerken.
    b. het verifiëren van digitale handtekeningen middels een check in core banking system.
    c. de klant dient zelf de afzender van de documenten of informatie te zijn.
4. het persoonlijk afhalen van debit cards door klanten zijnde natuurlijke personen (retail customers) waarbij de identificatie – alhoewel achteraf – toch nog face-to-face plaatsvindt middels overlegging van een identificatiebewijs, controle van de handtekening en zonodig het voeren van een gesprek.
5. het verstrekken van gecertificeerde identificatiedocumenten door een advocaat of notaris voorzover de klant buiten de grenzen van Suriname bevindt.
6. het afleggen van een on-site visit bij bedrijven en het spreken van keypersons: o.a. eigenaren, statutaire vertegenwoordigers, procuratiehouders.
7. het verifiëren van bepaalde door de klant aangeleverde documenten met openbare bronnen zoals de registers die worden bijgehouden door KKF, CBB, M.I. GLIS;
8. het verifiëren van documenten, afgegeven door werkgevers, rechtstreeks met de werkgever.
9. het zelf opvragen van belangrijke documenten van een bedrijf zoals uittreksels uit openbare registers van KKF, statuten, instellingsbesluiten.
10. het gebruik van de bankbronnen voor identificatie en verificatie van bestaande klanten.
11. introductie van nieuwe klanten via tussenpersonen, waaronder de werkgever van de klant, een pensioenfonds, vakorganisatie of een bestaande klant van de bank met goede reputatie.
12. geen non-face tot face onboarding van nieuwe klanten.

10.2 Non-face to face transactie (NFTF Transacties)

Voor de werking van deze policy wordt onder NFTF Transacties verstaan transacties die plaatsvindt zonder dat een klant fysiek aanwezig hoeft te zijn in de bank. Deze transacties worden uitgevoerd middels gebruikmaking van technologieën onder meer internetbankieren, telefonisch bankieren, debet cards en creditcards, ATM's en POS-apparaten. Deze transacties worden ook "transacties op afstand" genoemd.

Deze transacties op afstand zijn riskanter en gevoeliger voor money laundering en terrorisme financiering dan transacties van aangezicht tot aangezicht, aangezien de primaire identificatiemaatregelen die moeten worden uitgevoerd niet kunnen bestaan uit het matchen van het gezicht van de klant met een document.

10.2.1 Risicomitigatie maatregelen

Teneinde de ML/FT risico's te mitigeren, heeft de bank de volgende maatregelen getroffen:

1. De bank ziet erop toe dat zowel nieuwe als bestaande technologieën via welke zij haar diensten en producten aanbiedt aan de klant geen anonimiteit bevorderen.
2. De bank stelt een redelijke drempels vast met betrekking tot transacties bij gebruik van de technologieën door klanten.
3. De bank voert permanente controle (monitoring) en verscherpt onderzoek uit op de transacties van de klanten.
4. De bank heeft controle- en detectiesystemen ingevoerd om ML/FT risico's en fraude te detecteren.
5. De bank bewaart de transactiegegevens conform de bewaartermijn op een zodanige wijze dat reconstructie van individuele transacties mogelijk is.
6. Vóór de eerste storting moet de klant lijfelijk aanmelden bij de bank.

11. COMPLEXE EN GROTE TRANSACTIES EN ACTIVITEITEN

De bank schenkt bijzondere aandacht aan alle complexe en ongebruikelijk grote transacties en alle ongebruikelijke transactiepatronen zonder verklaarbaar economisch of legaal doel. Zij onderzoekt voor zover mogelijk de achtergrond en het doel van alle complexe, ongewone grote transacties en alle ongewone transactiepatronen waarvan de bevindingen schriftelijk worden vastgelegd en op aanvraag beschikbaar gesteld aan de bevoegde autoriteiten. Bij het geringste vermoeden dat er sprake is van een ongebruikelijke transactie, doet de bank een onverwijlde melding aan de FIU Suriname en verschaft haar daarbij voldoende informatie om een gedegen onderzoek te kunnen verrichten en indien nodig ook de nodige acties te kunnen ondernemen.

Wanneer de bank uit het onderzoek merkt dat de risico's op het witwassen van geld of financiering van terrorisme bij een dezer transacties hoger zijn, verricht zij overeenstemming met de vastgestelde risico's een verscherpt onderzoek (EDD). Zij past daarbij de mate en aard van monitoring van de zakelijke relatie aan om te bepalen of die transacties of activiteiten ongewoon
of verdacht lijken.

