

RISK MANAGEMENT AND COMPLIANCE PROGRAMME

PER SECTION 42 OF THE
FINANCIAL INTELLIGENCE CENTRE AMENDMENT ACT 1 of 2017

**Erasmus-Els Inc. t/a
Erasmus-Scheepers Attorneys**

172 Bronkhorst Street
Nieuw Muckleneuk
Pretoria/Tshwane

("the Firm")

Current Version

Version	2.0
Date	6 th December 2021
Next Review Date	6 th December 2022
Document Owner	Hannes De Waal (AML/CTF Compliance Officer)

Version Control

Version	Date	Revisions
2.0	22 Sept 22	Removal of Chris Morkel as AML/CTF Compliance Officer and replacement with Hannes De Waal.
1.0	6 Dec 21	Initial document signed off.

Declaration of implementation & compliance

As authorised by the firm, I confirm that:

- this document and version are recognised as the successor to all previous internal rules, documents, programmes, controls, and processes and is approved by the senior leadership of the firm
- this document and our risk-based approach will be reviewed annually and that it will be updated as is appropriate when business risk tolerance, processes, or legislation change
- this document and version will remain in force until such time as it is updated or rescinded.

Full name : HANNES DE WAAL

Signed : _____ Date:

1.	DEFINITIONS	6
2.	INTRODUCTION	10
2.1	KEY REQUIREMENTS OF FINANCIAL INTELLIGENCE CENTRE ACT ("FICA")	10
2.2	CONSEQUENCES OF NON-COMPLIANCE WITH FICA	11
3.	GOVERNANCE	11
3.1	APPOINTMENT OF AN AML/CTF COMPLIANCE OFFICER	11
3.2	REGISTRATION WITH THE FINANCIAL INTELLIGENCE CENTRE	12
3.3	RISK MANAGEMENT AND COMPLIANCE PROGRAMME ("RMCP")	12
3.4	MAINTENANCE OF THE RMCP	13
3.5	TRAINING	14
4.	RISK-BASED APPROACH	14
4.1	RISK CATEGORISATION	14
4.2	RISK FACTORS	15
4.2.1	<i>Product and Services</i>	15
4.2.2	<i>Higher-Risk Jurisdictions</i>	17
4.2.3	<i>Entity type</i>	18
4.2.4	<i>Source of funds</i>	18
4.2.5	<i>Nature and purpose of transaction or business relationship</i>	19
4.2.6	<i>Industry</i>	19
4.2.7	<i>Adverse Media</i>	21
4.2.8	<i>Foreign Prominent Public Officials and Domestic Prominent Influential Persons</i>	22
4.3	MANUAL DOWNGRADE OF RISK CATEGORISATION	22
4.4	MANUAL UPGRADE OF RISK CATEGORISATION	23
4.5	FALSE OR FICTITIOUS NAMES AND ANONYMOUS CLIENTS	23
4.6	DOUBTS SURROUNDING VERACITY OF INFORMATION OR EVIDENCE	24
4.7	TERMINATING CLIENTS BASED ON RISK ASSESSMENT	24
4.8	TERMINATING CLIENTS WHEN UNABLE TO CONDUCT DUE DILIGENCE SATISFACTORILY	24
4.9	SENIOR MANAGEMENT APPROVAL PROCESS	25
5.	DUE DILIGENCE	25
5.1	IDENTIFICATION	26
5.2	VERIFICATION	26
5.3	SINGLE TRANSACTIONS AND MINIMUM STANDARDS	26
5.4	ADDITIONAL DUE DILIGENCE FOR LEGAL PERSONS	27
5.4.1	<i>Related Parties</i>	27
5.4.2	<i>Ultimate Beneficial Owners ("UBO")</i>	28
5.5	REPRESENTATIVES ACTING ON BEHALF OF A CLIENT OR CLIENT ACTING ON BEHALF OF ANOTHER PERSON	28
5.6	SANCTIONS SCREENING	29
5.7	IDENTIFICATION OF FOREIGN PROMINENT PUBLIC OFFICIALS ("FPPO")	29
5.8	IDENTIFICATION OF DOMESTIC PROMINENT INFLUENTIAL PERSONS ("DPIP")	30
5.9	SOURCE OF FUNDS/WEALTH	32
6.	ONGOING DUE DILIGENCE	32
6.1	TRIGGER BASED REVIEWS – CLIENT INFORMATION CHANGES	33
6.2	TRIGGER BASED REVIEWS – SANCTION AND RESTRICTIVE LIST SCREENING ALERTS	33
6.3	TRIGGER BASED REVIEWS – SUSPICIOUS ACTIVITY/TRANSACTION	34
6.4	TIME-BASED PERIODIC REVIEWS	34
6.5	DOUBTS SURROUNDING THE VERACITY OF INFORMATION PREVIOUSLY OBTAINED	34
7.	ACTIVITY MONITORING	35
8.	REPORTS TO THE FINANCIAL INTELLIGENCE CENTRE (FIC)	35
8.1	CASH THRESHOLD REPORTS ("CTR"/"CTRA")	35

8.2	SUSPICIOUS ACTIVITIES OR TRANSACTIONS (“SAR”/“STR”)	36
8.3	TERRORIST RELATED PROPERTY, TRANSACTIONS OR ACTIVITIES	37
8.4	REMEDICATION OF NON-SUBMITTED REPORTS	37
8.5	AVOIDING TIPPING OFF	38
8.6	CONFIDENTIALITY OF PERSONAL AND REPORTED INFORMATION	39
8.7	PROTECTION OF REPORTING PERSONS	39
8.8	CONTINUATION OF TRANSACTIONS	39
8.9	RESPONDING TO REQUESTS FROM THE CENTRE	40
8.10	MONITORING ORDERS	40
9.	RECORDKEEPING	40
9.1	FIC REGISTRATION AND CHANGES	40
9.2	DUE DILIGENCE	40
9.3	TRANSACTIONS	41
9.4	THIRD-PARTY RECORD KEEPING	41
9.5	REPORTS TO THE FIC	42
9.6	CENTRE ACCESS TO RECORDS	42
10.	ANNEXURES:	43
10.1	SENIOR MANAGEMENT SIGN-OFF	44
10.2	DOCFOX SCREENING LISTS	45
10.3	DUE DILIGENCE STANDARDS	57
10.3.1	<i>Natural Persons – Adult</i>	58
10.3.2	<i>Natural Persons – Minor</i>	58
10.3.3	<i>Natural Persons – Sole Proprietor</i>	59
10.3.4	<i>Close Corporation</i>	60
10.3.5	<i>Listed Firm</i>	61
10.3.6	<i>Unlisted Firm</i>	62
10.3.7	<i>Non-Profit Firm & Other Entities</i>	63
10.3.8	<i>Partnership</i>	64
10.5.9	<i>Trusts</i>	65
10.5.10	<i>Late Estates</i>	66
○ 10.4	EXAMPLES OF ACCEPTABLE PROOF OF ADDRESS	67
○ 10.5	EXAMPLE EVIDENCE OF SOURCE OF FUNDS/WEALTH	68
○ 10.6	CLIENT PROFILE FORMS – NATURAL & LEGAL PERSONS	69

1. Definitions

In this document, the following bear the definitions ascribed to them and may not necessarily have the same meaning as that of a legal definition.

“Accountable Institution” means any of the entity types or businesses listed under Schedule 1 of the Financial Intelligence Centre Act, 2001 as amended.

“AML/CTF Compliance Officer” means the appointed Anti Money Laundering/Counter Terrorist Financing Compliance Officer who oversees the compliance function of the Accountable Institution and who is duly registered with the Financial Intelligence Centre as the Compliance Officer/Money Laundering Reporting Officer for the Firm.

“Beneficial Owner” or **“Ultimate Beneficial Owner”** or **“UBO”** means the natural person who, independently or together with another person, directly or indirectly owns a legal person or exercises effective control over it.

“Business Relationship” means an understanding between the client and firm to enter into a series of activities over time.

“Cash” means coin and paper money that is designated as legal tender in South Africa.

“Cash Threshold Report” or **“CTR”** means the report that must be submitted to the FIC where the firm pays or receives an amount of cash (or aggregated smaller amounts of cash) that exceed the total of R24 999.

“Client Due Diligence” or **“CDD”** means the process of client identification and verification.

“Client” means either a natural person or legal person who has engaged the activities, products or services of the firm. For clarity, ‘Clients’ include those entities or persons who instruct the firm under mandate to act for and on their behalf.

“Client Onboarding Process” means the steps used by the firm to onboard a new client in the firm.

“Cloud” means a network of remote servers operating as a single ecosystem designed to store and manage data, run applications, or deliver content or a service.

“Firm” means the Accountable Institution to which this RMCP refers.

“Counterparty” means any party (other than the client) in an agreement, activity or transaction to which the client is a party.

“DocFox” means the DocFox software as a solution application provided by DocFox Africa (Pty) Ltd that stores due diligence documents, screens and compares client information against aggregated data sources and facilitates risk rating.

“DPIP” or **“Domestic Prominent Influential Person”** means a person or their immediate family member or known close associate designated as a Domestic Prominent Influential Person, by the Financial Intelligence Centre Act, 2001 as amended.

“Effective Control” means the ability to make decisions or influence the activities of a legal person.

“Employee” means any employee of a legal person, including shareholders, directors, members, managers, employee, contract workers or representatives.

“Existing Client” is any natural or legal person with an existing business relationship with the firm before the FIC Amendment Act implementation date of 1st April 2019.

“FATF” means the Financial Action Task Force.

“FIC” or **“The Centre”** means the Financial Intelligence Centre.

“FICA” or **“FIC Act”** or **“The Act”** means the Financial Intelligence Centre Act, No. 38 of 2001, as amended.

“Firm” means the Accountable Institution to which this RMCP refers.

“FPPO” or **“Foreign Prominent Public Official”** means a person or their immediate family member or known close associate designated as a Foreign Prominent Public Official, by the Financial Intelligence Centre Act, 2001 as amended.

“Governmental Authority” means any global public authority or organ of state.

“ID” or **“Identify Document”** means any document issued by a governmental authority that identifies a natural person and displays the full name, unique identifying number, date of birth, and facial image.

“Implementation Date” means the date on which Accountable Institutions must be fully compliant with FICA Amendment Act (1 April 2019).

“Immediate family member” means, for the purposes of 21H, an immediate family member includes

- (a) the spouse, civil partner or life partner;
- (b) the previous spouse, civil partner or life partner, if applicable;
- (c) children and stepchildren and their spouse, civil partner or life partner;
- (d) parents; and
- (e) sibling and step sibling and their spouse, civil partner or life partner.

“Legal Person” means any person, other than a natural person such as a limited firm, close corporation, foreign firm, corporation or association.

“ML/TF” or **“Money Laundering/Terrorist Financing”** means money laundering and the financing of terrorism which refers to any activity which has the effect of disguising the true nature and source of funds and/or where the ultimate destination of funds is involved in the financing of terrorism or terrorist related activities.

“Non-compliance” means failure to comply with any of FICA’s regulations or directives, and the firm’s AML & CTF RMCP.

“POCDATARA” means the Protection of Constitutional Democracy Against Terrorism and Related Activities Act, No. 33 of 2004, as amended.

“POPIA” and **“POPI”** means the Protection of Personal Information Act, No. 4 of 2013, as amended.

“Prospective Client” means a party who expresses the intention to engage the services, products or activities of the firm but has not yet confirmed their intention.

“Representative” means the party who is authorised to act on behalf of the Client.

“RMCP” or **“Programme”** means the Risk Management and Compliance Programme.

“Sanctions” means a list of natural or legal persons, vessels or jurisdictions subject to resolution 1267 of the United Nations Security Council and the Targeted Financial Sanctions (TFS) list published by the Financial Intelligence Centre.

“Section” or **“s.”** means the identified section of the Financial Intelligence Centre Act, No. 38 of 2001, as amended.

“Single Transaction” means a single, discrete activity or transaction has no expectation for additional for future further engagement, activity or transactions.

“Source of Funds” means the true origin of the funds that will be used by the client in a transaction or activity.

“Source of Wealth” means the origin of the client’s body of wealth or the activities that have generated the total net worth of the client.

“Suspicious or Unusual Activity Report” or **“SAR”** means the report that must be submitted to the FIC where there is reasonable knowledge or suspicion of an activity that may relate to the proceeds of unlawful activities.

“Suspicious or Unusual Transaction Report” or **“STR”** means the report that must be submitted to the FIC where there is reasonable knowledge or suspicion of a transaction that may relate to the proceeds of unlawful activities.

“Terrorist Activities” means any of the offences specified in POCDATARA which relate to terrorism.

“Terrorist Financing” refers to any practise where the primary goal is the financing of terrorism and related activities.

“Terrorist Financing Activity Report” or **“TFAR”** means the report that must be submitted to the FIC where there is reasonable knowledge or suspicion that an activity may relate to the financing of terrorism and related activities.

“Terrorist Financing Transaction Report” or **“TFTR”** means the report that must be submitted to the FIC where there is reasonable knowledge or suspicion that a transaction may relate to the financing of terrorism and related activities.

“Terrorist Property Report” or **“TPR”** means the report that must be submitted to the FIC where the firm has either in its possession or under its control, any property associated with terrorist and related activities.

“Terrorist Property” means the property described in Section 1 of the Prevention of Organised Crime Act 121 of 1998 as amended.

“Transaction” means an activity where value is transferred between the client, its principal, and a counterparty.

2. Introduction

The firm recognises that by virtue of its nature of business it is identified as an Accountable Institution under Schedule 1 of the Financial Intelligence Centre Act (“FICA”) and as such, seen as more readily targeted by criminals for money laundering or terrorist financing purposes.

The firm has therefore committed itself to comply with FICA’s regulatory requirements to make it more difficult for criminals to implicate the firm in these activities and to comply with its requirements as an Accountable Institution through the implementation of guiding principles and mitigative control processes surrounding client interactions and activities both during onboarding and throughout the client relationship.

2.1 Key requirements of Financial Intelligence Centre Act (“FICA”)

In addition to acting in good faith regarding the spirit of the legislation, the firm endeavours to comply with the following key obligations of FICA:

- **Section 20A:** Avoid any business relationship or activity/transaction where clients have an apparent false or fictitious name
- **Section 21A:** Establish and verify the identity of all Clients, their authorised persons, nature and purpose of business relationship and intended source of funds before they enter a business relationship or conclude a single activity/transaction
- **Section 21B:** Undertake additional due diligence where a client is a Legal Person, Trust or Partnership
- **Section 21C:** Undertake ongoing monitoring and due diligence of existing business relationships
- **Section 21D:** Confirm the veracity of client information where there is doubt
- **Section 21E:** Avoid any business relationship or activity/transaction where it is unable to conduct CDD
- **Section 21F:** Undertake enhanced due diligence where a client is a Foreign Prominent Public Official
- **Section 21G:** Undertake enhanced due diligence where a client is a Domestic Prominent Influential Person
- **Section 21H:** Undertake enhanced due diligence where a client is a family member or a close associate of a DPIP or an FPPO
- **Section 22A, 23 & 24:** Safely keep records of due diligence and transactions for at least five (5) years after the termination of a relationship, the conclusion of the last transaction or when a report is made to the Centre
- **Section 26B & 26C:** Avoid any business relationship or activity/transaction with persons identified by the United Nations Security Council or the Targetted Financial Sanctions lists
- **Section 28:** Submit Cash Threshold Reports (CTR) within the required time limit
- **Section 28A:** Submit Terrorist Property Reports (TPR) within the required time limit
- **Section 29:** Submit Suspicious Transaction Reports (STR) and Suspicious Activity Reports (SAR) within the required time limit.
- **Section 42:** Implement a risk-based approach to anti-money laundering and counter-terrorist financing activities, documented in an RMCP
- **Section 42:** Implement oversight, governance and controls in line with the RMCP

- **Section 43B(1) & (4):** Register with the FIC and inform them of any changes to its registration particulars
- **Section 43:** Train all employees around FICA and the RMCP

2.2 Consequences of non-compliance with FICA

The firm recognises that non-compliance with FICA may result in considerable negative consequences for the firm, its management, controlling parties and employees. These consequences include, but are not limited to:

- reputational damage
- reduction of client, supplier, and market confidence
- financial losses
- civil or criminal fines
- custodial sentence/imprisonment.

3. Governance

The firm asserts to undertake mitigative action to minimise the risks of non-compliance with FICA through the implementation of reasonable and appropriate controls in the form of the processes and procedures outlined in this document as well as any other informal approaches as deemed helpful. In line with s.42(2), where appropriate, these are documented herein and implemented across the business.

As per Section 42A(1), the person or persons exercising the highest level of authority within the firm will ensure compliance by the firm and its employees with the provisions of this Act and its Risk Management and Compliance Programme.

3.1 Appointment of an AML/CTF Compliance Officer

In line with Section 42A(2) the firm management asserts to appoint, in writing, a named person who has sufficient independence, authority, skill, competence and seniority within the firm to act as AML/CTF Compliance Officer with the purpose of overseeing compliance by the firm and all its employees with FICA.

The AML/CTF Compliance Officer will ensure that their appointment is registered with the Financial Intelligence Centre within 90 days of appointment or as soon as possible should this period have passed.

The AML/CTF Compliance Officer will be assigned a variety of responsibilities that seek to mitigate the risk of the firm being implicated in the financial crimes of money-laundering and terrorist financing as well as non-compliance with FICA. These will include, but not be limited to:

- Managing and monitoring the firm's compliance with all aspects of the Financial Intelligence Centre Act
- Engaging with the FIC to remain up to date with FICA requirements, including any notice in the Gazette or in writing, issuing a directive which the AI must comply with

- Managing the review and update of the RMCP as appropriate notice in the Gazette or in writing, issue a directive to an institution to whom the provisions of this Act apply which the AI must comply with.
- Ensuring that the firm is registered with the FIC and that the registration is updated with any changes to the firm's particulars
- Be responsible for appropriate client termination or exit
- Be responsible for senior management approval of high risk clients, DPIPs or FPPOs
- Ensuring employees undergo annual FICA awareness training
- Acting as the central point of contact regarding all activities related to FICA
- Review and submit reports to the Financial Intelligence Centre on behalf of the firm

The role and appointment will be reviewed annually and reassigned where deemed necessary or appropriate.

3.2 Registration with the Financial Intelligence Centre

The AML/CTF Compliance Officer will ensure that the firm is registered with the Financial Intelligence Centre within 90 days of commencement of business or as soon as possible should this period have passed. This registration will include the recording the appointed AML/CTF Compliance Officer.

A record of the login information and confirmation of registration will be kept securely by the AML/CTF Compliance Officer and not shared with any other party.

The AML/CTF Compliance Officer will ensure that any changes to the firm business, location or contact details will be notified to the FIC through the update of the FIC 'GoAML' portal website within ninety (90) days of any such change. A record of the change will be kept on file by the AML/CTF Compliance Officer.

3.3 Risk Management and Compliance Programme ("RMCP")

In recognition of the consequences associated with non-compliance, and in acknowledgement of the requirements place on it by the Financial Intelligence Centre Amendment Act, the firm has established this AML & CTF RMCP which has been reviewed, signed off and adopted by the governing body of the firm and its compliance will be supervised by the appointed AML/CTF Compliance Officer.

The purpose of this Programme is to enable the firm to appropriately identify and mitigate the risk that the provision of its products or services may involve or facilitate money laundering activities or the financing of terrorism and apply its resources in a proportionate manner.