12. BUITENLANDSE ZAKENRELATIES IN EN TRANSACTIES NAAR HIGHRISK LANDEN

Er zijn landen die niet over adequate AML/CFT-systemen beschikken en/of geassocieerd worden met criminele activiteiten zoals drugshandel, terrorisme, fraude en corruptie. Daardoor vormen zij een hoger potentieel risico voor de bank. Transacties met klanten uit deze landen kunnen de bank blootstellen aan diverse risico's zoals reputatie risico, juridische risico en integriteitsrisico.
De maatregelen die de bank treft bij zakenrelaties en transacties met natuurlijke en rechtspersonen en financiële instellingen uit deze landen zijn als volgt:

1. het screenen van zakenrelaties en transacties met internationaal geldende lijst van landenrisico's waarbij – in geval een high risk land betreft – er een verscherpt onderzoek (EDD) wordt uitgevoerd alvorens de zakenrelatie wordt geaccepteerd of de transactie wordt uitgevoerd. In geval het een gesanctioneerd land of persoon betreft, voert de bank die transactie niet uit;
2. het betrachten van voorzichtigheid bij de acceptatie van gecertificeerde documenten van personen en instellingen uit deze landen, aangaande de legitimiteit en betrouwbaarheid van deze documenten;
3. wanneer transacties van of naar deze landen geen verklaarbaar economisch of legaal doel hebben, onderzoekt de bank de achtergrond en het doel van de transactie en legt deze vast;
4. de transacties van zakenrelaties, gevestigd in deze landen of jurisdicties, meldt de bank door aan FIU Suriname;
5. het bijhouden van een lijst van landen die aangemerkt worden als low, high risk en onacceptabele landen en het bekend maken daarvan aan de bankmedewerkers met duidelijke instructies.
6. de bank voert in beginsel geen transacties uit naar onacceptabele landen, terwijl zij transacties naar high-risk landen kan uitvoeren na het voeren van een EDD.
7. voorzover nodig beperkt de bank zakelijke relaties of financiële transacties met deze landen en de personen in die landen.
8. het systematisch melden van financiële transacties van en naar deze landen.

13. NON-PROFIT ORGANISATIE/ NIET-COMMERCIËLE ORGANISATIE

13.1 Algemeen

Non-profit organisaties (NPO's) zijn organisaties die niet op winst zijn gericht. De CBvS AML/CFT Richtlijn van 13 oktober 2016 omschrijft een NPO als een rechtspersoon, juridische constructie of organisatie die zich voornamelijk bezighoudt met het werven of verstrekken van fondsen voor doeleinden zoals liefdadige, religieuze, culturele, educatieve, sociale of sociëteitsactiviteiten, of voor het uitvoeren van andere vormen van "goede daden". Men noemt ze ook wel 'not-for-profit organisaties' of 'organisaties zonder winstoogmerk'.

Hun bestaansgrond is de voortbrenging van goederen en diensten die voorzien in een bepaald ideëel of maatschappelijk belang. Non-profit organisaties hebben niet als primair doel het verschaffen van een ondernemersloon of het bereiken van een zo hoog mogelijk rendement op het door de eigenaren geïnvesteerde vermogen. In deze zin zijn non-profit organisaties niet financieel-economisch

zelfstandig, maar zijn ze in aanzienlijke mate afhankelijk van collectieve, dat wil zeggen niet-marktgeoriënteerde, financiering.

De financieel-economische onzelfstandigheid betekent echter niet dat financiële of economische overwegingen bij de besturing van non-profit organisaties geen rol spelen. Zo is de financiële armslag die non-profit organisaties krijgen een belangrijke randvoorwaarde waarbinnen de ideële doelstellingen moeten worden uitgevoerd. Een doelmatiger gebruik van de toegekende middelen kan direct leiden tot meer en betere dienstverlening. Bovendien is het doelbewust creëren van een positief netto financieel resultaat soms zelfs noodzakelijk om reserves te kweken, teneinde de continuïteit van de dienstverlening ook voor de toekomst veilig te stellen.

13.2 Kenmerken van NPO's

De kenmerken van NPO's zijn als volgt:

1. Ze zijn vanwege uiteenlopende oorzaken bijzonder kwetsbaar voor misbruik door terroristen.
2. Ze genieten publiek vertrouwen.
3. Ze hebben toegang tot talrijke geldbronnen.
4. Ze gaan vaak om met contanten.

13.3 Risico's van NPO's

De risico's die NPO's kunnen vertegenwoordigen, zijn als volgt:

a. het profiteren van de kenmerken van NPO's door terroristen en terroristische organisaties door te infiltreren in de sector en middelen en activiteiten van NPO's;
b. het misbruiken van NPO's door terroristen voor ondersteuning of ter dekking vanterroristische activiteiten.

13.4 Maatregelen

1. De bank accepteert geen NPO's die hun vermogen verhullen, gelden witwassen of betrokken zijn bij een AML/CFT delict of zich schuldig maken aan terrorisme financiering. De bank voert op alle NPO's verscherpt clientenonderzoek uit ter voorkoming van misbruik van het financieel systeem door kwaadaardigen als doorsluiskanaal van opbrengsten afkomstig van criminele handelingen of voor de financiering van terrorisme.
2. De bank documenteert en analyseert op basis van uitgevoerde EDD en beoordeling van de risicogevoeligheid van de activiteiten van NPO's het volgende:
   a. het doel en de activiteiten van de organisatie;
   b. de landen waar er reeds activiteiten zijn ontplooid, alsmede het land van herkomst;
   c. de organisatiestructuur;
   d. de donoren en vrijwilligers;
   e. de identiteit van de eigenaar van de organisatie, inclusief senior officers, bestuursleden en beheerders;
   f. de voorwaarden voor het schenken van fondsen;
   g. de voorwaarden voor het bewaren/opslaan van documenten;
   h. de lijst van samenwerkende NPO's;
   i. de interne audit en controle van de NPO.