The RMCP will seek to appropriately provide for the manner to:

- determine if client entering a business relationship of single transaction
- determine is a client is anonymous or using false/fictitious name
- determine the establishment and verification of identities
- determine if future transactions are consistent with knowledge of client

- conduct additional due diligence measures in respect of legal persons, trusts and partnerships
- conduct ongoing due diligence and account monitoring in respect of business relationships
- examine complex or unusually large transactions and unusual patterns of transactions which have no apparent business or lawful purpose
- provide the manner and process by which the institution will confirm information relating to a client when the institution has doubts about the veracity of previously obtained information
- provide for the manner in which and the processes by which the institution will perform the customer due diligence during identification and verification and when the institution suspects that a transaction or activity is suspicious
- provide for the manner in which the accountable institution will terminate an existing business relationship when unable to conduct initial or ongoing due diligence
- provide for the manner in which and the processes by which the accountable institution determines whether a prospective client is a foreign prominent public official or a domestic prominent influential person
- provide for the manner in which and the processes by which enhanced due diligence is conducted for higher-risk business relationships and when simplified customer due diligence might be permitted in the institution;
- provide for the manner in which and place at which the records are kept in terms of Part 2 of this Chapter;
- enable the institution to determine when a transaction or activity is reportable to the Centre under Part 3 of the Act;
- provide for the processes for reporting information to the Centre under Part 3 of this Chapter;
- provide for the manner in which the RMCP is implemented so as to enable the institution to comply with its obligations under FICA

This document, once approved by the Management of the firm, will be made available to each of its employees involved in transactions to which this Act applies and will, on request, make a copy of the documentation describing the Risk Management and Compliance Programme available to the Centre; or a supervisory body which performs regulatory or supervisory functions.

Where any requirement of the Act is identified as not application to the firm, as required per Section 42(3), it will be clearly noted with justification for such decision.

As such, as the firm does not operate branches, subsidiaries or other operations of the institution in foreign countries, this is not provided for within this document.

3.4 Maintenance of the RMCP

The AML/CTF Compliance Officer will ensure that this RMCP and all related methods, processes and procedures are reviewed annually, but sooner should there be legislative or business changes which demand its update.

Changes to the RMCP or its related methods, processes, and procedures will be noted in the version control section of the RMCP. The updated RMCP will then be reviewed, signed

off and adopted by the governing body of the firm before changes are implemented, trained, and communicated to employees as appropriate.

3.5 Training

The AML/CTF Compliance Officer will ensure that all appropriate employees undergo training around anti-money laundering, the countering the financing of terrorism, FICA and the appropriate content of this AML & CTF compliance programme and its related methods, processes, and procedures to enable them to comply with the provisions of the Act and RMCP which are applicable to them. This will be provided to all staff at least every year or when changes in legislation demand it. Training will be provided to all new staff as appropriate before they are permitted to commence their duties.

The AML/CTF Compliance Officer will ensure that a record of all training undertaken is dated and kept for at least five (5) years from the date of the training.

4. Risk-based approach

A risk-based approach allows the firm to identify, assess, and understand the money laundering and terrorist financing risk to which it is exposed, and take the appropriate mitigative measures appropriate to the level of risk identified.

This flexibility allows for efficient use of limited resources to mitigate the money laundering/terrorist financing risks identified in the business. It enables enhanced measures to be taken in situations where the risks are higher and the application of more simplified measures where the risks are lower.

4.1 Risk categorisation

The firm will use a range of assessment criteria in combination with consideration of the client's level of engagement and behaviour to evaluate the potential risk of implication in money laundering or terrorist financing. Information and documentation obtained to evidence any criteria will be of such quality to be relied upon and provide suitable evidence.

The firm will use the gathered information during due diligence to calculate and assign each client a risk rating in the Docfox application. This risk assessment and subsequent resultant rating will be recorded in the Docfox application against the client record.

This risk rating will determine and inform the extent of due diligence that will be performed at onboarding and throughout any activity, transaction, or business relationship.

Where the potential risk is assessed higher, then enhanced due diligence will be performed and senior-management approval sought through the senior management sign-off process (Section 4.9).

Once a client is onboarded, the firm will continuously be mindful of risk and where appropriate, should a concern be raised that the assigned risk level is inappropriate, it will

be reported to the AML/CTF Compliance Officer as soon as possible but within one business day.

4.2 Risk factors

In taking a risk-based approach to its AML/CTF Compliance, the firm will consider a range of factors when assessing the potential level of money-laundering and/or terrorist financing exposure risk posed by a client. These are based on widely accepted elements known to be reasonable indicators of money laundering or terrorist-financing risk.

This framework and any associated risk factors will be reviewed in line with the periodic review of the firm's Risk Management & Compliance Framework and will consider any legislation, guidance, trends, and typologies that are available at the prevailing time.

As no single risk factor is likely to be able to infer heightened risk, all risk factors will be considered as part of a bigger holistic view of the client using all known information and evidence.

4.2.1 Product and Services

Certain products and services are more susceptible to being leveraged as part of money laundering/terrorist financing activities, such as:

- Products/services/activities that facilitate a degree of anonymity
- Products/services/activities that involve the receipt, holding, management or transmission of client money, securities or other assets
- Products/services/activities that involve the management of client bank, savings or securities accounts
- Products/services/activities that involve the formation, operation, management, sale or purchase of companies or legal persons
- Products/services/activities that involve the escrow, purchase, sale or transfer of assets
- Products/services/activities that involve the legitimisation or credibility of individuals, documents or transactions
- Products/services/activities that allow funds to be freely received from or paid to unrelated or unidentified third parties
- Products/services/activities that facilitate international transactions, particularly to higher-risk jurisdictions
- Products/services/activities that facilitate use of less regulated crypto/digital currencies or exchanges

Product and service alone would not necessarily result in the client being assessed as higher risk; however, it should be considered holistically as part of the overall risk assessment.

Whilst many of the products and services offered by the firm could be considered lower risk for money laundering and terrorist financing, the firm possesses a range of specialised skills, products and services that may be leveraged by criminals to enable them to transfer value obtained from criminal activities between parties or disguise ownership. As such, the firm has considered and assessed the ML/TF risk presented by the products, services

and activities it offers in order to identify, assess and manage the risk that they may facilitate money laundering activities or the financing of terrorist and related activities.

Client funds and accounts

Criminals may seek to use access to accounts in order to place, layer or integrate illicit funds into the legitimate financial system. Any client accounts and monies will be held separate to the firm's accounts at all times. No funds will be permitted to pass through any client account without being attached to an underlying transaction or valid purpose and the appropriate fee earner or staff member will be held responsible for accounting for all funds flowing through any account under control of the firm.

Escrow and early termination of products or services

Escrow, contracts or fixed-term products may be signed that are intended to continue for a pre-defined or ongoing period of time or be paid on a defined trigger basis. Where these are cancelled prematurely or unexpectedly, the appropriate fee earner or staff member will assess whether there is reasonable due cause for such cancellation, especially where a refund or repayment is subsequently made, or the client has disregard for any penalties.

Purchase, sale or transfer of property or assets

Commercial and residential property, as well as higher-value, liquid or mobile assets are demonstrated as vulnerable to money laundering or terrorist financing schemes as a way to hold, control or transfer value. Criminals may seek to invest the proceeds of crime or title assets in their own name or make use of false identities, family members, friends, business associates or legal persons. The firm will carefully consider who they are acting for at the outset of any transaction, whether the value of the property or asset appears fairly represented, who will have ultimate control, access or benefit of any property or asset and if any amounts paid or value transferred could realistically have been generated or earned by that particular party, under lawful conditions.

Repeated, multiple, divergent or convergent transactions

Transactions that repeat, move, divide or consolidate assets between accounts, institutions or jurisdictions, or that transfer ownership may indicate potential suspicious activity. Where this is identified, the firm will undertake appropriate review and monitoring of activities and assess whether the client has reasonable due cause for such transaction patterns and that any recipient of funds aligns to expected activity.

Physical storage of property, documents or assets

The provision of storage facilities may present an opportunity for schemes to hold, control or transfer value, primarily through physical access to the facilities provided. The firm will carefully consider who they are acting for at the outset of any transaction and undertake appropriate monitoring of activities and access control to any property or asset stored or held on behalf of the client to identify whether any activity is occurring under lawful conditions or may represent suspicious activity.

Funds in payment of fees, payments or deposits

Whenever clients make substantial funds available in payment of fees or deposits, especially where an element of dishonesty or illegality is linked to the client, even by a mere allegation, the appropriate fee earner or staff member will consider the client's source of funds and/or source of wealth, and any other relevant information in an attempt to reasonably determine whether the amount paid could realistically have been generated or earned by that particular client, under lawful conditions.

Third-Party Payments or Receipts

Third-party payments (or receipts) are payments (or receipts) made (or received) on behalf of the client into (or from) accounts not in the name of the client. Where third-party payments are made, or third-party receipts received, the firm will consider the relationship of the third-party to the client and the legitimacy of such third-party (for example, payment of fees by an unknown and apparently unrelated third-party). The appropriate fee earner or staff member will attempt to make reasonable assessment to identify the third party and determine whether any amount paid into the firm's account could realistically have been generated or earned by that particular third-party, under lawful conditions and if the reason for the third-party transaction appears reasonable.

Cross-border payments or asset transfers

Whenever clients are to send or receive a substantial amount of funds or assets cross-border, the appropriate fee earner or staff member will consider the client's source of funds and/or source of wealth, nature of business, counterparties to the transaction and any other relevant information in an attempt to reasonably determine the legitimacy of such cross-border activity and whether the funds could realistically have been generated or earned by that particular client under lawful conditions.

Products/services/activities that involve the formation, operation, management, sale or purchase of companies or legal persons

The use of complex legal persons and entities are one way in which the beneficial owner of assets may be disguised, or legitimacy provided to transactions or matters. Care will be taken in terms of assessing the legitimacy of requests when providing any products, services or activities that could be used to conceal identity or beneficial ownership.

Products/services/activities that involve the legitimisation or credibility of individuals, documents or transactions

Criminals may seek to use abuse the reputation of a Firm to provide an element of legitimacy to schemes or payments. The Firm will continue to monitor clients in line with the RMCP for any actual or potential suspicion that the firm, its products, services or reputation are being abused or misused.

4.2.2 Higher-Risk Jurisdictions

While no rigid formula can exist for determining whether a country falls into a higher-risk category, there are several factors that can be considered in making its determination, including:

- Countries subject to sanctions, embargoes or restrictive measures
- Countries that are not FATF members or have been identified by FATF as 'non-cooperative' countries or as having deficiencies in their anti-money laundering and counter terrorist financing controls

Geographic risk is an important component to leverage when assessing customer and transaction risk as each country poses different levels of risks; however, it is important to consider a client's *specific* relationship to those jurisdictions associated with higher levels of financial crime to assess the level of risk presented.

The firm has adopted the FATF guidance ([https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate))) around jurisdictions under increased monitoring as an indicator of the potential risk posed by various jurisdictions, and these have been included as a key element of the firm's risk rating criteria as identified below.

Jurisdictions identified as potentially higher risk for the purposes of this RMCP:

Albania	Iran	Pakistan
Barbados	Jamaica	Panama
Botswana	Malta	Philippines
Burkina Faso	Mauritius	Senegal
Cambodia	Morocco	South Sudan
Cayman Islands	Myanmar	Syria
Ghana	Nicaragua	Uganda
Haiti	North Korea (DKR)	Yemen
Jordan	Turkey	Zimbabwe

4.2.3 Entity type

Entity type on its own would not necessarily make a client higher risk; however, certain entity types are more susceptible to money laundering and/or terrorist financing, for example (but not limited to) entities that allow for complex structures that make control/ownership difficult to determine.

The risk a particular type of entity potentially presents will be considered holistically along with other risk factors, such as size and reputation, duration of relationship, purpose, jurisdictions in which it operates, as well as any adverse information found on the client.

4.2.4 Source of funds

Money Laundering is the deliberate disguising of funds obtained by illicit means so the firm will take adequate measures to establish the source of funds which involved in activities/transactions.

In line with FIC Amendment Act section 21a(c) the firm will identify the source of funds which a client expects to use in concluding transactions.

When dealing with an FPPO or DPIP, the firm will identify the source of funds and consider if there is any information about corruption or evidence that government or public funds are

being used inappropriately. In addition, the wider source of wealth for a DPIP or FPPO client will be considered.

The source of funds/wealth may not necessarily be used alone as a justification for inferring heightened risk and whilst there is no obligation to obtain proof of the source of funds, it may be prudent to ask for some supporting evidence to confirm the information provided where there is suspicion or doubt whether the source of funds is consistent with the risk profile of the client and their business. Guidance is provided in Annexure 10.

A range of credible sources (including FATF guidance) has been used to reasonably assess the potential risk posed by various funding sources and these have been included as a key element of the firm's risk rating criteria.

Sources identified as higher risk are those which are more difficult to evidence their true source such as gifts, donations, winnings, third party payments and any purported loans from non-financial institution parties.

4.2.5 Nature and purpose of transaction or business relationship

Whether a client is seeking to enter into a discrete single activity/transaction, or a longer-term business relationship – and their requested product or service can affect the level of risk.

Whilst product or relationship type alone may not necessarily be used as a justification for inferring heightened risk; other risk factors should be considered to assess whether the anticipated relationship type, and the purported purpose of any matter, product or service requested makes sense in light of all other information known.

As per Section 21A, the firm will take reasonable steps through client disclosure to establish the intended nature and purpose of the business relationship with the client.

This information will continue to be used throughout the client lifecycle to enable reasonable steps to be taken to ensure transactions performed in the course of a business relationship are consistent with the knowledge of the client.

4.2.6 Industry

The economic sector in which a customer or activity/transaction is involved can affect the level of risk. Corruption and financial crime can occur in any sector; however, based on several case studies and an analysis of their unique attributes by FATF, it appears that several sectors are more prone to corruption or use in a money laundering or financing of terrorism scheme.

As required by Section 21A(a) the firm will take reasonable steps through client disclosure and independent research (as appropriate) to establish the nature of the client business.

Some key sectors identified are described below; however, inclusion in itself does not necessarily mean an individual industry is wholly corrupt or incriminated in any financial crime or corruption, however, may present a higher risk.

- **Cash Intensive Entities:** Entities with access to high volumes of cash or cash-based income/ donations, may present the opportunity to move value through the misdirection of cash, or the co-mingling of illicit cash with genuine income
- **Charitable Firms / NGOs:** These entities often have a presence in higher risk jurisdictions by virtue of their philanthropic nature and may have access to high volume of cash-based donations. This may provide international money laundering operations with the ability to move value through mingling illicit cash with genuine donations or leveraging the framework for national and international financial distributions.
- **Chemicals:** Chemicals diverted from legitimate commerce may be used in the production of illicit drugs or weapons/explosives. Clients in the chemicals industry may not automatically be considered a higher risk, but it is important to understand the nature of the activity, the type and uses of chemicals (e.g. dual-use products) that are being produced/sold, the address from which the entity operates (e.g. it would be suspicious if the entity is operating from a residential address), the jurisdictions in which the client operates and with which it trades, counterparties, and any adverse information on the client or its related parties
- **Defence Industry:** Contracts with this industry may be subject to secrecy requirements because work relates to national security and is protected by secrecy and confidentiality legislation. There are also many restrictions on trading in weapons and other military equipment.
- **Developmental and Other Types of Assistance:** Activities related to significant amounts of foreign aid or investment may give rise to a risk of corruption and consequently a risk of corruption-related money laundering
- **Dormant or Passive Income:** Entities that generate substantial income yet appear dormant with no active business interests may indicate a potentially higher risk around their true source of funds.
- **Extractive Industries:** There has repeatedly been a correlation between countries that obtain their wealth from the extraction of natural resources, such as oil, coal, minerals and timber, and the incidence of financial related crime
- **Gambling and Gaming:** Casinos or gaming firms are popular money laundering targets because of their high volume of cash activities and may be used to co-mingle illicit funds with those that are legitimate
- **Government Procurement Activities:** Public procurement activities are significantly vulnerable to corruption. The scope of some of government acquisition projects can lead to a reduction of transparency, and the nature of contracts can make it difficult to analyse whether prices have been inflated as a result of corrupt activities
- **High-value assets:** Higher value assets may be purchased by illicit funds and used to transfer value. Those that provide easier transport/transfer may present a higher risk (e.g. jewellery, gems, coins, art, antiques, vehicles).
- **Import and Export Services/Freight and Logistics companies:** Import and export services may provide international money laundering operations with the ability to move value through under/overpricing of goods or misrepresenting quantities or descriptions. Import & export services, in general, are not necessarily higher risk; however, it is important to understand the nature of the activity, including the products/goods/services that are being exported/imported/stored, counterparties, and the jurisdictions in which the client operates and with which it trades.

- **Minerals – Precious Metals and Stones:** Mines and dealers provide launderers access to high-value assets that may sometimes be purchased with little or no client identification and then later sold to provide a 'legitimate' source of cash proceeds. Diamonds and precious metals mined in war zones are often sold to finance an insurgency or war. Clients involved in the mining of precious metals and stones may not automatically be considered a higher risk, but it is important to understand the nature of the activity, the jurisdictions in which the client operates and with which it trades, counterparties, any adverse information on the client or its related parties
- **Scrap, Second-hand & Recycling:** Clients that trade in scrap metal, recycling or second-hand goods are often cash-intensive and therefore at risk of being used as fronts for money laundering. In South Africa specifically, there is a risk that these businesses are involved in illicit trade in copper that has been stolen from public resources
- **Wild/Exotic Animals:** Clients with any involvement in wild/exotic animals are susceptible to environmental crimes and abuse of marine resources. For example, rhino poaching involves a range of factors, including game rangers, veterinarians, professional hunters, and farmers that conspire with criminal networks. Similarly, there is a complex web of interests in abalone poaching, including the collusion of local fishing communities

A range of sources has been used to reasonably assess the potential risk posed by various industries, markets, and sectors and these have been included as a key element of the firm's risk rating criteria

Industries identified as a higher risk for the purposes of this RMCP:

- Dormant and/or passive incomes
- Financial and insurance (Not Regulated)
- Gambling & betting
- Hunting & related services
- Import & export agency
- Manufacturing - chemicals/pharmaceuticals
- Manufacturing - defence and/or ammunitions
- Manufacturing - tobacco/hemp
- Mining, quarrying & related services
- Political activities
- Public & State-Owned Entities (SOE)
- Religious activities
- Wholesale, retail & repair trade - restaurants & takeaways
- Wholesale, retail & repair trade - tobacco/hemp
- Wholesale, retail & repair trade - jewellery, metals &, stones
- Wholesale, retail & repair trade - motor vehicles
- Wholesale, retail & repair trade - scrap & recycled materials

4.2.7 Adverse Media

Adverse media can be defined as unfavourable information from a variety of sources, including traditional newspapers, the internet or radio and television. It is important when

considering adverse media that the source of information is considered reliable, especially with the proliferation of personal blogs, social feeds and unstructured forums.

In line with best practice guidance from the Financial Action Task Force (FATF), adverse media checks can reveal involvement with crimes such as money laundering, financial fraud, drug trafficking, financial threat, organised crime, or terrorism. These links pose a serious threat to the firm's reputation.

The firm will undertake adverse media checks using the DocFox application and any other appropriate sources to assess whether any publicly available information identifies elements that can be considered as part of the client due diligence and risk assessment process. Evidence of these adverse media checks will be recorded against the client record held in Docfox.

4.2.8 Foreign Prominent Public Officials and Domestic Prominent Influential Persons

As per Sections 21F and 21G the firm must determine if their clients, including their beneficial owners and authorised representatives, hold a position of a domestic prominent influential persons (DPIP) or foreign prominent public official (FPPO) as defined in Schedule 3A of the FIC Amendment Act.

Clients that are family members and/or known close associates of DPIPs or FPPOs, although not themselves DPIPs or FPPOs, will be onboarded as though they are as per Section 21H.

Holding an identified position of a domestic prominent influential persons (DPIP) or foreign prominent public official (FPPO) in itself does not necessarily mean an individual is corrupt or that they have been incriminated in any financial crime or corruption; however, they potentially represent a higher risk because they may be in a position to exert influence or authority over, or have access to state assets and funds, policies and operations – including procurement awards, public expenditures, use of government-owned resources, control over regulatory approvals, the awarding of licenses and concessions.

It is important, however, to understand that not all those holding an identified position present the same level of risk and that this risk will vary depending on numerous factors, including the country of origin, relative position of control/power/influence, the industry/sector involved, and the products and services used.

The firm will treat transactions with Foreign Prominent Public Officials (or their immediate families or close associates) as inherently high risk. Domestic Prominent Influential Persons (or their immediate families or close associates) will undergo an appropriate enhanced initial due diligence and risk assessment that will inform the ongoing appropriate monitoring and due diligence requirements.

Regardless of the above all DPIP and FPPO clients (or their immediate families or close associates) will be subject to identification of source of funds/wealth, senior management sign-off and enhanced ongoing monitoring.

4.3 Manual downgrade of risk categorisation

New clients identified as higher risk should not be downgraded as there is no previous history with the client, and therefore, it is not always possible to demonstrate that the AML/CTF risk is reduced. However, due to limitations inherent in any fixed matrix, a more prudent approach was taken with respect to some risk factors so that certain clients would be flagged as high risk.

In certain circumstances therefore, a recommendation can be made that the client be downgraded where the client has been assigned an inappropriate risk rating in Docfox and due diligence shows that the client does not present a higher AML/CTF risk, for example;

- The client has undertaken a reasonable number of activities or transactions in terms of volume and value to be considered not dormant by the firm, and;
- Ongoing or enhanced due diligence has not led to the identification of any information, transaction or activity that is suspicious or unusual, and;
- The client has not been subject of, or related to, a report to the FIC
- The client is operating in a potentially higher risk industry, but is subject to strict regulatory oversight (e.g. publicly listed mining entities)

The following are clients and/or circumstances in which the client's AML/CTF Risk may never be adjusted downwards:

- There is evidence of potentially suspicious activity or property
- Clients with evidence or allegations in the public domain of bribery, corruption, fraud, embezzlement, tax evasion, gross misconduct, or criminal activity of a serious nature
- Clients identified on any sanctions watchlists (including the TFS and UN lists)
- Clients that are Foreign Prominent Public Officials (or their immediate families or close associates)
- Clients that have a Foreign Prominent Public Officials (or their immediate families or close associates) as an authorised person, related party or UBO

All changes to client ratings will be referred to the AML/CTF Compliance Officer for input and assessment of the AML/CTF risk prior to circulating to senior management for sign-off. The AML/CTF Compliance Officer will ensure that the firm keeps a record of all manual risk rating changes against the client profile with supporting justification/reason/evidence as appropriate.

4.4 Manual upgrade of risk categorisation

The firm may, at the sole discretion of the AML/CTF Compliance Officer, manually upgrade the risk categorisation of a client to increase the level of ongoing due diligence where due diligence and monitoring has led to the identification of any information, transaction or activity that warrants additional oversight. This would include all clients that have been subject of, or related to, a report to the FIC.

The AML/CTF Compliance Officer will ensure that the firm keeps a record of all manual risk rating changes against the client profile with supporting reasons.

4.5 False or fictitious names and anonymous clients

As required by Section 20A, the firm will not enter a relationship or perform a transaction with any client who appears to have a false or fictitious name, who appears anonymous, or where it is unable to establish or verify the identity of a client or other relevant person (Section 21E).

Where there is suspicion that a false or fictitious name is being used, the employee will report their suspicion to the AML/CTF Compliance Officer as soon as possible but within one business day of such a suspicion

The AML/CTF Compliance Officer will investigate all such reports, terminate any relationship or transaction, and submit a report to the FIC where appropriate. The AML/CTF Compliance Officer will keep a record of all potential or actual clients who are declined or terminated.

4.6 Doubts surrounding veracity of information or evidence

Where an employee has doubts about information obtained from a client, that gives rise to suspicion or concern, then the employee will report their suspicion to the AML/CTF Compliance Officer as soon as possible but within one business day of such a suspicion.

The AML/CTF Compliance Officer will investigate all such reports, attempt to confirm client information held through appropriate due diligence efforts, and where unable to do so, as appropriate, terminate any relationship or transaction and submit a report to the FIC. The AML/CTF Compliance Officer will keep a record of all potential or actual clients who are declined or terminated.

4.7 Terminating clients based on risk assessment

The firm commits to decline a single activity/transaction or business relationship where, based on the clients' risk assessment, the firm is unable to (at the sole discretion of the AML/CTF Compliance Officer) put in place mitigative strategies to reasonably address any potential or actual risk presented by a potential or actual client or where the profile of the client or their intended activity or transaction is outside of the risk appetite of the firm.

The AML/CTF Compliance Officer will investigate all such situations, terminate any relationship or activity/transaction, and submit a report to the FIC where appropriate. The AML/CTF Compliance Officer will keep a record of all potential or actual clients who are declined or terminated.

4.8 Terminating clients when unable to conduct due diligence satisfactorily

The firm commits to decline a single transaction/activity, decline a potential business relationship, or terminate an existing business relationship where the firm is unable to:

- Identify a client, their related parties, ultimate beneficial owner/s or authorised representatives
- Identify the source of any funds the client intends to use
- Identify the nature and purpose of the business relationship or activity/transaction

The AML/CTF Compliance Officer will investigate all such situations, terminate any relationship or activity/transaction, and submit a report to the FIC where appropriate. The AML/CTF Compliance Officer will keep a record of all potential or actual clients who are declined or terminated.

4.9 Senior Management approval process

The Senior Management approval process will be managed by the AML/CTF Compliance Officer and invoked whenever senior management sign-off is required. This includes, but is not limited to:

- Where it is established that a client, or a related party or beneficial owner is a DPIP or a known associate or immediate family member of such a person
- Where it is established that a client, or a related party or beneficial owner is an FPPO or a known associate or immediate family member of such a person
- Where a client has been identified as high-risk
- Where the AML/CTF Compliance Officer wishes to manually upgrade or downgrade the risk rating of a client

Where the AML/CTF Compliance Officer wishes to seek senior management sign-off, they will complete the senior-management sign-off form, or provide the same request and information by email, and/or record evidence of this in the DocFox application. Only when sign-off has been given can the activity that prompted senior management approval be continued or actioned. Refer Annexure 10.

5. Due diligence

As per Section 21, the firm will assert to identify and verify clients and collect information and evidence of sufficient quantity and quality so as to be able to assess the potential level of money laundering and terror financing risk presented. This due diligence will occur before entering a business relationship or concluding a single activity/transaction.

As part of this, the firm will reasonably satisfy itself that:

- The client is who they claim to be
- It knows whether the client is acting on their own behalf or on behalf of another party, and where appropriate, identify and verify those parties
- It knows the related parties and Ultimate Beneficial Owner/s ("UBO") of a legal person
- It knows the nature and purpose of the business relationship or single transaction
- It knows the source of funds of the client
- There are no prohibitions/restrictions to entering or continuing a business relationship or single activity/transactions with the client

Where a client was onboarded before the FIC Amendment Act was promulgated, as per Section 21(2), the firm will take reasonable steps to update their client due diligence to the standards of the FIC Amendment Act before concluding a transaction.

The firm will make use of the DocFox application to record and verify client information.

The following provides guidance as to the minimum requirement for onboarding of clients; however, discretion is advised in collecting sufficient information and evidence as it may be necessary to obtain a level of comfort around the client, their activities, their source of funds and the potential risk presented. Employees are guided to contact the AML/CTF Compliance Officer for support and assistance as appropriate.

Where an employee has identified suspicious or unusual activity, information that cannot be reasonably explained, transactions or requests that appear to have no valid or lawful purpose, or reasonable doubt surrounding the veracity of supplied identity information, they will notify the AML/CTF Compliance Officer as soon as possible but within one business day of such a suspicion.

5.1 Identification

Identification refers to the process of obtaining identification information from the client, their authorised representatives and related parties during the establishment of a business relationship or before concluding a single transaction.

Different client types will require different identification information, and these are discussed in detail in Annexure 10.

In addition to identity, the firm asserts to establish and understand any related parties, the UBO (as appropriate), the nature of the business relationship, the purpose of the business relationship and the source of funds anticipated to be used to conclude transactions.

5.2 Verification

Verification refers to the process of corroborating the identification information from the client, their representatives, and related parties by comparing the information against information contained in documents or electronic data or created by reliable and independent third-party source/s. Verification occurs during the establishment of a business relationship, before concluding a single transaction, or during a business relationship as part of a periodic or trigger-based review.

The firm will make use of the DocFox application to undertake reasonable verification of core documentation against CIPC and Home Affairs. Evidence of these verifications will be recorded in the Docfox system. The legitimacy and reliability of any other sources will be appraised when considering all information from third party sources. Sources that provide a high level of confidence may include government-issued documents or databases, widely recognised news outlets or face-to-face evidence.

5.3 Single transactions and minimum standards

The FIC Act and Guidance Note 7 define a single transaction as a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5000.00 (the amount is determined by the Minister of Finance in the Regulations).

This can be described as occasional or once business where there is no expectation on the part of the accountable institution or the client that the engagements would recur over a period of time.

The firm has determined what constitutes a single transaction in the context of its particular business for purposes of complying with the obligations of the FIC Act in as far as it applies to single transactions. This definition aligns to the guidance of the FIC inasmuch as a transaction other than a transaction concluded in the course of a business relationship and where the value of the transaction is not less than R5000.00 and there is no expectation on the part of the client or firm that there will be ongoing or additional transactions.

Whilst Accountable institutions are not required to carry out the full scope of CDD measures in respect of clients conducting single transactions below the value to be set by the Minister of Finance, this does not apply to the obligations set out in section 20A of the FIC Act. As such, the firm recognised that in spite of a single transaction being below the threshold, the accountable institution is still prohibited from dealing with an anonymous client or a client with an apparent false or fictitious name.

As a result, the firm will obtain and record at least some information describing the identity of the client, including the full name and identity number of the client and other information such as a contact number – with the option to undertake standard due diligence at the discretion of the firm.

Outside of single transactions, the firm has identified minimum requirements for due diligence and supporting evidence to support the risk-based approach. These are detailed in Annexure 10.

5.4 Additional due diligence for legal persons

As guided by Sections 21B(1)(2)(3)&(4), the firm will undertake additional due diligence to legal persons to identify and verify all related parties and the Ultimate Beneficial Owner/s (“UBO”), making use of the Docfox application.

5.4.1 Related Parties

A related party is any party that own the assets of, has control over, or are authorised to act behalf of a legal person.

Related parties would include (but are not limited to);

- Ultimate Beneficial Owner (“UBO”) of a legal person
- Partners to a Partnership
- Trustees, founder/settlor/donor, executors and beneficiaries to a trust
- Members of a close corporation
- Directors, or those in a position to exert considerable power over an entity
- Authorised persons of a client (e.g. authorised signatories, extra cardholders, guardians etc.)

Once the related parties have been identified, they will be required to be identified and verified as per a natural person client standard of this RMCP. Should any parties be identified as a DPIIP or FPPO (or their immediate families or close associates), the client file will be referred to the AML/CTF Compliance Officer for review and senior management sign-off.

5.4.2 Ultimate Beneficial Owners (“UBO”)

A UBO is the natural person or natural persons who, own a legal person or exercises effective control over it. In determining the UBO, a process of elimination is applied as follows:

1. Determination of the natural person who (independently or together with another person) has controlling ownership of the legal person. A standard shareholding of 25% will be used to determine majority ownership. Where an entity is considered a higher risk, this may be reduced to 10% shareholding.
2. Determination of who exercises control of the legal person through means other than majority shareholding
3. Determination of who exercises control over the management of the legal person, including in the capacity of CEO, CFO and COO

Whilst disclosure may be sufficient for simple organisations, where an organogram is requested for a more complex legal person structure, or there is doubt surrounding the veracity of the information provided by the client or their representative, the firm will request it be certified by an appropriate independent third party such as an auditor, attorney or accountant.

For a Partnership, the firm will identify and verify the partners and persons exercising executive control over the partnership. These will be considered the UBO.

For a Trust, the firm will identify and verify the donor/founder, trustee/s and beneficiary/ies. These will be considered the UBO.

Once the UBO has been identified, they will be required to be identified and verified as per a natural person client standard of this RMCP. Should the UBO be identified as a DPIIP or FPPO (or their immediate families or close associates), the client file will be referred to the AML/CTF Compliance Officer for review and senior management sign-off.

5.5 Representatives acting on behalf of a client or client acting on behalf of another person

Any natural or legal person seeking to act on behalf of another may only do so when supported by a valid evidence of authority, for example a power of attorney, court resolution, mandate, and/or authorised signatory letter as appropriate. Representatives of clients and the underlying client themselves will be subject to identification and verification scrutiny making use of the Docfox application. This evidence will be kept on file against the client records.

Once the representatives have been identified, they will be required to be identified and verified as per a natural person client standard of this RMCP. Should any parties be identified as a DIIP or FPPO (or their immediate families or close associates), the client file will be referred to the AML/CTF Compliance Officer for review and senior management sign-off.

Should there be suspicion or doubts around veracity of the authorisation of the representatives or the purpose of legality of any instruction given, no instructions shall be enacted and the AML/CTF Compliance Officer must be notified as soon as possible but within one business day of such a suspicion for further investigation.

5.6 Sanctions Screening

The firm acknowledges that it must avoid entering into an activity/transaction or business relationship with persons and entities identified on the UN Security Council Sanctions or Targeted Financial Sanctions (TFS) lists.

The firm will take reasonable measures to identify whether a client or client representative is designated on these lists through the use of the DocFox application which screens all clients on initial application and on a daily basis (refer Annexure 10) against a wide range of watchlists. Any potential 'hit' against a sanctions list will provide immediate notification by email to the firm's AML/CTF Compliance Officer.

If a client, related party, UBO or a client representative is suspected of being listed on the UN Sanction list or the TFS, the employee will report this suspicion to the AML/CTF Compliance Officer immediately.

The AML/CTF Compliance Officer will investigate all such reports, terminate the relationship and submit a report to the FIC where appropriate.

The firm notes that under Section 26C, the Minister may permit the provision of financial services or the dealing with property if it is necessary to:

- a) provide for basic expenses;
- b) satisfy a judgement of arbitral award before appearing on a sanctions list;
- c) make a payment due to a third party under contract or obligation made before appearing on sanctions list;
- d) accrue interest on accounts holding property under Section 26B;

In such circumstances, the firm will comply with any such written directives under Section 26C.

5.7 Identification of Foreign Prominent Public Officials ("FPPO")

A foreign prominent public official (FPPO) is an individual who holds, or has held at any time in the preceding twelve months, in a foreign country a function as listed in Schedule 3B of the FIC Act:

- Head of state or head of a country or government
- Government minister or equivalent senior political or leader of a political party

- Member of a foreign royal family
- High-ranking member of the military
- Senior judicial official
- Senior executive of a state-owned entity

The determination of FPPO applies to the client that is onboarded, the authorised representatives, related parties and beneficial owners of the client. Clients that are family members and/or known close associates of FPPOs, although not themselves FPPOs, must be treated as though they are.

The following relationships between a natural person and a client will be regarded as an immediate family member relationship:

- Parents
- A spouse, civil partner or a life partner
- A former spouse, civil partner or a life partner
- Children and stepchildren and their spouse, civil partner or a life partner
- Siblings and their spouse, civil partner or a life partner

The following relationships between a natural person and a client will be regarded as a close associate:

- Known partners (for example; girlfriends, boyfriends, mistresses)
- Prominent members of the same political party, civil firm, union
- Business partners or associates
- Any person who has sole ownership or control of an entity or arrangement set up for the sole benefit of the client

The firm will take reasonable measures to establish whether a client or party is an FPPO through client disclosure, general knowledge, internet searches and the DocFox application as appropriate.

FPPOs present an inherently higher ML risk and the firm will apply enhanced due diligence when establishing business relationships with FPPOs, as such, where it is established that a prospective client, a related party, or beneficial owner of the client, is an FPPO or a family member or close associate of such person, the employee must refer to the AML/CTF Compliance Officer to obtain senior management approval before continuing the activity/transaction or relationship. The relationship will be rated high risk, the client's wider source of wealth and source of funds established for each transaction.

5.8 Identification of Domestic Prominent Influential Persons ("DPIP")

A domestic prominent influential person (DPIP) is an individual who holds (including in an acting position) for a period exceeding six months, or has held at any time in the preceding 12 months in South Africa, a function listed in Schedule 3A of the FIC Act. The determination of DPIP applies to the client that is onboarded, the authorised representatives, related parties and beneficial owners of the client.

A person will also be considered to be a DPIP for at least a further 12 months from the date the person ceased to hold that position. Roles identified as DPIPs include:

- The president or deputy president
- A government minister or deputy minister
- The premier of a province
- A member of the Executive Council of a province
- An executive mayor of a municipality elected in terms of the Local Government Municipal Structures Act, 1998
- A leader of a political party registered in terms of the Electoral Commission Act, 1996
- A member of the royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003
- The head, accounting officer or chief financial officer of a national or provincial department or government component as defined in section 1 of the Public Service Act, 1994
- The municipal manager of a municipality appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 or a chief financial officer designated in terms of section 80(2) of the Municipal Finance Management Act, 1999
- The chairperson of the controlling body, the chief executive officer, or a natural person who is the accounting authority, the chief financial officer or the chief investment officer of a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999
- The chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000)
- A constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001
- An ambassador or high commissioner or other senior representative of a foreign government based in the Republic of South Africa
- An officer of the South African National Defence Force above the rank of major-general including general and lieutenant general
- The positions identified below of a firm, as defined in the Companies Act, 2008 if the firm provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceed an amount determined by the Minister of Finance by notice in the Gazette:
 - Chairperson of the board of directors
 - Chairperson of the audit committee
 - Executive officer
 - Chief financial officer
- The position of the head, or other executive directly accountable to that head, of an international firm based in the Republic of South Africa

The firm will take reasonable measures to establish whether a client or a client representative, related party or UBO is a DPIP (or immediate family members and/or known close associates of a DPIP) through client disclosure, using general knowledge, internet searches and the DocFox application (refer Annexure 10.) as appropriate.

Clients that are immediate family members and/or known close associates of DPIPs, although not themselves DPIPs, must be onboarded as though they are.