3. De bank doet onmiddellijk melding aan de FIU Suriname indien zij vermoedt of redelijke gronden heeft te vermoeden dat financiële middelen afkomstig zijn van of gerelateerd zijn aan terroristische activiteiten, of gebruikt zullen worden voor terrorisme, het plegen van terroristische handelingen, of door terroristische organisaties.

14. ELEKTRONISCHE GELDOVERMAKINGEN

14.1 Algemeen

Money Transfer (overboeking) verwijst doorgaans naar een van de volgende betalingswijzen of betalingssystemen zonder contant geld:

1. Electronic funds transfer (elektronische overboeking): een overkoepelende term die meestal wordt gebruikt voor op bankkaarten gebaseerde betalingen.
2. Money order (postwissel): overschrijving per postcheque, money gram of andere.
3. Wire transfer (bankoverschrijving of elektronische overmaking): een internationale versnelde overschrijving van bank naar bank.

In de afgelopen decennia is gebleken dat wire transfer zeer gevoelig ligt voor moneylaundering en terrorismefinanciering. Derhalve maakt de bank beleid op de elektronische overmaking om zodoende maatregelen te treffen ter voorkoming van misbruik van banksystemen voor het doorsluizen van gelden middels elektronische overschrijvingen door terroristen en andere criminelen.

De bank onderzoekt bij een verzoek tot overmaking of de transactie past in het klantprofiel van de betreffende klant en neemt op basis daarvan een besluit het al dan niet uitvoeren van de transactie. Voor het geval er een subjectieve indicator wordt bespeurd, voert de bank verscherpt clientenonderzoek (EDD) uit en voert de transactie niet uit zolang zijn zich niet heeft overtuigd dat de transactie een legale en feilloze transactie betreft.

Alle overmakingen van de bank geschieden via een elektronisch interbancair betaalsysteem, namelijk de Suriname Nationaal Elektronisch Betaalsysteem (SNEPS) van de CBvS. De clearing en settlement van betalingen middels overmakingen geschieden via de SNEPS.

14.2 Algemene maatregelen

1. Het overzichtelijk bewaren van basisinformatie over de opdrachtgever en begunstigde van elektronische geldovermakingen zodat die op verzoek onmiddellijk beschikbaar kan worden gesteld aan toezichthoudende -, rechtshandhavings- en/of vervolgingsinstanties om misbruik van elektronische geldovermaking op te sporen.
2. Het vaststellen en melden van verdachte transacties aan FIU Suriname;
3. Zich onthouden van het verrichten van transacties middels elektronische geldovermaking voor of naar aangewezen personen en entiteiten overeenkomstig de Resoluties van de Veiligheidsraad van de Verenigde Naties, betreffende de voorkoming en bestrijding van terrorisme en terrorismefinanciering.

4. Het bijhouden van de vereiste en accurate gegevens over de gehele betalingsketen van zowel de opdrachtgevende, de bemiddelende als de begunstigde financiële instelling.
5. Het voor ogen houden van de indicatoren voor moneylaundering bij zowel binnenlandse als grensoverschrijdende elektronische geldovermakingen, zoals genoemd in het Besluit Indicatoren Ongebruikelijke Transacties.

14.3 Specifieke maatregelen

14.3.1 Binnenlandse elektronische geldovermaking

Bij binnenlandse elektronische overschrijvingen zorgt de bank ervoor dat naast de informatie die de overmaking begeleidt tevens informatie over de opdrachtgever zijn opgenomen, zoals is aangegeven voor grensoverschrijdende overschrijvingen.

14.3.2 Buitenlandse elektronische geldovermaking

1. Voor grensoverschrijdende elektronische overmakingen van niet meer dan USD/EUR 1.000, neemt de bank de volgende gegevens op:
   i. de naam van de opdrachtgever;
   ii. de naam van de begunstigde; en
   iii. een rekeningnummer voor elk, of een uniek referentienummer van de transactie.
2. Grensoverschrijdende elektronische overmakingen boven het bedrag van USD/EUR 1000, dienen altijd de volgende begeleidende informatie te bevatten:
   a. de naam van de betaler;
   b. het rekeningnummer van de opdrachtgever wanneer deze rekening voor de verwerking van de transactie wordt gebruikt;
   c. het adres van de opdrachtgever, of het nationale identiteitsnummer of klantenidentificatienummer, of datum en plaats van geboorte;
   d. de volledige naam van de begunstigde, identificatiebewijs; en tevens (e) het rekeningnummer van de begunstigde, wanneer deze rekening voor de verwerking van de transactie wordt gebruikt.

   Bij het ontbreken van een rekening, wordt een uniek referentienummer van de transactie opgenomen dat mogelijk maakt om de transactie te traceren.
3. Indien meerdere afzonderlijke grensoverschrijdende elektronische overschrijvingen van één opdrachtgever in een batchbestand zijn gebundeld voor verzending aan begunstigden, kan de bank in plaats van de vereisten met betrekking tot de opdrachtgeverinformatie het rekeningnummer van de opdrachtgever of het unieke referentienummer van de transactie gebruiken, terwijl het batch bestand de vereiste en nauwkeurige informatie bevat betreffende de opdrachtgever en volledige informatie over de begunstigde, die volledig traceerbaar is in het land van de begunstigde.

14.4 Finabank als opdracht gevende instelling

Onder opdracht gevende financiële instelling wordt verstaan de financiële instelling die elektronische overschrijving begint en die de gelden overmaakt na ontvangst van het verzoek om een elektronische overschrijving namens de opdrachtgever te verrichten.

De verantwoordelijkheden van de bank hierbij zijn als volgt:

1. ervoor zorgen dat in aanmerking komende overschrijvingen de vereiste en nauwkeurige informatie over de opdrachtgever en de begunstigde bevatten.
2. het waarborgen dat grensoverschrijdende elektronische overschrijvingen onder de minimus drempel de naam van de opdrachtgever en van de begunstigde bevatten en van beide het rekeningnummer, of een uniek referentienummer van de transactie.
3. het bewaren van alle informatie over betalers en begunstigden conform de bewaartermijn zoals opgenomen in deze policy.
4. het niet uitvoeren van de elektronische overschrijving als deze niet voldoet aan de hierboven aangegeven vereisten.
5. Het rapporteren (aan FIU Suriname) van de poging tot overmaking indien uit EDD blijkt dat de opdrachtgever geen adequate onderbouwing kan geven en mogelijk een ongebruikelijke transactie zou zijn.

14.5 Finabank als begunstigde financiële instelling

Een begunstigde financiële instelling is een financiële instelling die de elektronische overschrijving ontvangt van de opdracht gevende financiële instelling, eventueel via een bemiddelende financiële instelling, en de gelden beschikbaar stelt aan de begunstigde.

De verantwoordelijkheden van de bank hierbij zijn als volgt:

1. De bank voert geen opdrachten tot grensoverschrijdende elektronische overschrijvingen uit waaraan vereiste informatie over de opdrachtgever of begunstigde ontbreekt en meldt deze aan de FIU Suriname als een ongebruikelijke transactie.
2. Bij in aanmerking komende elektronische overschrijvingen stelt de bank de identiteit van de begunstigde vast indien de identiteit niet eerder is geverifieerd. Zij bewaart deze informatie voor de periode als opgenomen in deze policy als bewaartermijn.

15. ULTIMATE BENEFICIAL OWNER/ UITEINDELIJKE BEGUNSTIGDE

15.1 Algemeen

Een belangrijke maatregel in het kader van de uitvoering van KYC/CDD is de vaststelling van de identificatie van de uiteindelijk begunstigde, hierna: "UBO", en het nemen van redelijke maatregelen om de identiteit van de UBO te verifiëren, zodanig dat de bank ervan overtuigd is dat zij weet wie de UBO is. Voor rechtspersonen en juridische constructies omvat dit onder meer voor de bank redelijke maatregelen om de eigendoms- en zeggenschapsstructuur van de klant te begrijpen.

De bank accepteert in beginsel alleen klanten die maximaal 3 (drie) lagen c.q. layers in haar UBO-structuur hebben die transparant zijn en tijdens het uitvoeren van KYC/CDD zonder enige mate van complexiteit of ingewikkeldheid kan worden onderzocht.

15.2 Typen van UBO's

De UBO wordt onderverdeeld in twee typen:

1. Economische UBO: de persoon die op basis van een contract of afspraak met de juridische UBO op de voorgrond optreedt en/of voor en namens de juridische UBO de aandelen aanhoudt, stemrechten en/of zeggenschapsrechten uitoefent. De economische UBO wordt ook wel pseudo UBO genoemd;
2. Juridische UBO: de persoon die juridisch de werkelijke uiteindelijke begunstigde, aandeelhouder of eigenaar is en de winsten, waaronder dividend, uitgekeerd krijgt.

Voor de bank is het relevant om deze typen UBO's op adequate wijze te herkennen bij de uitvoering van de due diligence. Daarvoor is voor de bankmedwerkers ook nodig om de verhoudingen tussen beide in de rechtspersonen en andere juridische constructies goed te begrijpen.

15.3 De naamloze vennootschap en haar UBO's

15.3.1 Algemeen

Aan aandelen in een naamloze vennootschap zijn twee soorten rechten verbonden:

a. Zeggenschapsrechten: geven recht op het uitbrengen van stemrecht in de algemene vergadering van aandeelhouders van de vennootschap;
b. Economische rechten: geven recht op onder meer dividend.