The following relationships between a natural person and a client will be regarded as an immediate family member relationship:

- Parents
- A spouse, civil partner or a life partner
- A former spouse, civil partner or a life partner
- Children and stepchildren and their spouse, civil partner or a life partner
- Siblings and their spouse, civil partner or a life partner

The following relationships between a natural person and a client will be regarded as a close associate:

- Known partners (for example; girlfriends, boyfriends, mistresses)
- Prominent members of the same political party, civil firm, union
- Business partners or associates
- Any person who has sole ownership or control of an entity or arrangement set up for the sole benefit of the client

DPIPs are not automatically considered as presenting a high ML risk and must be fully assessed to determine the risk and risk rating that a transaction or business relationship with the DPIP poses. Where it is established that a prospective client, a related party, or beneficial owner of the client, is an DPIP or a family member or close associate of such person, the employee must refer to the AML/CTF Compliance Officer to obtain senior management approval before continuing the activity/transaction or relationship. Where, on a risk basis, the transaction or relations is rated higher risk, the client's wider source of wealth identified, and source of funds established for each transaction.

5.9 Source of funds/wealth

The firm will reasonably identify every client's source of funds (and source of wealth where appropriate), and any other relevant information to reasonably determine whether any amount made available for transactions align to the declared source of funds, could realistically have been generated or earned by that particular client, under lawful conditions and make sense in light of the holistic profile or apparent standing of the client.

Where there is any suspicion around the source of funds, it may be prudent to requires additional supporting documentation or refer to the client for further investigation by the AML Compliance Officer.

6. Ongoing Due Diligence

The firm will undertake risk-based ongoing due diligence to identify any information, transactions or activities that are suspicious, unusual or unlawful. Ongoing due diligence will be carried out on a trigger and/or time basis.

Where an employee has identified suspicious or unusual activity, information that cannot be reasonably explained, transactions or activities that have no valid or lawful purpose, or there is reasonable doubt surrounding the veracity of previously supplied identity

information, they will notify the AML/CTF Compliance Officer of this suspicion as soon as possible but within one business day of such a transaction.

Under some risk-based circumstances, including where a client business relationship has longevity and there has been no identified suspicious or unusual activity, the firm may consider making use of the risk-based manual risk adjustment procedure to reduce the resource burden of ongoing due diligence for clients who have provided the firm with a level of comfort around their risk level.

6.1 Trigger based reviews – client information changes

The firm will undertake to perform appropriate due diligence on all clients where a request is made to update or change the particulars or information recorded at the time of onboarding.

The client information triggered due diligence process will include the evidencing/verification of all changes to:

- The client's name
- The client's address
- The client's registration or identity number
- Any person authorised to act on behalf of the client
- Any related party to the client
- Any Ultimate Beneficial Owner of the client
- The client's tax information
- The client's bank account

The changed particulars will be updated in the firm records and the client re-risk assessed where appropriate.

6.2 Trigger based reviews – sanction and restrictive list screening alerts

The firm's clients are loaded into the DocFox application which undertakes overnight screening of clients against various international watchlists and sanctions. Where a client has a potential hit, an automated email will be sent to the AML/CTF Compliance Officer to review the possibility of the alert being a false positive.

A false positive is where an alert indicates a given condition exists when it does not. For example, where an alert is received for a name which either matches or is very similar to the clients but through a process of elimination of additional information (e.g. date of birth, nationality, employment) it has proven beyond a reasonable doubt that the alert does not refer to the client.

Should this alert notification appear to be a true positive hit, then the AML/CTF Compliance Officer will perform a full due diligence review before taking any appropriate actions regarding client termination and reports to the FIC.

6.3 Trigger based reviews – suspicious activity/transaction

The AML/CTF Compliance Officer will undertake to perform enhanced due diligence reviews on all clients where suspicion is raised by an employee. This will include reviewing the client identity and verification documents as well as activities undertaken for at least the preceding 12 months, including, where necessary:

- The background and purpose of all complex or unusual activities or transaction
- The source of funds/wealth
- The recipient of funds

Where any suspicion or concerns exists, the AML/CTF Compliance Officer will undertake such actions as deemed appropriate including but not limited to client termination, risk rating adjustment or report to the FIC.

6.4 Time-based periodic reviews

The firm will undertake to perform periodic reviews on all clients within a risk-based, reasonable period where a review has not taken place elsewhere.

The due diligence review will confirm that information obtained during the client onboarding is still correct and where appropriate, review any activities/transactions for the preceding 12 months for any unusual, unlawful or suspicious activity.

Changes or updates to the following client information will require evidencing/verification:

- The client's name
- The client's address
- The client's registration or identity number
- Any person authorised to act on behalf of the client
- Any related party to the client
- Any Ultimate Beneficial Owner of the client
- The client's tax information
- The client's bank account

The changed particulars will be updated in the firm records and the client re-risk rated where appropriate.

Where a suspicion or concern around the client exists, the employee will notify the AML/CTF Compliance Officer as soon as possible but within one business day.

6.5 Doubts surrounding the veracity of information previously obtained

Where an employee has doubts about information previously obtained from an existing client, they will take reasonable steps to re-identify and verify the client to satisfy themselves as to that information accuracy or otherwise, and such reasonable steps may include (but are not limited to);

- Requesting independently certified documents
- Requesting sighting of original documents

- Requesting confirmation from an independent person
- Requesting evidence of contracts or agreements

Should the inaccuracy of previously obtained information be identified, but (at the sole discretion of the AML/CTF Compliance Officer) not be of such as to give rise to suspicion or concern then the affected information will be updated in the records in line with a client-information based trigger review.

Should the inaccuracy of previously obtained information be identified, and (at the sole discretion of the AML/CTF Compliance Officer) be of such as to give rise to a suspicion or concern then the employee will notify AML/CTF Compliance Officer as soon as possible but within one business day of such a suspicion.

7. Activity Monitoring

Where activities, transactions or services are requested by an existing client, the appropriate employee will briefly consider the current request against existing knowledge of the client gained throughout the course of the business relationship including (but not limited to):

- The source of any funds/wealth, to assess if they are consistent with the firm's knowledge of the client and the client's business and risk profile, and
- The recipient of any funds, to assess if they are consistent with the firm's knowledge of the client and the client's business and risk profile, and
- The background and purpose of complex or unusual activities/transactions or those that have no apparent lawful purpose, and
- The clients access to, and use of funds or assets, to assess if they are as expected and consistent with the firm's knowledge of the client and their business and risk profile, and
- The client's behaviour and tone are as expected, and
- Any information about corruption or evidence that government funds or assets are being used inappropriately where dealing with an FPPO or DPIP.

Discretion is permitted in requesting additional evidence to obtain a level of comfort around any doubts or concerns around the client, their activities or behaviour and the potential risk levels. Employees are guided to contact the AML/CTF Compliance Officer for support and assistance as appropriate.

Where any suspicion or concerns exists, the employee will notify the AML/CTF Compliance Officer of this instruction/transaction as soon as possible but within one business day who will investigate as appropriate and record their findings.

8. Reports to the Financial Intelligence Centre (FIC)

8.1 Cash Threshold Reports ("CTR"/"CTRA")

In line with Section 28, the firm will report a transaction as a cash threshold report ("CTR") to the FIC if an amount of cash that exceeds the prescribed amount of R24,999 is received (or paid) by the firm from (or to) a client, or from (or to) a client representative.

The firm will report a transaction as a cash threshold report aggregate (“CTRA”) to the FIC if a series of cash transactions are carried out separated by a period of not more than 24 hours that appear linked or from the same source exceeds the prescribed amount of R24,999 is received (or paid) by the firm from (or to) a client, or from (or to) a client representative. All such appropriate transactions will be reported in the single CTRA.

For the avoidance of doubt, cash is defined in section 1 of the FIC Act as:

- coin and paper money of the Republic or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue
- travellers’ cheques

Where an employee identifies such cash transactions, they will notify the AML/CTF Compliance Officer of that fact as soon as possible, but at most one business day after such a transaction.

The AML/CTF Compliance Officer will submit a Cash Threshold Report to the FIC as soon as possible but not later than two days. The AML/CTF Compliance Officer will keep a record of all reports submitted to the FIC with a record of all evidence, transactions and activities which gave rise to the report.

The firm is aware of the requirements of “dual reporting” where more than one institution reports the same transaction, but different sides of the transaction (e.g. receipt of cash by an attorney and the payment of that cash to the Bank).

8.2 Suspicious Activities or Transactions (“SAR”/“STR”)

As per Section 29, any person who knows or ought reasonably to have known or suspected that the firm has been used or is about to be used in any way for money laundering purposes or the financing of terrorist activities must report this knowledge or suspicion to the FIC.

This includes, but is not limited to knowledge or suspicion that:

- the business has received or is about to receive the proceeds of
- unlawful activities or property which is connected to an offence
- relating to the financing of terrorist and related activities;
- a transaction or series of transactions to which the business is a party —
 - facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities;
 - has no apparent business or lawful purpose;
 - is conducted for the purpose of avoiding giving rise to a reporting duty under this Act;
 - may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service;

- relates to an offence relating to the financing of terrorist and related activities; or
- relates to the contravention of a prohibition under section 26B; or
- the business has been used or is about to be used in any way for money laundering purposes or to facilitate the commission of an offence relating to the financing of terrorist and related activities.

Where an employee has such knowledge or reasonable suspicion, they will notify the AML/CTF Compliance Officer as soon as possible but within one business day of such a suspicion.

The AML/CTF Compliance Officer will submit a Suspicious or Unusual Activity or Transaction Report to the FIC as soon as possible but not later than fifteen days. The AML/CTF Compliance Officer will keep a record of all reports submitted to the FIC with a record of all evidence, transactions and activities which gave rise to the report.

The firm may, at the discretion of the AML/CTF Compliance Officer continue such transaction unless otherwise instructed by the FIC, supervising body or similar authority.

8.3 Terrorist Related Property, Transactions or Activities

As per Section 28A, the firm acknowledges that it must avoid entering into an activity/transaction or business relationship with persons and entities identified on the UN Security Council Sanctions or Targeted Financial Sanctions (TFS) lists.

The firm will make a report where the firm has identified when has in its possession or under its control, property owned or controlled by or on behalf of, or at the direction of:

- any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004;
- a specific entity identified in a notice issued by the President, under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; or
- a person or an entity identified pursuant to a resolution of the Security Council of the United Nations

The AML/CTF Compliance Officer will seek to create a Terrorist Financing Activity Report ("TFAR"), Terrorist Financing Transaction Report ("TFTR") Terrorist Property Report ("TPR") as appropriate and submit to the FIC as soon as possible but not later than five days.

The AML/CTF Compliance Officer will keep a record of all reports submitted to the FIC with a record of all evidence, transactions and activities which gave rise to the report.

8.4 Remediation of non-submitted reports

In line with FIC PCC50 (mitigation of loss of intelligence), should the firm become aware at any point that it ought to have filed a report the Centre but failed to do so (whether through its own accord, as a result of a supervisory inspection, external audit or through other means) it will seek to mitigate the loss of intelligence data to the Centre.

The FIC Directive 3 (2014) process will be followed when the firm becomes aware of a non-submitted report.

Remediation of a non-submitted report includes, but are not limited to, the submission of all non-submitted reports; and a review and amendment of existing internal systems and/or reporting methodology as detailed in the reporters' RMCP (as appropriate) to ensure that the reporting failure does not re-occur

As prescribed in Directive 3, the firm will notify the Centre, in writing, of the reporting failures relating to the non-submission of a report as soon as the reporter becomes aware thereof. This notification must contain the details regarding the nature and extent of the loss of data and the proposed remediation actions as follows:

- The time period over which the non-submitted report(s) range;
- The extent of the non-submitted report(s), including but not limited to the volume and value of the impacted transactions;
- The root cause(s) of the reporting failure;
- Any factors that may impact the remediation process, including mitigating or aggravating factors;
- Steps that the entity may have already taken to mitigate the current, and re-occurrence of the reporting failures; including a proposed remediation plan indicating time period for successful completion.

Where the reporter does not have all the information as required at the time of notifying the Centre, the reporter is to provide all preliminary information available

Upon completion of the Directive 3 process, the firm will provide the Centre with a formal, written close out report detailing the steps taken to remediate the non-submitted reports and prevent a re-occurrence of the reporting failure. The close out report must include reconciliation reports submitted as part of the corrective action and confirm that all non-submitted reports have been successfully filed.

All Directive 3 related notifications must be sent to the Executive Manager: Compliance and Prevention at Directive3@fic.gov.za.

8.5 Avoiding tipping off

Section 29(3,4) states that no person who made or must make a report in terms of this section, or who knows or suspects that a report has been or is to be made subject to subsection 45B(2A), may disclose that fact or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, otherwise than:

- a) within the scope of the powers and duties of that person in terms of any legislation;
- b) for the purpose of carrying out the provisions of this Act;
- c) for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
- d) in terms of an order of court.

To encourage compliance with this requirement, Tipping Off will be included in employee FICA training and expected to only communicate any relevant knowledge or suspicion with the appointed AML Compliance Officer.

8.6 Confidentiality of personal and reported information

The firm acknowledges that Section 37(1) states that no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by an accountable institution to report with the exception of common law right to legal professional privilege as between an attorney and the attorney's client noted in Section 37(2) in respect of communications made in confidence between:

- a) the attorney and the attorney's client for the purposes of legal advice or litigation which is pending or contemplated or which has commenced; or
- b) a third party and an attorney for the purposes of litigation which is pending or contemplated or has commenced.

8.7 Protection of reporting persons

Section 38(1) confirms that no action, whether criminal or civil, lies against an accountable institution, including any director, employee or other person acting on behalf of such accountable institution when making a report in good faith.

It is noted that Section 38(2) states that any person who has made, initiated or contributed to a report to the Centre or who has furnished additional information concerning such a report or the grounds for such a report is competent, but not compellable, to give evidence in criminal proceedings arising from the report.

As per Section 38(3), no evidence concerning the identity of a person who has made, initiated or contributed to a report to the Centre or who has furnished additional information concerning such a report or the grounds for such a report is admissible as evidence in criminal proceedings unless that person testifies at those proceedings.

8.8 Continuation of transactions

Section 33 confirms that an accountable institution may continue with and carry out a transaction in respect of which the report is required to be made to the Centre, unless the Centre directs the accountable institution, reporting institution or person not to proceed with the transaction.

In such cases, under Section 34, the Centre may direct the accountable institution, reporting institution or person in writing not to proceed with the carrying out of that transaction or proposed transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period not longer than 10 business days

8.9 Responding to requests from the Centre

Under Section 27 and Section 32 of the Act, an authorised representative of the FIC may request an Accountable Institution make a report in terms of section 29, or to advise the Centre with such additional information, including prescribed information relating to transactional activity and supporting documentation, concerning the report and the grounds for any report.

All requests will be passed immediately to the AML Compliance Officer.

In such cases the firm will respond to the Centre through the AML Compliance Officer as soon as possible and within the requested time.

8.10 Monitoring orders

Section 35 allows for a judge, for the purposes of the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992) to order an accountable institution to report to the Centre all transactions concluded by a specified person with the accountable institution, or all transactions conducted in respect of a specified account or facility at the accountable institution, if there are reasonable grounds to suspect that they:

- a) may relate to the financing of terrorist and related activities
- b) may related to proceeds of unlawful activities.

In such cases the firm will respond through the AML Compliance Officer as required and notes that an order in terms of Section 35 lapses after three months unless extended for further periods not exceeding three months at a time by a judge.

9. Recordkeeping

9.1 FIC registration and changes

The AML/CTF Compliance Officer will ensure that the firm keeps a record of its registration with the FIC and GoAML system and any subsequent updates or changes. This record will include evidence of the AML/CTF Compliance Officer appointment.

These records will be kept securely whilst the firm is in operation and FIC GoAML login details will never be shared.

9.2 Due diligence

The AML/CTF Compliance Officer will ensure that the firm keeps a record of all due diligence information and supporting documentation/evidence of clients (including those which were declined, terminated and/or gave rise to a suspicious and unusual transaction report) for at least five years from whichever is the later of:

- The date of last transaction

- The date the client terminated their relationship with the firm
- The date on which a report was submitted to the FIC

These records will be kept securely in physical and/or electronic format in the firm storage systems. The firm can readily access this information upon request by the FIC or an investigating authority acting with the permission of the FIC.

9.3 Transactions

The AML/CTF Compliance Officer will ensure that the firm keeps a record of all transactions (including value, volume, currencies, counterparties, nature of transaction, account numbers and supporting documentation) and activities undertaken on behalf of clients (including those which gave rise to the any report to the FIC) for at least five years from whichever is the later of:

- The date of last transaction
- The date the client terminated their relationship with the firm
- The date on which a report was submitted to the FIC.

These records will include all parties and amounts involved and be kept securely in physical and/or electronic format in the firm storage systems. The firm can readily access this information upon request by the FIC or an investigating authority acting with the permission of the FIC.

9.4 Third-party record keeping

The firm makes use of the DocFox application to verify client information and documentation, undertake daily watchlist screening and perform risk-rating calculations. As part of this, due diligence identification information and supporting documentary evidence is stored within the DocFox application in the 'Cloud'. These are readily accessible to the firm and capable of being reproduced in legible format on demand.

In terms of the FIC Act, Accountable Institutions are required to provide the FIC with the particulars of a third-party keeping records of the accountable institution. These are recorded as follows:

The registered name of the third-party	DocFox Africa (Pty) Ltd K2015/275633/07
The registered address of the third-party	37 Bath Avenue Rosebank Johannesburg Gauteng, 2196
The name under which the third-party conducts business	DocFox Africa
The full name and contact details of the individual who has control over the access of the records	The firm's AML/CTF Compliance Officer
The address where the records are kept	Amazon AWS Data Centre Greenhills Road, Tymon North,

	Dublin, Ireland
The address from where the third-party exercises control over the records	2nd Floor, 37 Bath Avenue, Rosebank Gauteng, 2196
The full name and contact details of the person who liaises with the third-party on behalf of the accountable institution concerning the retention of records.	The firm's AML/CTF Compliance Officer

In line with Section 24, the firm acknowledges that it remains accountable for compliance with the FIC Act at all times and responsible for any failure of a third party in their record keeping duties.

9.5 Reports to the FIC

The AML/CTF Compliance Officer will keep a record of all supporting evidence and reasons that gave rise to a suspicious report submitted to the FIC for at least five years from the date on which the report was submitted.

These records will be kept securely in physical and/or electronic format in the firm storage systems. The firm can readily access this information upon request by the FIC or an investigating authority acting with the permission of the FIC.

9.6 Centre access to records

Section 27A allows for an authorised representative of the Centre to have access to records held by the Firm:

- 1) during normal working hours and may exam, make extracts or copies of records that are public
- 2) by virtue of a warrant granted on reasonable grounds for non-public records

In such cases the firm will comply as required through the assigned AML Compliance Officer.

10. Annexures:

10.1 Senior Management sign-off

Senior Management Sign Off Request

Re: Client Name

As the appointed AML/CTF Compliance Officer, I hereby request approval to:

Onboard with an identified ☐ DPIP ☐ DPIP family member ☐
 DPIP close associate

☐ FPPO ☐ FPPO family member ☐ FPPO close
 associate

High Risk Client ☐ Onboard ☐ Downgrade ☐ Terminate

Identified DPIP/s and/or FPPO/s and relationship to client/transaction:

Details of factors promoting risk:

Adverse Media ☐ No ☐ Yes

Details of adverse media:

On behalf of the firm, I ☐ APPROVE ☐ DECLINE the request.