De zeggenschapsrechten kunnen worden losgekoppeld door het certificeren van aandelen. Bij certificering van aandelen worden aandelen in vehikels – meestal in een stichting – geplaatst, die daarmee de zeggenschap over de aandelen uitoefenen. Deze stichting geeft vervolgens certificaten van aandelen uit aan de oorspronkelijke aandeelhouder. Het bestuur van de vehikel oefent dan vervolgens de stemrechten in de vennootschap.

15.3.2 De rol van het vehikel en uitgifte van certificaten

Het vehikel kan in economisch opzicht worden gezien als een doorgeefluik. Als door de vennootschap (een deel van) de winst wordt uitgekeerd, dan is de stichting verplicht deze winst door te storten aan de certificaathouder(s). De bank onderzoekt bij de uitvoering van de due diligence op naamloze vennootschappen of er vehikels in het geding is en of er certificaten zijn uitgegeven.

Bij de oprichting van de stichting kunnen aanvullende bepalingen worden opgenomen in de statuten ten aanzien van de bestuursbevoegdheid, de opvolging van de bestuursleden en de wijze waarop de bestuursleden van deze stichting worden benoemd. Bij het uitvoeren van due diligence onderzoekt de bank in de statuten of die bepalingen bevatten die mogelijkheden scheppen tot gebruik van vehikels.

15.3.3 Bedrijfsopvolging

In het kader van een bedrijfsopvolging kunnen aandelen worden gecertificeerd door een DGA/ondernemer, als gevolg waarvan hij ten tijde van de certificering alle aandelen in de (holding) N.V. overdraagt aan een vehikel (stichting) en hiertegen certificaten van aandelen
terugkrijgt. Vervolgens kan hij als bestuurder van de stichting de zeggenschap op de aandelen uitoefenen.

Tot op het moment van overlijden van de ondernemer verandert er dus nog niets ten opzichte van de situatie voorafgaand aan de certificering. Echter, op het moment van overlijden van de ondernemer zullen de aandelen niet vererven aangezien deze zich op dat moment in de stichting bevinden. De zeggenschap van de aandelen zal in de stichting blijven, ten aanzien waarvan de oprichter in de statuten zijn opvolgende bestuurder(s) kan benoemen.

15.3.4 Blokkeringsregeling

In de statuten van een naamloze vennootschap wordt meestal een blokkeringsregeling opgenomen. Deze houdt vaak in dat, indien een aandeelhouder door hem gehouden aandelen in de N.V. wil overdragen, deze aandeelhouder deze aandelen dient aan te bieden aan de medeaandeelhouders. Deze medeaandeelhouders hebben dan een eerste recht om de aandelen te verkrijgen. Pas als de medeaandeelhouders afstand doen van dit aanbod om de aandelen te verkrijgen, kunnen de aandelen worden overgedragen aan een derde.

In de statuten of huishoudelijk reglement van de stichting kan worden bepaald dat de blokkeringsregeling, die in de statuten van de naamloze vennootschap is opgenomen ten aanzien van de aandelen, ook van toepassing wordt verklaard op de overdracht van de voor de stichting uitgegeven certificaten van aandelen. In dat geval moeten ook certificaten van aandelen in de vennootschap eerst worden aangeboden aan de mede-certificaathouders. Bij die overdracht voert de bank due diligence op de mede-certificaathouders om hun integriteit te toetsen. Indien die toets bezwaren in de zin van onaanvaardbare integriteitsrisico's ontmoet, en de overdracht van de certificaten van aandelen desondanks plaatsvindt, gaat de bank over tot de-risking van de klant.

15.3.5 Schenking van certificaten

Een DGA kan om belastingtechnische redenen bij leven certificaten van aandelen schenken aan zijn kinderen. Het voordeel van de schenking van certificaten in plaats van de schenking van aandelen is hierbij dat de DGA door de schenking geen zeggenschap in de vennootschap verliest (zelfs bij een schenking van de meerderheid van de uitstaande certificaten), wat wel het geval is bij schenking van aandelen. In het van schenking blijft de bank due diligence uitvoeren op de DGA.

15.3.6 Toepassing bij werknemersparticipatie

Een andere toepassing voor certificering van aandelen betreft een werknemersparticipatie. Een ondernemer kan besluiten om zijn medewerkers te laten participeren in de onderneming echter zonder zeggenschap. In dat geval draagt hij geen aandelen aan de

betreffende medewerker(s), maar certificaten van aandelen. Als gevolg hiervan worden – ook bij deze toepassing – alleen de aan de aandelen verbonden financiële rechten overgedragen, maar wordt de zeggenschap door de ondernemer behouden.

Bij een werknemersparticipatie geldt echter nog een ander aspect, namelijk dat de ondernemer de werknemer(s) waarschijnlijk enkel een participatie in de onderneming biedt in het geval dat deze personen zijn verbonden aan de onderneming. Om dit te realiseren, kan bij de overdracht van de certificaten aan de medewerker(s) worden bedongen dat deze medewerker(s) verplicht zijn de betreffende certificaten van aandelen terug te leveren ingeval de medewerker besluit het bedrijf te verlaten.