Comments:

Name: _____

Signed: _____

Date: _____

10.2 DocFox screening lists

(as of August 2020)

Abbreviation	Country	Name/Description
ALASP	ALBANIA	ALASP - Albanian State Police
ONDCP	ANTIGUA & BARBUDA	OFFICE OF NATIONAL DRUG & MONEY LAUNDERING CONTROL POLICY - ONDCP
ACNV	ARGENTINA	ACNV - Argentinean National Securities Commission - Comision Nacional De Valores.
ARAFIP	ARGENTINA	ARAFIP - Federal Administration of Public Revenues
ARINAES	ARGENTINA	ARINAES - National Institute Of Associativism And Social Economy
ARUIF	ARGENTINA	ARUIF - Argentine Financial Information Unit
ASSN	ARGENTINA	ASSN - Superintendence of Insurance of the Nation - Superintendencia De Seguros De La Nacion
ACCC	AUSTRALIA	ACCC - Australian Competition and Consumer Commission
ANS-TERR	AUSTRALIA	ANS-TERR - Australian National Security
APRA	AUSTRALIA	APRA - Australian Prudential Reg. Authority
ASIC	AUSTRALIA	ASIC - Securities and Investments Comm
ASIC-ALERT	AUSTRALIA	ASIC-ALERT - Australian Securities and Investments Commission - Investor Alert
AUASX	AUSTRALIA	AUASX - Australian Securities Exchange
AUS-EMB	AUSTRALIA	AUS-EMB - Implementation of UN and Autonomous Sanctions Country or Region Embargo
AUS-ISEL	AUSTRALIA	AUS-ISEL - Iran Specified Entities List
AUSTRAC	AUSTRALIA	AUSTRAC - Australian Transaction Reports and Analysis Centre
DFAT-AS	AUSTRALIA	DEPT FOREIGN AFFAIRS & TRADE - AUTONOMOUS SANCTIONS - DFAT-AS
DFAT-ASTB	AUSTRALIA	DEPT FOREIGN AFFAIRS & TRADE - AUTONOMOUS SANCTIONS TRAVEL BANS - DFAT-ASTB
DFAT	AUSTRALIA	DEPT FOREIGN AFFAIRS & TRADE - DFAT
DFAT-TB	AUSTRALIA	DEPT FOREIGN AFFAIRS & TRADE - ENTRIES ONLY SUBJECT TO A TRAVEL BAN - DFAT-TB
DFAT-UN	AUSTRALIA	DEPT OF FOREIGN AFFAIRS & TRADE - UNSC FINANCIAL SANCTIONS - DFAT-UN
DFAT-UNTB	AUSTRALIA	DEPT OF FOREIGN AFFAIRS AND TRADE - SUBJECT TO UNSC TRAVEL BAN - DFAT-UNTB
DFAT-ASFRR	AUSTRALIA	DFAT-ASFRR - Dept Foreign Affairs - Financial Restrictions Russia
ICACAUS	AUSTRALIA	IND. COMM. AGAINST CORRUPTION - ICACAUS
ACB	AUSTRIA	ACB - Oesterreichische National Bank - Terrorism List
ACB-SANC	AUSTRIA	ACB-SANC - Oesterreichische National Bank - Sanction Lists
FMA	AUSTRIA	FMA - Financial Market Authority
AZFMS	AZERBAIJAN	AZFMS - Financial Monitoring Service - Sanctions Notices
AZHTL	AZERBAIJAN	AZHTL - Azerbaijan Human Trafficking List
AZMOT	AZERBAIJAN	AZMOT - Ministry of Taxes Azerbaijan
BSSCB	BAHAMAS	BSSCB - Bahamas Securities Commission
CBBW	BAHAMAS	CENTRAL BANK WARNING NOTICES - CBBW
BHTOL	BAHRAIN	BHTOL - Bahrain Terrorist Firms List
BDACC	BANGLADESH	BDACC - Bangladesh Anti Corruption Commission
BDBB-SANC	BANGLADESH	BDBB-SANC - Bangladesh Bank Domestic Sanctions
BDDNC	BANGLADESH	BDDNC - Bangladesh Department of Narcotics Control
BDSEC	BANGLADESH	BDSEC - Bangladesh Securities Exchange Commission
BYMNS	BELARUS	BYMNS - Belarus Ministry of Taxes and Duties
BEFOJ	BELGIUM	BEFOJ - Belgium Federal Public Service Justice Terrorism List
CBF	BELGIUM	CBF- Financial Services and Markets Authority - FSMA (formerly CBF).
BZFSC	BELIZE	BZFSC - Financial Services Commission - Advisory Notices
BZCB	BELIZE	CENTRAL BANK OF BELIZE - WARNING NOTICES - BZCB
BMA	BERMUDA	BMA - Bermuda Monetary Authority

BACBH	BOSNIA AND HERZEGOVINA	BACBH - Court of Bosnia and Herzegovina
BAPO	BOSNIA AND HERZEGOVINA	BAPO - Prosecutor's Office of Bosnia and Herzegovina
BRBCB	BRAZIL	BRBCB - Brazil Central Bank
BRCADE	BRAZIL	BRCADE - Brazil Competition Authority
BRCEIS	BRAZIL	BRCEIS - National Registry of Ineligible and Suspended Companies
BRCOAF	BRAZIL	BRCOAF - Council for Financial Activities Control
BRIRAC	BRAZIL	BRIRAC - Brazilian Integrated Registry of Administrative Convictions
BRMTE	BRAZIL	BRMTE - Department of Labour Inspection - Combating Forced Labour
CVM	BRAZIL	CVM - Securities and Exchange Commission
DENARC	BRAZIL	DPO DE INVESTIGACOES SOBRE NARC. - DENARC
BGCPC	BULGARIA	BGCPC - Commission for Protection of Competition
BGFSC	BULGARIA	BGFSC - Bulgaria Financial Supervision Commission
BDRQ	CANADA	BDRQ - Bureau de Decision et de Revision Quebec
CAALERT	CANADA	CAALERT - Alberta Law Enforcement Response Teams
CAAMF	CANADA	CAAMF - Autorite Des Marches Financiers
CAASC	CANADA	CAASC - Alberta Securities Commission
CACBSA	CANADA	CACBSA - Canada Border Services Agency
CACCB	CANADA	CACCB - Canada Competition Bureau
CACRA	CANADA	CACRA - Canada Revenue Agency
CADA	CANADA	CADA - Canadian Institute of Chartered Accountants - Disciplined Accountants
CADL	CANADA	CADL - Canadian Law Society - Disciplined Lawyers
CAEC	CANADA	CAEC - Environment Canada
CAFCAA	CANADA	CAFCAA - Saskatchewan Financial and Consumer Affairs Authority
CAFCNB	CANADA	CAFCNB - Financial Consumer Services Commission New Brunswick
CAFIC	CANADA	CAFIC - Financial Institutions Commission of British Columbia
CALPS	CANADA	CALPS - London Canada Police Service
CAMFDA	CANADA	CAMFDA - Mutual Fund Dealers Association of Canada
CAMSC	CANADA	CAMSC - Manitoba Securities Commission
CES	CANADA	CANADIAN ECONOMIC SANCTIONS - CES
CANS	CANADA	CANADIAN SANCTIONS - CANS
CSA-CTO	CANADA	CANADIAN SEC. ADMIN. - CEASE TRADE ORDERS - CSA-CTO
CSA-ALERT	CANADA	CANADIAN SECURITIES ADMINISTRATORS - ALERTS - CSA-ALERT
CAN-AN	CANADA	CAN-AN - Advisory Notices.
CANBSC	CANADA	CANBSC - New Brunswick Securities Commission.
CANEMBARGO	CANADA	CANEMBARGO - Country or Region Embargo List.
CANSEMSS	CANADA	CANSEMSS - Special Economic Measures - South Sudan.
CAOSC	CANADA	CAOSC - Ontario Securities Commission
CARENA	CANADA	CARENA - Quebec Enterprises Ineligible for Public Contracts
CARQ	CANADA	CARQ - Quebec Ministry of Revenue
CASFSC	CANADA	CASFSC - Saskatchewan Financial Services commission
CASQ	CANADA	CASQ - Surete Du Quebec
CATMF	CANADA	CATMF - Quebec Administrative Tribunal of Financial Markets
CAUPAC	CANADA	CAUPAC - Quebec Permanent Anti-Corruption Unit.
CFSEU	CANADA	CFSEU - Special Enforcement Units
CCC	CANADA	CRIMINAL CODE - TERRORISM DESIGNATIONS - CCC
CSA-DP	CANADA	CSA-DP - Canadian Securities Administrators - Disciplined Parties
CAFSCO	CANADA	FINANCIAL SERVICES COMMISSION OF ONTARIO - CAFSCO
FINTRAC	CANADA	FINANCIAL TRANSACTIONS REPORTS ANALYSIS CENTRE - FINTRAC
CANFACFO	CANADA	FREEZING ASSETS OF CORRUPT FOREIGN OFFICIALS - CANFACFO
IIROC	CANADA	IIROC - Investment Industry Reg. Firm of Canada
NSSC	CANADA	NSSC - Nova Scotia Securities Commission
OSFI	CANADA	OSFI - Bank Warning Notices
TPS	CANADA	POLICE SERVICE, TORONTO - TPS
PRPS	CANADA	PRPS - Reg. Police Service, Peel.
QCSF	CANADA	QCSF - Quebec Chambre De La Securite Financiere
RCMP	CANADA	RCMP
YRPS	CANADA	REG. POLICE SERVICE, YORK - YRPS
SECBC	CANADA	SECBC - British Columbia Securities Comm.
CANSEMB	CANADA	SPECIAL ECONOMIC MEASURES - BURMA (MYANMAR) - CANSEMB

CANSEMIR	CANADA	SPECIAL ECONOMIC MEASURES - IRAN - CANSEMIR
CANSEMRUS	CANADA	SPECIAL ECONOMIC MEASURES - RUSSIA - CANSEMRUS
CANSEMSYR	CANADA	SPECIAL ECONOMIC MEASURES - SYRIA - CANSEMSYR
CANSEMUJR	CANADA	SPECIAL ECONOMIC MEASURES - UKRAINE - CANSEMUJR
CANSEMZ	CANADA	SPECIAL ECONOMIC MEASURES - ZIMBABWE - CANSEMZ
CANSEMRUS-FSR	CANADA	SPECIAL ECONOMIC MEASURES (RUSSIA-Schedules 2&3) FINANCIAL SERVICES RESTRICTIONS - CANSEMRUS-FSR
UNSTR	CANADA	UN SANCTIONS TERRORISM - UNSTR
CIMA	CAYMAN ISLANDS	MONETARY AUTH. - CIMA
CLSBIF	CHILE	CLSBIF - Chilean Superintendency of Banks and Financial Institutions
CLUAF	CHILE	CLUAF - Chilean Financial Analysis Unit
SVS	CHILE	SVS - Chilean Securities and Insurance Supervisor
CIRC	CHINA	CIRC - China Insurance Regulatory Commission.
CNCCDI	CHINA	CNCCDI - Central Commission for Discipline Inspection
CNCCDI-WANTED	CHINA	CNCCDI-WANTED - Central Commission for Discipline Inspection - Most Wanted
CNSAT	CHINA	CNSAT - China State Administration of Taxation
CNSSE	CHINA	CNSSE - SHANGHAI STOCK EXCHANGE
CSRC	CHINA	CSRC - China Securities Regulatory Commission.
CSRC-ALERT	CHINA	CSRC-ALERT - China Securities Regulatory Commission - Alert
PBC-ETIM	CHINA	PBC-ETIM - People's Bank of China - Eastern Turkistan Islamic Movement
PBC	CHINA	PEOPLE'S BANK OF CHINA - UNITED NATIONS SANCTIONS - PBC
AMVC	COLOMBIA	AMVC - Autorregulador del Mercado de Valores
BVC	COLOMBIA	BVC - Bolsa De Valores De Colombia
CDNE	COLOMBIA	CDNE - Colombian National Narcotics Directorate
COANLA	COLOMBIA	COANLA - National Authority of Environmental Licenses
COCGR	COLOMBIA	COCGR - Comptroller Generals Office of Colombia
COPGO	COLOMBIA	COPGO - Prosecutor Generals Office of Colombia
COPOL	COLOMBIA	COPOL - Colombian National Police
COSFC	COLOMBIA	COSFC - Financial Superintendence of Colombia
COSIC	COLOMBIA	COSIC - Superintendence of Industry and Commerce
CRSGV	COSTA RICA	CRSGV - General Superintendence of Securities of Costa Rica
CIPLCC	COTE D'IVOIRE	CIPLCC - Ivory Coast Platform Combating Cyber Criminality
BNA	CURACAO	BNA - Central Bank of Curacao and Sint Maarten -Bank Warning Notices
CSEC	CYPRUS	CSEC - Cyprus Securities & Exchange Commission.
CZUOHS	CZECH	CZUOHS - Czech Office for the Protection of Competition
CSC	CZECH	SECURITIES COMM. - CSC
CZCNB	CZECH REPUBLIC	CZECH NATIONAL BANK - CONSUMER PROTECTION - CZCNB
DKFSA	DENMARK	FINANCIAL SUPERVISORY AUTHORITY - DKFSA
MFDOMINICA	DOMINICA	MIN OF FINANCE - MFDOMINICA
ECSBS	ECUADOR	ECSBS - Superintendence of Banks of Ecuador
ECSCVS	ECUADOR	ECSCVS - Superintendence of Companies Securities and Insurance
EGYE-AF	EGYPT	EGYPTIAN EXCHANGE - ASSET FREEZE - EGYE-AF
EEFI	ESTONIA	EEFI - Estonian Financial Supervision Authority
EU-AN	EU	ADVISORY NOTICE - EU-AN
EU-AQ	EU	ASSET FREEZE AND TRAVEL BAN - AL-QAIDA - 2002/402/CFSP, EC 881/2002 - EU-AQ
EU-GNB	EU	ASSET FREEZE AND TRAVEL BAN - REP. OF GUINEA-BISSAU - 2012/237/CFSP, EU 377/2012 - EU-GNB
EU-TA	EU	ASSET FREEZE AND TRAVEL BAN - TALIBAN - 2011/486/CFSP EU 753/2011 - EU-TA
EU-UKR2	EU	ASSET FREEZE AND TRAVEL BAN - UKRAINE - 2014/145/CFSP, EU 269/2014 - EU-UKR2
EU-BLR	EU	ASSET FREEZE BELARUS - 2006/362/CFSP, EC 765/2006 - EU-BLR
EU-CI	EU	ASSET FREEZE COTE D'IVOIRE - 2004/852/CFSP, EC 560/2005 - EU-CI
EU-DRC	EU	ASSET FREEZE D.R. CONGO - 2005/440/CFSP, EC 889/2005 - EU-DRC
EU-DPRK	EU	ASSET FREEZE DEM. PEOPLE'S REP. OF KOREA - EC 329/2007 - EU-DPRK
EU-EGY	EU	ASSET FREEZE EGYPT - 2011/172/CFSP, EU 270/2011 - EU-EGY
EU-ICTY	EU	ASSET FREEZE ICTY - 2004/694/CFSP, EC 1763/2004 - EU-ICTY
EU-IRN	EU	ASSET FREEZE IRAN - 2007/140/CFSP, EC 423/2007 - EU-IRN
EU-IRQ	EU	ASSET FREEZE IRAQ - 2003/495 CFSP, EC 1210/2003 - EU-IRQ
EU-LIB	EU	ASSET FREEZE LIBERIA - 2004/487/CFSP, EC 872/2004 - EU-LIB
EU-LBY	EU	ASSET FREEZE LIBYA - 2011/137/CFSP, EU 204/2011 - EU-LBY
EU-GN	EU	ASSET FREEZE REPUBLIC GUINEA - 2009/788/CFSP, EU1284/2009 - EU-GN

EU-S	EU	ASSET FREEZE SUDAN - 2005/411/CFSP, EC 1184/2005 - EU-S
EU-ZIM	EU	ASSET FREEZE ZIMBABWE - 2002/145/CFSP, EC 314/2004 - EU-ZIM
EUAC	EU	BAN ON AIRLINES - EUAC
EU-BDI	EU	EU-BDI - Asset Freeze and Travel Ban Burundi - Burundi
EU-CAR	EU	EU-CAR - Asset Freeze - Central African Republic - 2013/798/CFSP, 224/2014
EUEMBARGO	EU	EUEMBARGO - Country or region Embargo.
EU-FRYSM	EU	EU-FRYSM - Asset Freeze FRYSM - 2000/696/CFSP.
EU-HRTC	EU	EU-HRTC - High Risk Third Countries - Regulation (EU) 2016/1675
EUMW	EU	EUMW - Europe's Most Wanted
EUMY-LTM	EU	EUMY-LTM - Myanmar Logging, Timber & Mining Enterprises.
ECC	EU	EUROPEAN COMMISSION - COMPETITIONS - ECC
EU-SYR	EU	EUROPEAN UNION - ASSET FREEZE AND TRAVEL BAN SYRIA - 2011/273/CFSP, EU 442/2011, EU 36/2012 - EU-SYR
EU-SS	EU	EUROPEAN UNION - ASSET FREEZE SOUTH SUDAN - SOUTH SUDAN - EU-SS
EU-TUN	EU	EUROPEAN UNION - ASSET FREEZE TUNISIA - 2011/72/CFSP - EU-TUN
EUFSR-RUS	EU	EUROPEAN UNION - FINANCIAL SERVICES RESTRICTIONS ART 2 and 5 - EU 833/2014 - EUFSR-RUS
EUFSR-SYR	EU	EUROPEAN UNION - FINANCIAL SERVICES RESTRICTIONS Art 24/25 - EU 36/2012 - EUFSR-SYR
EUTB-LBY	EU	EUROPEAN UNION - TRAVEL BAN LIBYA - 2011/137/CFSP - EUTB-LBY
EU	EU	EUROPEAN UNION SANCTIONS - EU
EUTB-FRYSM	EU	EUTB-FRYSM - Travel Ban FRYSM - 2000/696/CFSP, EC 2488/2000
EU-UKR	EU	EU-UKR - Asset Freeze - Ukraine - 2014/119/CFSP, 208/2014
EU-YEM	EU	EU-YEM -Yemen - Asset Freeze and Travel Ban 2014/932/CFSP, 1352/2014
EU-MY	EU	FIN. RESTRICTIONS MYANMAR - 2004/423/CFSP, EC 817/2006 - EU-MY
EU-TAF	EU	TERROR ASSET FREEZE - 2001/931/CFSP, EC 2580/2001 - EU-TAF
EU-TCO	EU	TERROR CO-OPERATION - 2001/931/CFSP - EU-TCO
EUTB	EU	TRAVEL BAN - EUTB
EUTB-BLR	EU	TRAVEL BAN BELARUS - 2006/276/CFSP, EC 765/ 2006 - EUTB-BLR
EUTB-CI	EU	TRAVEL BAN COTE D'IVOIRE - 2004/852/CFSP - EUTB-CI
EUTB-FYROM	EU	TRAVEL BAN FYROM - 2004/133/CFSP - EUTB-FYROM
EUTB-ICTY	EU	TRAVEL BAN ICTY 2004/293/CFSP - EUTB-ICTY
EUTB-MD	EU	TRAVEL BAN MOLDOVA - 2004/179/CFSP - EUTB-MD
EUTB-MY	EU	TRAVEL BAN MYAMAR - 2004/423/CFSP, EC 817/2006 - EUTB-MY
EUTB-GN	EU	TRAVEL BAN REPUBLIC OF GUINEA - 2009/788/CFSP - EUTB-GN
EUTB-ZIM	EU	TRAVEL BAN ZIMBABWE - 2002/145/CFSP, EC 314/2004 - EUTB-ZIM
EU-SOM	EU	EUROPEAN UNION - ASSET FREEZE SOMALIA - 2009/138/CFSP, EU 356/2010 - EU-SOM
FIFSA	FINLAND	FINANCIAL SUPERVISORY AUTHORITY - FIFSA
FRAMF	FRANCE	AUTORITE DES MARCHES FINANCIERS - FRAMF
FRAC	FRANCE	FRAC - Autorite De La Concurrence
FRACPR	FRANCE	FRACPR - French Prudential Supervisory Authority
MINEFI	FRANCE	MIN. OF FINANCE - MINEFI
MINEFI-NAT	FRANCE	MINEFI-NAT -Ministry of Finance National Terrorism List
MINEFI-MN	FRANCE	MINISTRY OF FINANCE MESURES NATIONALES - MINEFI-MN
GEISG	GEORGIA	INVESTIGATION SERVICE GEORGIA - GEISG
GETCC	GEORGIA	TBILISI CITY COURT - GETCC
BAFIN	GERMANY	BAFIN
DBB	GERMANY	DBB - Deutsche Bundesbank Sanctions List
DEBKA	GERMANY	DEBKA - German Federal Cartel Office
GIBFSC	GIBRALTAR	FIN. SERVICES COMM. - GIBFSC
GRHCMC	GREECE	GRHCMC - Hellenic Capital Markets Commission
HCC	GREECE	HELLENIC COMPETITION COMMISSION - HCC
GFSC	GUERNSEY	GFSC - Financial Services Commission.
HKGZ	HONG KONG	GAZETTED SANCTIONS LIST - HKGAZ
HKEX	HONG KONG	HKEX - Hong Kong Stock Exchange
HKFSC-ALERT	HONG KONG	HKFSC-ALERT - H K Sec. and Futures Comm.- Investor Alert.
HKMA	HONG KONG	HKMA- Hong Kong Monetary Authority.
HKMAW	HONG KONG	HKMA WARNING - HKMAW
HKMA-AN	HONG KONG	HONG KONG MONETARY AUTHORITY ADVISORY NOTICE - HKMA-AN
ICACHK	HONG KONG	IND. COMM. AGAINST CORRUPTION - ICACHK
HKSFC	HONG KONG	SEC. & FUTURES COMM. - HKSFC