Werknemersparticipatie kan dienen als mogelijke constructie voor witwassen. Derhalve merkt de bank deze aan als verhoogd risico en beheert de relatie onder toepassing van de risicogebaseerde benadering.

15.3.7 Stemrechtloze aandelen

In het Nederlandse vennootschapsrecht is de mogelijkheid gecreëerd om stemrechtloze aandelen uit te geven in een B.V. Hoewel deze stemrechtloze aandelen in hoofdlijnen hetzelfde bewerkstelligen als certificaten van aandelen, namelijk splitsing van zeggenschap en financiële rechten, is het belangrijkste verschil dat bij stemrechtloze aandelen de houder hiervan per definitie vergaderrecht heeft in de algemene vergadering van aandeelhouders van de vennootschap.

Bij certificering van aandelen is het mogelijk om statutair te bepalen of aan de certificaathouders dit vergaderrecht toekomt. Hiernaast is het bij certificering van aandelen mogelijk om te bepalen dat de overdracht van deze certificaten onderhands kan plaatsvinden. Deze mogelijkheid bestaat niet bij stemrechtloze aandelen, zodat bij iedere overdracht een notariële akte is vereist.

Aangezien op dit soort punten het systeem van certificering van aandelen meer flexibel is dan stemrechtloze aandelen, wordt – ondanks de introductie van stemrechtloze aandelen – in de praktijk nog vaak gekozen voor certificering. De mogelijkheid tot onderhandse overdracht van de certificaten van aandelen is zeer gevoelig voor ML/FT door accommodatie van 'duistere figuren'. De bank sluit in de overeenkomst met de klant de onderhandse overdracht van de certificaten van aandelen uit. Indien de klant desondanks zich hieraan schuldig maakt, gaat de bank over tot de-risking van de klant.

15.4 Vereniging en Stichting

De vereniging wordt onderscheiden in:

1. Vereniging met rechtspersoonlijkheid: deze mogen rechtshandelingen verrichten en zijn volledig rechtsbevoegd. Deze vereniging wordt gezien als een rechtspersoon (zelfstandig drager van rechten en verplichtingen in het rechtsverkeer), waarbij de vereniging zelf aansprakelijk is voor alle handelingen die in naam van de vereniging worden verricht en niet de bestuursleden in privé.

2. Vereniging zonder rechtspersoonlijkheid: deze mogen geen rechtshandelingen verrichten. De bestuurders zijn hoofdelijk aansprakelijk en zijn derhalve de UBO's.

Voor de uitvoering van deze policy wordt onder de UBO van een vereniging of een stichting verstaan een natuurlijke persoon die:

1. direct of indirect meer dan 25% van het eigendomsbelang houdt in de vereniging of de stichting;
2. direct of indirect meer dan 25% van de stemmen kan uitoefenen bij besluitvorming ter zake van wijziging van de statuten van de vereniging of de stichting;
3. feitelijk zeggenschap kan uitoefenen over de vereniging of de stichting.

Wanneer er onder toepassing van de bovenstaande punten de UBO niet kan worden vastgesteld of er twijfel bestaat wie de UBO van de vereniging of stichting is, worden de bestuursleden als UBO aangemerkt. Dit wordt ook wel de pseudo-UBO genoemd. Bij een eenmansstichting of een vereniging met één bestuurder, is de enige bestuurder automatisch de UBO.

15.5 Overige juridische constructies

De bank registreert als Ultimate Beneficial Owner bij de volgende juridische constructies als volgt:

Juridische constructie	UBO
Vennootschap onder firma	Vennoten
Commanditaire vennootschap	Vennoten en commanditaire vennoten
Maatschap	Maten
Naamloze vennootschap i.o.	Oprichters
Eenmanszaak	Eigenaar

16. US PERSON

16.1 Wat is FATCA?

De Foreign Account Tax Compliance Act (FATCA) is de Amerikaanse wetgeving, die als doel heeft belastingontduiking door Amerikanen, waar ook ter wereld, te voorkomen. De wetgeving vereist van alle financiële instellingen dat zij al hun Amerikaanse klanten identificeren. Daarnaast dienen zij gegevens over de identiteit en het vermogen van deze Amerikaanse klanten door te geven aan de Amerikaanse belastingdienst, de Internal Revenu Service (IRS). Suriname heeft geen IGA (Intergovernmental Agreement) gesloten, waardoor de verantwoordelijkheid voor het uitwisselen van informatie met de IRS volledig komt te liggen bij de lokale financiële instellingen zelf.