HUFSA	HUNGARY	FINANCIAL SUPERVISORY AUTHORITY - WARNING NOTICES - HUFSA
GVH	HUNGARY	GVH - Hungarian Competition Authority - Gazdasági Versenyhivatal
HUPOL	HUNGARY	HUPOL - Hungarian Police Wanted
HUMNB	HUNGARY	NATIONAL BANK OF HUNGARY - HUMNB
CBII	INDIA	CENTRAL BUREAU OF INVESTIGATION - CBII
INCCI	INDIA	COMPETITION COMMISSION OF INDIA - INCCI
INNIA	INDIA	INDIAN NATIONAL INVESTIGATION AGENCY - INNIA
INIRDAI	INDIA	INIRDAI - Insurance Regulatory and Development Authority of India
INMCA-DD	INDIA	INMCA-DD - India Ministry of Corporate Affairs - Disqualified Directors
INMCA-MLM	INDIA	INMCA-MLM - India Ministry of Corporate Affairs - Multi-Level Marketing
INMCAVC	INDIA	INMCAVC - India Ministry Of Corporate Affairs - Vanishing Companies
INNCB	INDIA	INNCB - India Narcotics Control Bureau
INTDL	INDIA	INTDL - India Tax Defaulters List
INWCCB	INDIA	INWCCB - India Wildlife Crime Control Bureau
IMHA-BTO	INDIA	MINISTRY OF HOME AFFAIRS - BANNED TERRORIST FIRMS - IMHA-BTO
RBI	INDIA	RESERVE BANK OF INDIA - RBI
RBI-SANC	INDIA	RESERVE BANK OF INDIA - SANCTIONS NOTICES - RBI-SANC
RBI-NBFC	INDIA	RESERVE BANK OF INDIA VANISHING NON-BANKING FINANCIAL COMPANIES - RBI-NBFC
SEBI	INDIA	SECURITIES & EXCHANGE BOARD - SEBI
BAPEPAM	INDONESIA	BAPEPAM - Capital Markets & Fin. Institutions Supervisory Agency
IDOJK	INDONESIA	IDOJK - Indonesian Financial Services Authority
IQCBI-EH	IRAQ	IQCBI-EH - Central Bank of Iraq - Exchange Houses
CBI	IRELAND	CENTRAL BANK - CBI
IFSRA	IRELAND	IFSRA - Financial Services Reg. Authority
IEODCE	IRELAND	OFFICE OF THE DIRECTOR OF CORPORATE ENFORCEMENT - IEODCE
IEREV	IRELAND	RECEIVER OF REVENUE - IEREV
IAA	ISRAEL	ANTITRUST AUTHORITY - IAA
ILITA	ISRAEL	ILITA - Israel Tax Authority
ILITA-C	ISRAEL	ILITA-C - Israel Tax Authority - Customs
IMOD	ISRAEL	ISRAEL MINISTRY OF DEFENCE - TERRORISM LIST - IMOD
IMOF	ISRAEL	ISRAEL MINISTRY OF FINANCE - IMOF
IMOJ-GL	ISRAEL	ISRAEL MINISTRY OF JUSTICE - GAMBLING LIST - IMOJ-GL
AGCM	ITALY	AGCM - Autorita Garante Della Concorrenza E Del Mercato
CONSOB	ITALY	CONSOB - National Comm. Borsa
ITBDI	ITALY	ITBDI - Central Bank of Italy
JMFSC	JAMAICA	FINANCIAL SERVICES COMMISSION - JMFSC
JP-ASF	JAPAN	JAPAN ANTI SOCIAL FORCES - JP-ASF
JFSA	JAPAN	JAPAN FINANCIAL SERVICES AGENCY - JFSA
JFIO	JAPAN	JFIO - Financial Intelligence Office.
JPSIA	JAPAN	JPSIA - Public Security Intelligence Agency
JMETI-WMD	JAPAN	MINISTRY OF ECONOMY, TRADE & INDUSTRY - JMETI-WMD
JMOF	JAPAN	MINISTRY OF FINANCE - INTERNATIONAL SANCTIONS - JMOF
JNPA-DB	JAPAN	NATIONAL POLICE AGENCY - DESIGNATED BORYOKUDAN - JNPA-DB
JFSC	JERSEY	JFSC - Financial Services Comm.
JERSANC	JERSEY	STATES OF JERSEY - SANCTIONS ORDERS - JERSANC
KZAFN	KAZAKHSTAN	KZAFN - National Bank Financial Market and Organization Control and Supervision.
KZFINPOL	KAZAKHSTAN	KZFINPOL - Kazakhstan Financial Police
KZKFM	KAZAKHSTAN	KZKFM - Kazakhstan Financial Monitoring Committee
KZKGD	KAZAKHSTAN	KZKGD - State Revenue Committee of The Ministry of Finance
KEEACC	KENYA	ETHICS AND ANTI CORRUPTION COMMISSION - KEEACC
KEODPP	KENYA	KEODPP - Kenyan Director of Public Prosecutions
KESEL	KENYA	KESEL - Kenyan Specified Entity List
KOFIU	KOREA, SOUTH	KOFIU - Financial Intelligence Unit.
KRFTC	KOREA, SOUTH	KOREA FAIR TRADE COMMISSION - KRFTC
KRMSF	KOREA, SOUTH	KRMSF - Ministry of Strategy and Finance - Sanctions
KGFINPOL	KYRGYZSTAN	KGFINPOL - Kyrgyzstan Financial Police
KGFIU	KYRGYZSTAN	KGFIU - Kyrgyzstan Financial Intelligence Service
LVFCMC	LATVIA	FINANCIAL AND CAPITAL MARKET COMMISSION - LVFCMC
LVCC	LATVIA	LVCC - Competition Council of Latvia

LYNTC	LIBYA	LYNTC - Libyan National Transitional Council Law 36
LGB	LIECHTENSTEIN	LANDESGESETZBLATT - LGB
LTLCB	LITHUANIA	CENTRAL BANK OF LITHUANIA - WARNING NOTICES - LTLCB
LTCC	LITHUANIA	COMPETITION COUNCIL OF LITHUANIA - LTCC
CSSF	LUXEMBOURG	CSSF - Comm. De Surv. Du Secteur Financier.
CSSFW	LUXEMBOURG	CSSFW - Commission De Surveillance Du Secteur Financier - Warning Notices
BNM	MALAYSIA	BNM - Bank Negara Malaysia
BNM-SANC	MALAYSIA	BNM-SANC - Bank Negara Malaysia Sanctions Order
MSC	MALAYSIA	MSC - Securities Commission
MYAGC-SANC	MALAYSIA	MYAGC-SANC - Malaysian Attorney Generals Chambers Sanctions Order
MYBURSA	MALAYSIA	MYBURSA - Bursa Malaysia Berhad
MYMACC	MALAYSIA	MYMACC
MLFIAU	MALTA	MALTA FINANCIAL INTELLIGENCE ANALYSIS UNIT - MLFIAU
MFSA	MALTA	MFSA - Financial Services Authority
MLMGA	MALTA	MLMGA - Malta Gaming Authority
MFSANC	MALTA	SANCTIONS LIST - MFSANC
MUFSC	MAURITIUS	MUFSC - Mauritius Financial Services Commission
MUICAC	MAURITIUS	MUICAC - Mauritius Independent Commission Against Corruption
BANXICO	MEXICO	BANXICO - Central Bank of Mexico
CNBV	MEXICO	CNBV - Mexican National Banking Securities Commission
CONDUSEF	MEXICO	CONDUSEF - Comision Nacional Para La Proteccion Y Defensa De Los Usuarios De Servicios Financieros
MXSFP	MEXICO	MEXICAN PUBLIC FUNCTION SECRETARIAT- MXSFP
MXCNSF	MEXICO	MXCNSF - Mexican Insurance and Surety National Commission
MXPGR	MEXICO	MXPGR - Mexican Prosecutors General Offices
MXSAT	MEXICO	MXSAT - Mexican Tax Administration Service
MDMAI	MOLDOVA	MDMAI - Ministry of Internal Affairs of Moldova
SICCFIN	MONACO	MIN. OF STATE - FIN. INFORMATION & CONTROL SERVICE - SICCFIN
NAACC	NAMIBIA	NAACC - Anti-Corruption Commission of Namibia
NPNCB	NEPAL	NPNCB - Nepal Narcotics Control Bureau
AFM	NETHERLANDS	AFM - Autoriteit Financiële Markten
NNTS	NETHERLANDS	NETHERLANDS NATIONAL TERRORISM SANCTIONS - NNTS
NZCO	NEW ZEALAND	COMPANIES OFFICE - NZCO
NZMCA	NEW ZEALAND	MIN. OF CONSUMER AFFAIRS - NZMCA
NZ-MFAT	NEW ZEALAND	MINISTRY FOREIGN AFFAIRS & TRADE - UNSC SANCTIONS - NZ-MFAT
NZCOMC	NEW ZEALAND	NEW ZEALAND COMMERCE COMMISSION - NZCOMC
NZPOL	NEW ZEALAND	POLICE DESIGNATED TERRORISTS - NZPOL
RBNZ	NEW ZEALAND	RBNZ - Reserve Bank.
SECNZ	NEW ZEALAND	SECNZ - Sec. & Exchange Comm.
SFONZ	NEW ZEALAND	SERIOUS FRAUD OFFICE - SFONZ
NZPOL-TSA	NEW ZEALAND	TSA DESIGNATED TERRORIST - NZPOL-TSA
NISIB	NICARAGUA	NICARAGUA SUPERINTENDENCE OF BANKS - NISIB
NDLEA	NIGERIA	NDLEA - NATIONAL DRUG LAW ENFORCEMENT AGENCY
NGICPC	NIGERIA	NGICPC - Independent Corrupt Practices Commission
NGSEC	NIGERIA	NGSEC - Nigerian Securities and Exchange Commission
NGEFCC	NIGERIA	NIGERIAN ECONOMIC AND FINANCIAL CRIMES COMMISSION - NGEFCC
NOFSA	NORWAY	FINANCIAL SUPERVISORY AUTHORITY - WARNING NOTICES - NOFSA
NAB	PAKISTAN	NAT. ACCOUNTABILITY BUREAU - NAB
PKFIA	PAKISTAN	PAKISTAN FEDERAL INVESTIGATION AGENCY - PKFIA
PKANF	PAKISTAN	PKANF - Pakistan Anti Narcotics Force
PKATAAL	PAKISTAN	PKATAAL - Pakistan Anti Terrorism Act Activists List
PKSEC	PAKISTAN	PKSEC - Securities and Exchange Commission of Pakistan
CONAV	PANAMA	CONAV - National Securities Commission - Comision Nacional De Valores
SBP	PANAMA	SUPERINTENDENCY OF BANKS OF PANAMA - SUPERINTENDENCIA DE BANCOS DE PANAMA - SBP
PYCNV	PARAGUAY	NATIONAL SECURITIES COMMISSION OF PARAGUAY - PYCNV
PESBS	PERU	PESBS - Superintendence of Banks, Insurance and Private Pension Funds
PESMV	PERU	PESMV - Peru Securities Market Superintendency
PHBSP	PHILIPPINES	CENTRAL BANK OF THE PHILIPPINES - PHBSP
PHOMB	PHILIPPINES	OFFICE OF THE OMBUDSMAN - PHOMB
PHSEC	PHILIPPINES	SECURITIES AND EXCHANGE COMMISSION - PHSEC

PLFSA	POLAND	PLFSA - Polish Financial Supervision Authority
PLUOKIK	POLAND	PLUOKIK - Polish Office of Competition and Consumer Protection
PTCB	PORTUGAL	CENTRAL BANK OF PORTUGAL - PTCB
PTADC	PORTUGAL	PTADC - Portugal Competition Authority
PTCMVM	PORTUGAL	PTCMVM - Comissao Do Mercado De Valores Mobiliarios
ADB	ADB	Asian Development Bank
AFDB	AFDB	African Development Bank - Debarred Entities
ECVES	ECVES	Embargoed Country or Region Maritime Vessel
EBRD	EU	EUROPEAN BANK FOR RECONSTRUCTION AND DEVELOPMENT - EBRD
FATF	FATF	Financial Action Task Force.
IDB	INTE	AMERICAN DEVELOPMENT BANK - IDB
BSICIJ-WC	INTERNATIONAL	BSICIJ-WC - International Consortium of Investigative Journalist Bahamas Corporates - World-Check Data
FIRSE-WC	INTERNATIONAL	FIRSE-WC - Former Iran Sanctioned Entity World Check Data
INSAE-WC	INTERNATIONAL	INSAE-WC - International Sanctions Relevant Entity World Check Data
IRAN-WC	INTERNATIONAL	IRAN-WC - Iran - Relevant World-Check Data
ISIS-WC	INTERNATIONAL	ISIS-WC - Islamic State - Relevant World-Check Data
PAICIJ-WC	INTERNATIONAL	PAICIJ-WC - International Consortium of Investigative Journalists - World-Check Data
RSSRE-WC	INTERNATIONAL	RSSRE-WC - Russian Sectoral Sanctions Relevant Entity World-Check Data
INTERPOL	INTERNATIONAL	InterPol List
WORLD BANK	INTERNATIONAL	World Bank List
ROANI	ROMANIA	ROANI - Romanian National Integrity Agency
ROASF	ROMANIA	ROASF - Romanian Financial Supervision Authority
RODIICOT	ROMANIA	RODIICOT - Romanian Organised Crime & Terrorism Investigation Directorate
RODNA	ROMANIA	RODNA - Romanian National Anti-corruption Directorate
ROIGPR	ROMANIA	ROIGPR - General Inspectorate of Romanian Police
ROPGO	ROMANIA	ROPGO - Romanian Prosecutor General Office
RCC	ROMANI	ROMANIAN COMPETITIONS COUNCIL-RCC
RUCBR	RUSSIAN FEDERATION	CENTRAL BANK OF RUSSIAN FEDERATION - RUCBR
FASRF	RUSSIAN FEDERATION	FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION - FASRF
FFMS	RUSSIAN FEDERATION	FFMS - Federal Financial Monitoring Service
RUPGO	RUSSIAN FEDERATION	RUPGO - Prosecutor Generals Office Russian Federation
RUSCRF	RUSSIAN FEDERATION	RUSCRF - Russian Federal Investigative Committee
RUFDCS	RUSSIAN FEDERATION	RUSSIAN FEDERAL DRUG CONTROL SERVICE - RUFDCS
RUFSIN	RUSSIAN FEDERATION	RUSSIAN FEDERAL PENAL SERVICE - RUFSIN
RUMVD	RUSSIAN FEDERATION	RUSSIAN MINISTRY OF INTERNAL AFFAIRS - RUMVD
RWPPA	RWANDA	RWANDAN PUBLIC PROCUREMENT AUTHORITY - RWPPA
RWNP	RWANDA	RWNP - Rwanda National Police
SAMOI	SAUDI ARABIA	SAUDI MINISTRY OF INTERIOR MOST WANTED - SAMOI
RSBAC	SERBIA	BELGRADE APPELLATE COURT - RSBAC
RSVSB	SERBIA	RSVSB - High Court of Serbia
SYFSA	SEYCHELLES	FINANCIAL SERVICES AUTHORITY SEYCHELLES - SYFSA
SYSIBA	SEYCHELLES	SEYCHELLES INTERNATIONAL BUSINESS AUTHORITY - SYSIBA
CADSG	SINGAPORE	CADSG - Commercial Affairs Dept. Prosecutions.
MAS	SINGAPORE	MAS - Monetary Authority Sanctions Lists
MAS-AN	SINGAPORE	MAS-AN - Monetary Authority - Advisory Notices.
MASE	SINGAPORE	MASE - Monetary Authority - Enforcement.
MAS-TSOFA	SINGAPORE	MAS-TSOFA - Monetary Authority of Singapore - Terrorism Suppression of Financing Act.
MASW	SINGAPORE	MASW - Monetary Authority Warnings
SGCPIB	SINGAPORE	SINGAPORE CORRUPT PRACTICES INVESTIGATION BUREAU - SGCPIB
SKNBS	SLOVAKIA	NATIONAL BANK OF SLOVAKIA - SKNBS
SIGPD	SLOVENIA	SLOVENIAN GENERAL POLICE DIRECTORATE - SIGPD
SISMA	SLOVENIA	SLOVENIAN SECURITIES MARKET AGENCY - SISMA
RSA-CC	SOUTH AFRICA	RSA-CC - South African Competitions Commission
SAPS	SOUTH AFRICA	SOUTH AFRICAN POLICE SERVICE - SAPS
RSA-AT	SOUTH AFRICA	UNSCR 1267 - AL QAIDA TALIBAN - RSA-AT
ZAFSB	SOUTH AFRICA	ZAFSB - Financial Services Board
CNMV	SPAIN	CNMV - Com. Nacional Del Mercado De Valores
DGSFP	SPAIN	DGSFP - Directorate General of Insurance and Pension Funds

ESGC-MW	SPAIN	ESGC-MW - Guardia Civil - Most Wanted
UE	SPAIN	SANCTIONS LISTS - UE
SLGAZ	SRI LANKA	SLGAZ - Sri Lanka Government Gazette Terrorism List
FISE	SWEDEN	FISE - Finansinspektionen.
SESCA	SWEDEN	SESCA - Swedish Competition Authority
BL	SWITZERLAND	BL - Fed. Banking Comm. - All Bush Lists
FDFA	SWITZERLAND	FEDERAL DEPARTMENT OF FOREIGN AFFAIRS - FDFA
FINMA	SWITZERLAND	FINMA - Swiss Financial Market Supervisory Authority
SECO-BLRTB	SWITZERLAND	SECO - BLRTB - State Secretariat for Econ. Affairs - Belarus Travel Ban.
SECO	SWITZERLAND	SECO - State Secretariat for Econ. Affairs.
SECO-Y	SWITZERLAND	SECO - YUGOSLAVIA - SECO-Y
SECO-AT	SWITZERLAND	SECO -AT - State Secretariat for Econ. Affairs - Al Qaida & Taliban.
SECO-BDI	SWITZERLAND	SECO-BDI - State Secretariat for Econ. Affairs - Burundi
SECO-BLR	SWITZERLAND	SECO-BLR - State Secretariat for Econ. Affairs - Belarus Asset Freeze.
SECO-CAR	SWITZERLAND	SECO-CAR - State Secretariat for Econ. Affairs - Central African Republic
SECO-CI	SWITZERLAND	SECO-CI - State Secretariat for Econ. Affairs - Cote D'Ivoire.
SECO-DPRK	SWITZERLAND	SECO-DPRK -State Secretariat for Econ. Affairs - Dem. People's Rep. of Korea.
SECO-DRC	SWITZERLAND	SECO-DRC - State Secretariat for Econ. Affairs - Dem. Rep. Congo.
SECOEMBARGO	SWITZERLAND	SECOEMBARGO - State Secretariat for Econ. Affairs - Country or Region Embargo.
SECO-GN	SWITZERLAND	SECO-GN - State Secretariat for Econ. Affairs - Guinea
SECO-GNB	SWITZERLAND	SECO-GNB - State Secretariat for Econ. Affairs - Guinea-Bissau
SECO-GNTB	SWITZERLAND	SECO-GNTB - State Secretariat for Econ. Affairs - Guinea Travel Ban.
SECO-IRN	SWITZERLAND	SECO-IRN - State Secretariat for Econ. Affairs - Iran.
SECO-IRQ	SWITZERLAND	SECO-IRQ - State Secretariat for Econ. Affairs - Iraq.
SECO-LBY	SWITZERLAND	SECO-LBY - State Secretariat for Econ. Affairs - Libya Asset Freeze
SECO-LBYTB	SWITZERLAND	SECO-LBYTB - State Secretariat for Econ. Affairs - Libya Travel Ban
SECO-LIB	SWITZERLAND	SECO-LIB - State Secretariat for Econ. Affairs - Liberia Asset Freeze.
SECO-LIBTB	SWITZERLAND	SECO-LIBTB - State Secretariat for Econ. Affairs - Liberia Travel Ban.
SECO-MY	SWITZERLAND	SECO-MY - State Secretariat for Econ. Affairs - Myanmar.
SECO-S	SWITZERLAND	SECO-S - State Secretariat for Econ. Affairs - Sudan.
SECO-SOM	SWITZERLAND	SECO-SOM - State Secretariat for Econ. Affairs - Somalia.
SECO-SS	SWITZERLAND	SECO-SS - State Secretariat for Econ. Affairs - South Sudan
SECO-SYR	SWITZERLAND	SECO-SYR - State Secretariat for Econ. Affairs - Syria
SECO-TUN	SWITZERLAND	SECO-TUN - State Secretariat for Econ. Affairs - Tunisia
SECO-UKR	SWITZERLAND	SECO-UKR - State Secretariat for Economic Affairs - Ukraine
SECO-UKRFSR	SWITZERLAND	SECO-UKRFSR -State Secretariat for Economic Affairs - Ukraine - Financial Services Restrictions Art 5
SECO-YEM	SWITZERLAND	SECO-YEM - State Secretariat for Econ. Affairs - Yemen
SECO-Z	SWITZERLAND	SECO-Z - State Secretariat for Econ. Affairs - Zimbabwe.
SIXEX	SWITZERLAND	SIXEX - Six Swiss Exchange
TWFSC	TAIWAN	FINANCIAL SUPERVISORY COMMISSION - TWFSC
MJIB	TAIWAN	MINISTRY OF JUSTICE INVESTIGATION BUREAU - MJIB
TJFIU	TAJIKISTAN	TJFIU - Tajikistan Financial Intelligence Unit
TJMVD	TAJIKISTAN	TJMVD - Ministry of Internal Affairs of Tajikistan
SECTHAI	THAILAND	SEC. EXCHANGE COMM. - SECTHAI
THAMLO	THAILAND	THAI ANTI MONEY LAUNDERING OFFICE - THAMLO
TTFIU	TRINIDAD AND TOBAGO	TTFIU - Trinidad and Tobago Financial Intelligence Unit - Terrorism Orders
TRCOM	TURKEY	TRCOM - Council of Ministers of Turkey - Terrorism Linked Firms
TRMOI	TURKEY	TRMOI - Turkish Ministry of Interior - Most Wanted Terrorists
TRSPK	TURKEY	TRSPK - Capital Markets Board of Turkey
SCFM-TERR	UKRAINE	STATE COMMITTEE FOR FINANCIAL MONITORING - TERRORISM LIST - SCFM-TERR
SCFM	UKRAINE	STATE COMMITTEE FOR FINANCIAL MONITORING - UN SANCTIONS PROGRAMMES - SCFM
UAMVS	UKRAINE	UAMVS - Ukraine Ministry of Internal Affairs
UANBU	UKRAINE	UANBU - National Bank of Ukraine
UANSDC	UKRAINE	UANSDC - National Security and Defence Council of Ukraine.
UAAMC	UKRAINE	UKRAINIAN ANTIMONOPOLY COMMITTEE - UAAMC
UN-CIAC	UN	CHILDREN IN ARMED CONFLICT UN RES 1612 - UN-CIAC
UN-CI	UN	COTE D'IVOIRE - UNSCR 1572 - ASSET FREEZE AND TRAVEL BAN - UN-CI
UNIR	UN	IRAQ UNSCR 1483 & 1518 - UNIR
UN-LIB	UN	LIBERIA UNSCR 1532 - UN-LIB

UN-LBY	UN	UN SANCTIONS - UN RES 1970 - LIBYA - ASSET FREEZE - UN-LBY
UNTB-LBY	UN	UN TRAVEL BAN - LIBYA UN RES. 1970 (2011) - UNTB-LBY
UN1267	UN	UN1267 - United Nations UNSCR 1267 (1999) and 2253 (2015) ISIL - Al Qaida - Asset Freeze & Travel Ban
UN1737	UN	UN1737 United Nations UNSCR 1737 & 2231 - Iran Non - Proliferation - Asset Freeze & Travel Ban
UN1988	UN	UN1988- United Nations UN Res 1988 (2011) - Taliban - Asset Freeze and Travel Ban
UN2140	UN	UN2140- United Nations UN Res 2140 (2014) - Yemen - Asset Freeze And Travel Ban
UN-CAR	UN	UN-CAR - United Nations UNSCR 2127 - Central African Republic
UN-DRC	UN	UN-DRC - United Nations UNSCR 1533 - DR Congo - Asset Freeze & Travel Ban
UNEMBARGO	UN	UNEMBARGO - Country or Region Embargo.
UN	UN	UNITED NATIONS SANCTIONS - UN
UNTB	UN	UNITED NATIONS TRAVEL BAN - UNTB
UN-DPRK	UN	UNITED NATIONS UNSCR 1718 - DEM. PEOPLE'S REP. OF KOREA ASSET FREEZE & TRAVEL BAN - UN-DPRK
UN-SOM	UN	UNITED NATIONS UNSCR 751 & 1907 - SOMALIA & ERITREA - UN-SOM
UNTB-GNB	UN	UNITED NATIONS UNSCR. 2048 - GUINEA-BISSAU TRAVEL BAN - UNTB-GNB
UN-S	UN	UN-S - United Nations UNSCR 1591 - Sudan.
UN-SS	UN	UN-SS - United Nations UN Res 2206 (2015) - South Sudan - Asset Freeze And Travel Ban
UNTB-LIB	UN	UNTB-LIB - United Nations UNSCR 1521 - Travel Ban Liberia.
AEDFSA	UNITED ARAB EMIRATES	AEDFSA - Dubai Financial Services Authority
AEDTO	UNITED ARAB EMIRATES	AEDTO - UAE Designated Terrorist Firms
IOMFSC-D	ISLE OF MAN	FIN. SUPERVISION COMM. - DISSOLVED COs - IOMFSC-D
IOMFSC	ISLE OF MAN	FIN. SUPERVISION COMM. - IOMFSC
IOMFSC-S	ISLE OF MAN	FIN. SUPERVISION COMM. - STRUCK OFF COs - IOMFSC-S
IOMSO	ISLE OF MAN	SANCTIONS ORDERS & FINANCIAL RESTRICTIONS - IOMSO
BBA	UK	BBA - British Banker's Association - Tag List (Temporary)
UKCOLP	UK	CITY OF LONDON POLICE - UKCOLP
DISQUALIFIED DIRECTORS	UK	COMPANIES HOUSE - DISQ. DIRECTORS
DTI-SEC	UK	DTI - STRATEGIC EXPORT CONTROL IRAN - DTI-SEC
FSA	UK	FSA - Financial Conduct Auth. (previously fin services auth)
FSA-UFI	UK	FSA-UFI - Financial Conduct Auth. (previously fin services auth) Unauthorised Firms or Individuals
FSA-UIB	UK	FSA-UIB - Financial Conduct Auth. (previously fin services auth) List of Unauthorised Internet Banks.
FSA-UOF	UK	FSA-UOF - Financial Conduct Auth. (previously fin services auth) List of Unauthorised Overseas Firms.
UK CUSTOMS	UK	HM CUSTOMS & EXCISE - UK CUSTOMS
UKHMRC-TD	UK	HM REVENUE & CUSTOMS TAX DEFAULTERS - UKHMRC-TD
UKHMT	UK	HM TREASURY - UKHMT
UKHMT-AN	UK	HM TREASURY ADVISORY NOTICE - UKHMT-AN
UKHO	UK	HOME OFFICE - UKHO
METPOL	UK	METPOL - Metropolitan Police
SFO	UK	SFO - Serious Fraud Office
UKHMT-FR	UK	UKHMT-FR - HM Treasury Financial Restrictions.
UKHMT-IB	UK	UKHMT-IB - HM Treasury Investment Ban
UKNCA	UNITED KINGDOM	UK NATIONAL CRIME AGENCY - UKNCA
UKGC	UNITED KINGDOM	UKGC - UK Gambling Commission
EC-AIRPORT	UNKNOWN	AIRPORT - Embargoed Country or Region - Airport
EC-PRT	UNKNOWN	PRT - Embargoed Country or Region - Port
ECAIR	UNKNOWN	ECAIR - Embargoed Country Airport
BCU	URUGUAY	BCU - Central Bank Account Closures
BCUPEP	URUGUAY	BCUPEP - Central Bank of Uruguay - PEP List
561LIST	USA	561LIST - Foreign Financial Institutions Subject to Part 561 of IFSR (the 561 List)
ADOI	USA	ADOI - Dept. of Insurance
NYBB	USA	BANKING BOARD, NY STATE - NYBB
BISN	USA	BISN - Bureau of Int Sec & Non-proliferation
BISN.IR-IQ	USA	BISN.IR-IQ - Bureau of Int Sec & Non-proliferation
BISN-CBW	USA	BISN-CBW - Bureau of Int Sec & Non-proliferation.
BISN-EIBA	USA	BISN-EIBA - Bureau of Int Sec & Non-proliferation
BISN-EO12938	USA	BISN-EO12938 - Bureau of Int Sec & Non-proliferation
BISN-EO13382	USA	BISN-EO13382 - Bureau of Int Sec & Non-proliferation

BISN-IRAN	USA	BISN-IRAN - Bureau of Int Sec & Non-proliferation
BISN-IRSY	USA	BISN-IRSY - Bureau of Int Sec & Non-proliferation
BISN-LME	USA	BISN-LME - Bureau of Int Sec & Non-proliferation.
BISN-MIS	USA	BISN-MIS - Bureau of Int Sec & Non-proliferation
BISN-NPPA	USA	BISN-NPPA - Bureau of Int Sec & Non-proliferation
BPI	USA	BPI - OFAC SDN List - Blocked Pending Investigation
BPI-PA	USA	BPI-PA - OFAC SDN List - BPI-Property & Assets
BPI-SDNT	USA	BPI-SDNT - OFAC SDN List - BPI-Specially Designated Narcotics Trafficker.
BPI-SDNTK	USA	BPI-SDNTK - OFAC SDN List - BPI-Specially Designated Narcotics Trafficker Kingpin
INKSNA	USA	BUR OF VERIF, COMPLIANCE & IMPLEMENT - IRAN, N KOREA & SYRIA NONPRO - INKSNA
BXA	USA	BXA - Bureau Ind and Sec Denied Persons List
BXAENT	USA	BXAENT - Bureau of Industry and Security - Entity List
BXAUNVER	USA	BXAUNVER - Bureau Industry and Security - Unverified List
CADI	USA	CADI - California Department of Insurance
CORPCA	USA	CALIFORNIA DEPARTMENT OF CORPORATIONS - CORPCA
USCBOE	USA	CHICAGO BOARD OPTIONS EXCHANGE - USCBOE
CFTC	USA	COMMODITY FUTURES TRADING COMM. - CFTC
PDGS	USA	DEPT GEN. SERVICES, PENNSYLVANIA - PDGS
WISCONSIN DT	USA	DEPT OF TRANSPORTATION, WISCONSIN - WISCONSIN DT
USDTC-CA	USA	DIR. OF DEFENSE TRADE CONTROLS - CONSENT AGREEMENTS - USDTC-CA
USDEA	USA	DRUG ENFORCEMENT ADMIN. - USDEA
EPLS	USA	EXCLUDED PARTIES LISTING SYSTEM - EPLS
FBI	USA	FBI
FDIC-FB	USA	FED DEPOSIT INS. CORP. - FAILED BANKS - FDIC-FB
FDIC	USA	FED DEPOSIT INS. CORP. - FDIC
USFRB	USA	FEDERAL RESERVE BOARD - USFRB
USFTC	USA	FEDERAL TRADE COMMISSION - USFTC
FINCEN	USA	FINANCIAL CRIMES ENFORCEMENT NETWORK - ENFORCEMENT ACTIONS - FINCEN
FINRA	USA	FINANCIAL INDUSTRY REGULATORY AUTHORITY - FINRA
FSEL	USA	FSEL - Foreign Sanctions Evaders List.
HHS	USA	HHS - Dept of Health & Human Services
HHS-CMP	USA	HHS-CMP - Department of Health & Human Services - Civil Monetary Penalties
ICE	USA	IMMIGRATION & CUSTOMS ENFORCEMENT - ICE
MAGNIT	USA	MAGNIT - OFAC SDN LIST - Magnitsky Sanctions
USNCUA	USA	NAT. CREDIT UNION ADMIN - USNCUA
MIPT	USA	NAT. MEMORIAL INST. PREVENTION OF TERRORISM - MIPT
NFA	USA	NATIONAL FUTURES ASSOC. - NFA
NYDFS	USA	NEW YORK DEPARTMENT OF FINANCIAL SERVICES - NYDFS
NYSE	USA	NEW YORK STOCK EXCHANGE - NYSE
NS-IRAN	USA	NS-IRAN - NON SDN List Iran (EO13599)
NS-PLC	USA	NS-PLC - OFAC - Palestinian Legislative Council List.
OCCEA	USA	OCC ENFORCEMENT ACTIONS - OCCEA
OCCBANK	USA	OCC NATIONAL BANKS - OCCBANK
CIVPEN	USA	OFAC CIVIL PENALTIES - CIVPEN
OFAC-NONSDN	USA	OFAC NON SDN List - OFAC-NONSDN
OFAC-BK	USA	OFAC SDN LIST - BALKANS - OFAC-BK
OFAC-BLR	USA	OFAC SDN LIST - BELARUS - OFAC-BLR
OFAC-BM	USA	OFAC SDN LIST - BURMA - OFAC-BM
OFAC-CAR	USA	OFAC SDN LIST - CENTRAL AFRICAN REPUBLIC - OFAC-CAR
OFAC-COTED	USA	OFAC SDN LIST - COTE D'IVOIRE - OFAC-COTED
OFAC-C	USA	OFAC SDN LIST - CUBA - OFAC-C
OFAC-DFR	USA	OFAC SDN LIST - DARFUR - OFAC-DFR
OFAC-DPRK	USA	OFAC SDN LIST - DEM. PEOPLE'S REP. OF KOREA - OFAC-DPRK
OFAC-DRC	USA	OFAC SDN LIST - DRCONGO - OFAC-DRC
OFAC-EO13622	USA	OFAC SDN LIST - EO 13622 - OFAC-EO13622
OFAC-EO13645	USA	OFAC SDN LIST - EO 13645 - OFAC-EO13645
OFAC-FSEIR	USA	OFAC SDN LIST - FOREIGN SANCTIONS EVADERS EO - IRAN - OFAC-FSEIR
FTO	USA	OFAC SDN LIST - FOREIGN TERRORIST FIRM - FTO
SDGT	USA	OFAC SDN LIST - GLOBAL TERRORIST - SDGT