Indien de bank zich dus niet aan de wetgeving houdt, kan de bank te maken krijgen met boetes die opgelegd worden door de Amerikaanse autoriteiten. Daarnaast kan de bank te maken krijgen met belasting die wordt ingehouden op alle betalingen die direct of indirect afkomstig zijn uit Amerika en die gedaan worden aan een financiële instelling die niet meedoet aan FATCA. Het niet tijdig voldoen aan de wetgeving kan dus kostbaar zijn en kan Finabank buiten de keten van betrouwbare financiële instellingen plaatsen.

16.2 Wie is een US Person?

De IRS omschrijft een Amerikaans belastingplichtige als een U.S. Person. Van een U.S. Person is sprake wanneer een of meerdere van de onderstaande kwalificaties (US-indicia) op de klant van toepassing is/zijn. De klant kan zijn een natuurlijke persoon of een rechtspersoon (bedrijf of organisatie). Een US Person is te herkennen aan de volgende criteria, echter niet limitatief opgesomd:

- heeft een Amerikaans paspoort;
- woont in de V.S.;
- is geboren in de V.S.;
- heeft een Amerikaans woon- , postadres of telefoonnummer;
- maakt periodiek geld over naar de V.S.;
- heeft een gevolmachtigde met een Amerikaans adres;
- heeft een per adres (p/a) in de V.S;
- een bedrijf gevestigd in de V.S.;
- heeft een rekening in de V.S.

17. ANONIEME KLANTEN OF TRANSACTIES

De bank opent geen rekeningen voor klanten op onmiskenbaar gefingeerde namen noch voert zij anonieme rekeningen in haar boeken. Evenzo staat de bank niet toe dat er op rekeningen anonieme transacties worden uitgevoerd.

18. DE-RISKING (OPZEGGING EN BEËINDIGING VAN DE KLANTRELATIE)

1. 1. De bank is gerechtigd om een bestaande klantrelatie te beëindigen wanneer de integriteitsrisico die de klant vertegenwoordigt of met zich meebrengt buiten de risk appetite van de bank komt en derhalve een voor de bank als onacceptabel risico wordt aangemerkt.
2. Het besluit tot de-risking wordt op basis van een risk assessement op voordracht van de OII genomen door de RCC. De redenen tot de-risking moeten genoegzaam zijn onderbouwd. Het besluit bevat ook de redelijke opzegtermijn waarbinnen de afwikkeling van de klantrelatie moeten hebben plaatsgevonden. Afhankelijk van de ernst en de mate van de risico's kan de RCC besluiten tot onmiddellijke beëindiging van de klantrelatie. In dit geval worden de rekeningen van de klanten onmiddellijk geblokkeerd en de klant wordt de toegang tot andere bankproducten ontzegd en/of geweigerd.
3. De klant wordt na het besluit van de RCC tot de-risking met inachtneming van de Internal Watchlist Policy op de Internal Watchlist geplaatst door de FoD, terwijl de OII dit proces begeleidt en controleert.

4. Het proces van de de-risking na het besluit van de RCC wordt begeleid door de Legal Affairs Department in samenwerking met de FoD die als relatiebeheerder verantwoordelijk blijft voor het geheel.
5. De OII doet een melding van de de-risking aan de FIU Suriname.

19. SANCTIE TREFFERS

Ten aanzien van treffers op het gebied van sanctieregulering (Wet Internationale sancties 2014) is de bank verplicht zijn administratie zodanig te controleren dat rechtspersonen en entiteiten die in de sanctieregeling worden genoemd, kunnen worden opgespoord. Het moet mogelijk zijn de financiële tegoeden onmiddellijk te bevriezen en/of te voorkomen dat financiële tegoeden en/of diensten aan deze (natuurlijke) personen en entiteiten ter beschikking worden gesteld. Indien de bank constateert dat de identiteit van een relatie overeenkomt met die van een natuurlijke of rechtspersoon of entiteit als bedoeld in de sanctielijst, dan zal de bank dit onmiddellijk melden aan de CBvS. Bij een treffer van een sanctie kan de bank per case beslissen om de treffer te delen met de toezichthouder. Bij een vermoeden van financiering van terrorisme meldt de instelling deze transacties aan de CBvS en de FIU.

20. BEWAARTERMIJN EN REGISTER

De Bank neemt in het kader van haar wettelijke bewaarplicht een bewaartermijn van 10 (tien) jaren in acht voor het op toegankelijke wijze bewaren van alle noodzakelijke gegevens betrekking hebbende op transacties, clientenonderzoek, zoals aangegeven in WID, MOT en WTK. Indien en voorzover de bank door een daartoe bevoegde autoriteit wordt verzocht, bewaart zij alle gegevens ook na de genoemde tien jaren op een toegankelijke wijze en zal op verzoek deze beschikbaar stellen voorzover niet beperkt door de wet.

De bank houdt in elektronische vorm een register bij van de door clientenonderzoek verkregen gegevens en van gegevens met betrekking tot transacties. Dit register is met name haar core banking system, T24 genaamd, alsmede de databestanden c.q. folders welke mede ter voldoeningvan dat doeleinde dienen of als aanvulling van die gegevens in T24 dienen.