OFAC-HRIT	USA	OFAC SDN LIST - HUMAN RIGHTS INFORMATION TECHNOLOGY - OFAC-HRIT
IFSR	USA	OFAC SDN LIST - IRAN FINANCIAL SANCTIONS REGULATION - IFSR
IRAN-HR	USA	OFAC SDN LIST - IRAN HUMAN RIGHTS - IRAN-HR
OFAC-ISA	USA	OFAC SDN LIST - IRAN SANCTIONS ACT - OFAC-ISA
IRAN-TRA	USA	OFAC SDN LIST - IRAN THREAT REDUCTION ACT- IRAN-TRA
OFAC-IRN	USA	OFAC SDN LIST - IRAN: SDN AND NON SDN (designated under EO 13599) - OFAC-IRN
IRAQ.2	USA	OFAC SDN LIST - IRAQ.2
IRAQ.3	USA	OFAC SDN LIST - IRAQ.3
IRGC	USA	OFAC SDN LIST - ISLAMIC REVOLUTIONARY GUARD CORP - IRGC
OFAC-LBN	USA	OFAC SDN LIST - LEBANON - OFAC-LBN
OFAC-L	USA	OFAC SDN LIST - LIBERIA - OFAC-L
SDNTK	USA	OFAC SDN LIST - NARC. TRAFF. KINGPIN - SDNTK
SDNT	USA	OFAC SDN LIST - NARCOTICS TRAFFICKER - SDNT
OFAC-NK	USA	OFAC SDN LIST - NORTH KOREA - OFAC-NK
NPWMD	USA	OFAC SDN LIST - NPWMD
OFAC-SOM	USA	OFAC SDN LIST - SOMALIA - OFAC-SOM
OFAC-SYR	USA	OFAC SDN LIST - SYRIA: SDN AND NON SDN (designated under EO 13582) - OFAC-SYR
SDT	USA	OFAC SDN LIST - TERRORIST - SDT
OFAC-TCO	USA	OFAC SDN LIST - TRANSNATIONAL CRIMINAL ORGANIZATIONS - OFAC-TCO
OFAC-YEM	USA	OFAC SDN LIST - YEMEN - OFAC-YEM
OFAC-Z	USA	OFAC SDN LIST - ZIMBABWE - OFAC-Z
OFAC	USA	OFAC SDN LIST (OFFICE OF FOREIGN ASSETS CONTROL) - OFAC
OFAC-BDI	USA	OFAC-BDI - OFAC SDN List - Burundi
OFAC-CYBER2	USA	OFAC-CYBER2 - OFAC SDN List - Significant Malicious Cyber-Enabled Activities
OFAC-DPRK2	USA	OFAC-DPRK2 - OFAC SDN List -Dem People's Rep of Korea
OFAC-DPRK3	USA	OFAC-DPRK3 - OFAC SDN List -Dem People's Rep of Korea
OFAC-LIBYA2	USA	OFAC-LIBYA2 - OFAC SDN List - Libya
OFAC-LIBYA3	USA	OFAC-LIBYA3 - OFAC SDN List - Libya
OFAC-S	USA	OFAC-S - OFAC SDN List - Sudan.
OFAC-SS	USA	OFAC-SS - OFAC SDN List - South Sudan.
OFAC-UKR	USA	OFAC-UKR - OFAC SDN List - EO13660 (Ukraine)
OFAC-UKR13685	USA	OFAC-UKR13685 - OFAC SDN List - EO13685 (Ukraine)
OFAC-UKR2	USA	OFAC-UKR2 - OFAC SDN List - EO13661 (Ukraine2)
OFAC-VE	USA	OFAC-VE - OFAC SDN List - Venezuela
OTS	USA	OFFICE OF THRIFT SUPERVISION - OTS
USPS	USA	POSTAL INSPECTION SERVICE - USPS
PCAOB	USA	PUBLIC FIRM ACCOUNTING OVERSIGHT BOARD - PCAOB
SDTEL	USA	SDTEL -State Dept. Terrorist Excl. List.
SEC	USA	SECURITIES EXCHANGE COMM - SEC
SEC-PAUSE	USA	SECURITIES EXCHANGE COMM - UNREG SOLICITING ENTITIES - SEC-PAUSE
USSIGIR	USA	SPECIAL INSPECTOR GENERAL FOR IRAQ RECONSTRUCTION - USSIGIR
ITRSHRA	USA	STATE DEPT - IRAN THREAT REDUCTION & SYRIA HUMAN RIGHTS ACT - ITRSHRA
NYSID	USA	STATE INSURANCE DEPT, NY - NYSID
UKR-EO13662	USA	UKR-EO13662 - Sectoral Sanctions Identifications List.
USBIS-EV	USA	US BUREAU OF INDUSTRY & SECURITY - EXPORT VIOLATIONS - USBIS-EV
USINL	USA	US BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT - USINL
USDOL-OLMS	USA	US DEPARTMENT OF LABOR, OFFICE OF LABOR - MANAGEMENT STANDARDS - USDOL-OLMS
US MARSHALLS	USA	US MARSHALLS
USATF	USA	USATF - Bureau of Alcohol Tobacco Firearms & Explosives
USDOJ	USA	USDOJ - Dept. of Justice.
USDOJ-EOIR	USA	USDOJ EXECUTIVE OFFICE FOR IMMIGRATION REVIEW - DISCIPLINED PRACTITIONERS LIST - USDOJ-EOIR
USDOL-EBSA	USA	USDOL-EBSA - US Department of Labor, Employee Benefits Security Administration
USDTC	USA	USDTC - Dir. of Defense Trade Controls.
USEMBARGO	USA	USEMBARGO - Country or Region Sanctions.
USSAG	USA	USSAG - US State Attorneys General
USSIGAR	USA	USSIGAR - Special Inspector General for Afghanistan Reconstruction
USSPSC	USA	USSPSC - US State Prohibited or Scrutinized Companies
USTREAS.311	USA	USTREAS.311 - Patriot Act Section 311.

ISA	USA	ISA - Iran Sanctions Act
VCNV	VENEZUELA	NAT. SECURITIES COMM. OF VENEZUELA - COMISION NACIONAL DE VALORES - VCNV
SUDESEG	VENEZUELA	SUPERINTENDENCIA DE LA ACTIVIDAD ASDURADORA - SUDESEG
VECGR	VENEZUELA	VECGR - Comptroller Generals Office of Venezuela
SUDEBAN	VENEZUELA	VENEZUELAN SUPERINTENDENCY OF BANKING SECTOR INSTITUTIONS - SUDEBAN
SSCVN	VIET NAM	STATE SECURITIES COMMISSION OF VIETNAM - SSCVN
BVIFSC	VIRGIN ISLANDS (BRITISH)	BVIFSC- Financial Services Comm. - Advisory Warnings

10.3 Due diligence standards

The firm acknowledges that different client types will have different identification and verification requirements and that those requirements are dependent on their risk rating.

The minimum requirements are identified, along with suggested further evidence and actions to undertake enhanced due diligence as appropriate to obtain a level of comfort around the client.

In order to undergo the client risk rating, identification and verification the following information will be obtained at client onboarding and will be kept up to date during the duration of the business relationship for existing clients.

Individuals/Natural Persons	Legal Persons
Client Attributes	
- Client type - Occupation/Industry - Source of funds/wealth	- Client type - Occupation/Industry - Source of funds/wealth
Jurisdictional	
- Country of citizenship - Country of residence	- Country of incorporation/registration - Country of operation
Product & Service	
- Product and/or Service required - Channel of delivery (e.g. non face to face)	- Product and/or Service required - Channel of delivery (e.g. non face to face)

Risk level	Level of due diligence
Low	Simplified due diligence
Medium	Standard due diligence
High	Enhanced due diligence

10.3.1 Natural Persons – Adult

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Standard due diligence	Enhanced due diligence
Full name	South African: Green bar-coded ID book or ID card (front and back) Foreign: Valid international passport with valid permit issued by home affairs	Sighted documents Certified copies
Date of birth		
Country of citizenship/Nationality		
Identity Number		
Current physical address	Documentary evidence of residential address dated within the last three months	Supporting additional documentary evidence of address dated within the last three months Sighted documents Certified copies Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	Documentary evidence
Source of funds	Client disclosure	Documentary evidence
Source of wealth	Client disclosure	Documentary evidence
DPIP or FPPO?	Client disclosure	
Industry of occupation	Client disclosure	Documentary evidence of employment where veracity doubted

10.3.2 Natural Persons – Minor

Simplified due diligence consists of the same requirements as standard due diligence.

The guardian/representative of the minor will be subject to identification and verification as a natural person.

Information Required	Standard due diligence	Enhanced due diligence
Full name	Birth Certificate	Sighted documents Certified copies
Date of birth		
Country of citizenship/Nationality		
Identity Number		
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	Documentary evidence
Source of funds	Client disclosure	Documentary evidence
Source of wealth	Client disclosure	Documentary evidence
DPIP or FPPO?	Client disclosure	
Industry of occupation	Client disclosure	Documentary evidence of employment where veracity doubted

10.3.3 Natural Persons – Sole Proprietor

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Standard due diligence	Enhanced due diligence
Full name	South African: Green bar-coded ID book or ID card (front and back) Foreign: Valid international passport with valid permit issued by home affairs	Sighted documents Certified copies
Date of birth		
Country of citizenship/Nationality		
Identity Number		
Current physical address	Documentary evidence of residential address dated within the last three months	Supporting additional documentary evidence of address dated within the last three months Sighted documents Certified copies Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business trading name	Client disclosure	Supporting additional documentary evidence such as insurances or invoices
Business trading address	Client disclosure	If different from residential physical address, supporting additional documentary evidence such as insurances or invoices
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	Documentary evidence
Source of funds	Client disclosure	Documentary evidence
Source of wealth	Client disclosure	Documentary evidence
DPIP or FPPO?	Client disclosure	
Business activities/industry	Client disclosure	

10.3.4 Close Corporation

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Registered name	CIPC documentation	Certified Copies
Registration number		
Registered address		
Trading address	Documentary evidence of address dated within the last three months	Supporting additional documentary evidence of address dated within the last three months Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of funds	Client disclosure	Documentary evidence
Business activities/industry	Client disclosure	Documentary evidence, independent research
Member/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Face to face Certified copies Evidence of address
Authorised Persons/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Face to face Certified copies Evidence of address

10.3.5 Listed Firm

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Registered name	Client disclosure verified by listing at approved stock exchange.	
Registration number		
Registered address		
Trading address	Client disclosure	Supporting additional documentary evidence of address dated within the last three months Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of funds	Client disclosure	Documentary evidence
Business activities/industry	Client disclosure	Documentary evidence, independent research
Ultimate Beneficial Owner/s (where applicable, else default to the Principal Executive Officers)	Client disclosure with supporting ID document, supporting residential address document and contact details.	Independent organogram Face to face Certified copies
Authorised Persons/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Face to face Certified copies Evidence of address

10.3.6 Unlisted Firm

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Registered name	CIPC or Foreign Firm Register documentation	
Registration number		
Registered address		
Trading address	Client disclosure	Supporting additional documentary evidence of address dated within the last three months Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of funds	Client disclosure	Documentary evidence
Business activities/industry	Client disclosure	Documentary evidence, independent research
Related Parties (e.g. Principle Executive Officers, Directors)	Client disclosure with supporting ID document, supporting residential address document and contact details.	Independent organogram Face to face Certified copies Evidence of address
Ultimate Beneficial Owner/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Independent organogram Face to face Certified copies
Authorised Persons/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Face to face Certified copies Evidence of address

10.3.7 Non-Profit Firm & Other Entities

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Registered name	Client disclosure verified by listing at approved stock exchange.	
Registration number		
Registered address		
Trading address	Client disclosure	Supporting additional documentary evidence of address dated within the last three months Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of funds	Client disclosure	Documentary evidence
Industry operated in	Client disclosure	Documentary evidence, independent research
UBO & Related Parties (As appropriate; UBO, Principle Executive Officers, Directors, Voting Members as appropriate)	Client disclosure with supporting ID document, supporting residential address document and contact details.	Independent organogram Face to face Certified copies
Authorised Persons/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Face to face Certified copies Evidence of address

10.3.8 Partnership

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Registered name	Partnership agreement	Certified Copies Verification (Docfox)
Registration number		
Registered address		
Trading address	Documentary evidence of address dated within the last three months	Supporting additional documentary evidence of address dated within the last three months Physical visit Google street view
Contact telephone/email	Client disclosure	
SA tax registration	Client disclosure	Documentary evidence of tax registration from tax authority (e.g. SARS) dated within the last three months
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of funds	Client disclosure	Documentary evidence
Industry operated in	Client disclosure	Documentary evidence, independent research
Partners	Client disclosure with supporting ID document, supporting residential address document and contact details.	Independent organogram Face to face Certified copies
Authorised Person/s	Client disclosure with supporting ID document, supporting residential address document and contact details.	Face to face Certified copies Evidence of address

10.5.9 Trusts

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Registered name	Where applicable; Trust Deed, copy of Letter of Authority issued by Master of the High Court giving authority to Trustee to act	Certified documents
Registration number		
Address of Master of the High Court where trust registered		
Contact address	Client disclosure	Supporting documentary evidence of address dated within the last three months
Contact telephone/email	Client disclosure	
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of wealth	Client disclosure	Documentary evidence
Source of funds	Client disclosure	Documentary evidence
Occupation/Previous Occupation/Industry operated in	Client disclosure	Documentary evidence, independent research
Related Parties: Founders/Donors/Settlers/Executor/Trustee/Curator/Tutor/Named Beneficiaries	Client disclosure confirmed against Trust Deed with supporting ID document, residential address and contact details.	Face to face Certified copies Evidence of address
Authorised Person/s, Representatives	Client disclosure with supporting ID document, residential address and contact details.	Face to face Certified copies Evidence of address

10.5.10 Late Estates

Simplified due diligence consists of the same requirements as standard due diligence.

Information Required	Evidence – Standard	Evidence - Enhanced
Estate name	Where applicable; Trust Deed, copy of Letter of Authority issued by Master of the High Court giving authority to Trustee to act	Certified documents
Registration number (if applicable)		
Address of Master of the High Court where Estate registered		
Contact address	Client disclosure	Supporting documentary evidence of address dated within the last three months
Contact telephone/email	Client disclosure	
Business relationship type	Client disclosure	
Reason for transaction/s	Client disclosure	
Source of wealth	Client disclosure	Documentary evidence
Source of funds	Client disclosure	Documentary evidence
Last Occupation/Industry operated in	Client disclosure	Documentary evidence, independent research
Testator/Deceased	Client disclosure with supporting ID with residential address written on.	Face to face Certified copies Evidence of address
Related Parties: Founders/Donors/Settlers/Executor/Trustee/Curator/Tutor/Named Beneficiaries	Client disclosure confirmed against Trust Deed with supporting ID document, residential address and contact details.	Face to face Certified copies Evidence of address
Authorised Person/s	Client disclosure with supporting ID document, residential address and contact details.	Face to face Certified copies Evidence of address

○ 10.4 Examples of acceptable proof of address

Document type	Document date	Validity
Bank letter/statement	Less than three months	• Only acceptable from a bank operating from, or incorporated in, a Financial Action Task Force (FATF) member country • Must indicate an existing product relationship with the institution, <i>excluding marketing material</i> • If obtained from a bank directly, it must include the bank stamp • Note: transaction history is not considered a bank statement
Employer declaration for foreign nationals	Less than three months	• Letter on a firm letterhead from the employer Confirming employment, contract period (if not permanent) and address. Must be accompanied by a valid residency permit and/or work visa
Insurance firm contract or letter	Less than one year	• Must be on the letterhead of the insurance firm • Letter or contract must confirm the existence of an active long-term or short-term insurance policy
Lease or rental agreement	Must be in occupancy term	• Must be signed by the client (tenant/lessee) and the landlord/lessor and be in term • If the lease has expired and the residential address is as per the lease, the terms must be reviewed to Confirm that the lease allows for continued occupancy and Confirmation of occupancy must be obtained from the landlord/lessor
Levy/statement issued by a body corporate, homeowner's association or managing agent	Less than three months	• Applicable for properties in sectional title, cluster or share-block developments • Must be on the letterhead of the applicable body corporate, homeowner's association or managing agent
Mobile phone account or Telkom account	Less than three months	• Must detail full name and address of client • Mobile phone accounts only from South African mobile phone companies (eg MTN, Vodacom etc)
Utility bill	Less than three months	• Can include pre-paid and metering services
Cohabitation declaration	Less than six months	• Must detail full name, ID and address of client and the signatory as well as signed and dated with support ID and proof of address from signatory
Official SARS document / certificate	Less than one year	• Must detail full name, ID and address of client
Motor vehicle licence document	Less than one year	• Must detail full name, ID and address of client
Letter from Municipal representative	Less than three months	• Must detail full name, ID and address of client • Must be on the letterhead of the applicable municipality and identify full name of representative making declaration
Letter from traditional authority	Less than three months	• Must detail full name, ID and address of client • Must identify full name of representative making declaration
Retail/Credit account statement	Less than three months	• Must detail full name, ID and address of client
Mortgage/Bond statement	Less than three months	• Must detail full name, ID and address of client

○ 10.5 Example evidence of source of funds/wealth

The following represents a selection of potential sources of funds and wealth and suggested sources of further evidence for enhanced due diligence.

Source	Potential evidence
Allowances	Confirmation from the Payee
Bursary	- Confirmation from the Payee - Bursary grant documentation
Firm Profits	- Latest audited accounts/financial statements - Letter from accountant/auditor
Firm Sale	Sale agreement
Court Order	Official court documentation
Directors/Members Fees	Bank statement, pay slips or proof of payment showing receipt of 3 months regular salary payments from named employer
Dividends from investments	- Certificate of dividend - Investment statement
Divorce settlement	- Final court order - Divorce decree - Signed letter from attorney
Gift/Donation	Confirmation from the Payee
Income from Employment	- Bank statement, pay slips or proof of payment showing receipt of 3 months regular salary payments from named employer - Letter of appointment if before first pay date - Latest accounts if self-employed
Income from Previous Employment	- Bank statement, pay slips or proof of payment showing receipt of 3 months regular salary payments from named employer for stated period - Old letter of appointment
Inheritance	Copy of will or letter from Executor including details such as value and beneficiaries of the Estate
Loan	Loan agreement or recent loan statements
Lottery/Winnings/Gambling	Notification of winnings from appropriate body/entity
Maintenance	- Final court order - Divorce decree - Signed letter from attorney
Maturing Investments	Investment certificate or notification of maturing investment
New Investment/ Capital Raise	- Reputable news article - Letter from attorney - Legal documentation supporting capital raise
Pension	Pension or provident certificate/confirmation
Sale of Asset	- Completed sale contract/proof of sale - Letter from attorney
Sale of Shares	- Legal sale document - Confirmation from attorney or accountant if business shares sold - Proof of sale/agreement
Deceased Estate	- Copy of will - Trust deed - Letter from the Executor of the Estate
Trust Distribution	- Copy of will - Beneficiary proof of payout - Trust deed - Letter from the Executor of the Estate
Rental Income	- Bank statement showing receipt of rental income - Rental agreements

○ 10.6 Client Profile Forms – Natural & Legal Persons

Personal Information			
Full name			
Nationality		ID/Passport Number	
Residential address			
Postal address			
Telephone		Email	
Occupation (or occupation prior to retirement)			
Main Employer Business/Activity (or activity prior to retirement)			
Are any of the persons named, their immediate family members or close associates considered a Domestic Prominent Influential Person or Foreign Prominent Public Official? This includes senior judicial officials, senior executives of state-owned entities, political leaders, government representatives, high-ranking military, head of an international firm based in South Africa? Yes/No If yes, please provide details of the individual/s and their relationship			
Do you anticipate single transaction or ongoing relationship?		☐ Single Transaction ☐ Ongoing Relationship	
Main reason for transaction/s			
What is the main source of funds for the transactions?			
Product/services anticipated			

Firm Information			
Registered name			
Trading name		Firm registration number	
Registered address		SARS Tax number	
		VAT number Import No.	
Operating address		Main telephone number	
		Website address	
Key Contact person		Telephone	
Cell phone		Email	
Main Business Activity & Industry			
Business Executive Management and Control		Business Ownership > 25% shareholding	
Please list all personals of the firm who have Executive Control (e.g. Directors, Partners, Members, Trustees, Executor) and provide a copy of the ID/Passport documents with physical address and contact details.		Please list all natural and legal person shareholders of the firm with a holding of 25% or more . Please provide a copy of the ID/Passport documents along with physical address and contact.	
Full name of all Executive Staff		Full name of person or Entity	% holding
1)		1)	
2)		2)	
3)		3)	
4)		4)	
5)		5)	
Ultimate Beneficial Owner/s: If different to Business Ownership above, please list the natural person/s who ultimately owns the legal person or exercises effective control over it either directly, through an ownership structure or as a Donor, Trustee or Beneficiary. Please provide a copy of the ID/Passport documents with physical address and contact details.			
1)		2)	
3)		4)	
Are any of the persons named, their immediate family members or close associates considered a Domestic Prominent Influential Person or Foreign Prominent Public Official? This includes senior judicial officials, senior executives of state-owned entities, political leaders, government representatives, high-ranking military, head of an international firm based in South Africa? Yes/No If yes, please provide details of the individual/s and their relationship			
Do you anticipate single transaction or ongoing relationship?		☐ Single Transaction ☐ Ongoing Relationship	
Main reason for transaction/s			
What is the main source of funds for the transactions?			
Product/services anticipated			