21. UITZONDERINGSBELEID

In deze policy is het KYC/CDD beleid van de bank gecodificeerd. Het maken van uitzonderingen op dit beleid behoort tot het prerogatief van de RCC. De uitzonderingsverzoeken worden door de OII voorgelegd aan de RCC. De behandeling van en besluitvorming over die verzoeken vinden plaats op de wij als voorgeschreven in de RCC Charter.
Uitzonderingen op dit beleid worden niet gemaakt mits in voldoende mate de noodzaak totafwijking van het beleid is aangetoond. De uitzondering moet zuiver een integriteitsoverweging zijn, geen commerciële overweging. Een uitzondering mag geenszins een overtreding van een nationale of internationale wet- en regelgeving of normen inhouden.

22. ESG COMPLIANCE

In 2021 heeft Finabank ook haar ESG-policy geïmplementeerd. Het nieuw risico die hierbij besproken wordt is ESG-risk. Daarom is het van belang ESG onderdeel te maken van het Customer Due Diligence (CDD) proces. De bank zal het volgende in achtnemen:

1. Het respecteren en beschermen van het milieu, mensenrechten en arbeidsrechten.
2. Vermijdt negatieve beïnvloeding en meer impact voor de ecologische en sociale gebieden.
3. Het aanbieden van producten en diensten ten einde bij te dragen aan de duurzame ontwikkeling van mensen, het milieu en ons economie.
4. Bemoedigen en ondersteunen van de stakeholders en overwegend de bijdrage aanduurzaamheid.
5. Uitwisselen van kennis voor stakeholders onderling.

In dit kader zal Finabank bij het uitvoeren van KYC op haar toekomstige klanten aandacht besteden aan bovengenoemde zaken. Van belang is gedurende de clientenonderzoek ook de focus te leggen KYC en aanverwante bepalingen waaronder Know Your Business (KYB) en Know Your Transaction (KYT). Know Your Business staat erom bekend dat klanten en zakenpartners van financiële diensten en producten te begrijpen in termen van hun identiteit, blootstelling aan politieke prominente personen (PEP), zakelijke activiteiten, bron van inkomen en de herkomst van fondsen. Middels deze benadering kan het risico op milieucriminaliteit geïdentificeerd worden.

Voorbeeld van activiteiten die onder milieucriminaliteit vallen zijn als volgt:

- Illegale extractie
- Handel in bosbouw en mineralen
- Illegale landontginning en afvalhandel
- Milieucriminaliteit met aanverwante misdaden zoals corruptie, menselijke veiligheid, drugshandel en mensenrechtenschendingen.

23. GEGEVENSBESCHERMING

Alle gegevens die verzameld zijn in het kader van het clientenonderzoek dienen gebruikt te worden met het oog op het voorkomen van witwassen en financiering van terrorisme. De klantgegevens mogen niet gebruikt worden voor commerciële- of andere doeleinden die niet in lijn staan met het voorkomen van witwassen en financieren van terrorisme.

24. RAPPORTAGE

De Manager OII is verantwoordelijk voor het plegen van interne en externe rapportages uit hoofde van deze policy. Interne rapportages worden minimaal maandelijks gepleegd aan de RCC en de RC, terwijl externe rapportages conform vereiste gepleegd worden naar de FIU Suriname en de CBvS toe.

25. HANDHAVING

Het is de verantwoordelijkheid van alle medewerkers van Finabank om dit beleid na te leven. Transparantie en integriteit zijn belangrijk voor Finabank en daarom worden in het bijzonder employees aangemoedigd misstanden te rapporteren via rapportagekanalen zoals uiteengezet in de whistleblower policy. Het niet naleven of opzettelijk schenden van het beleid kan leiden tot disciplinaire maatregelen. Alle vragen met betrekking tot de inhoud en interpretatie van dit beleid kunnen worden gericht aan de Office of Institutional Integrity.

26. AUTORITEIT

Dit beleid is goedgekeurd door de risk & Compliance Comité en en de Risk Commissie van de raad van commissarissen. Het beleid zal ten minste om de twee jaar gereviseerd worden door de Office of Institutional Integrity.

27. MONITORING EN REVIEW

Deze KYC-CDD policy wordt jaarlijks door OII geëvalueerd en getoetst op haar effectiviteit en zo nodig herzien.

Finabank hoofdkantoor Dr. Sophie Redmondstraat 59-61 T.(+597) 472266

Finabank filialen
Finabank Zuid Mr. J. Lachmonstraat 49 T.: (+597) 430300
Finabank Noord Hoek Jozef Israëlstraat/Kristalstraat T.: (+597) 455169
Finabank Nickerie A.K. Doerga Sawhstraat 72 T.: (+597) 230027
Finabank Wanica Indira Ghandiweg 144 T.: (+597) 581885
Website: www.finabanknv.com
E-mail: customercare@finabanknv.com

Finabank Online
Finabank Facebook Messenger
Finabank Mobile Banking
Finabank Online Banking
Website: www.finabanknv.com
E-mail: customercare@finabanknv.com

FinaBank