TO:	**INVESTMENT MANAGERS** **LINKED INVESTMENT SERVICE PROVIDERS** **STOCK-BROKERS** **UNIT TRUST MANAGEMENT COMPANIES** **UNLISTED INVESTMENT MANAGERS** **LONG-TERM INSURANCE COMPANIES** **MICROLENDERS**
GUIDELINES NO.:	**AML/02/2023**
DATE:	**18 JULY 2023**
SUBJECT:	**GUIDELINES ON THE APPLICATION OF AML/CFT/CPF RISK-BASED APPROACH**

1. DEFINITIONS AND ACRONYMS

"AIs" Accountable Institution, which means a person or entity listed in Schedule 1 of the Financial Intelligence Act, No. 13 of 2012 ("FIA").

"Beneficial Owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

"Business relationship" means an arrangement between a client and an accountable institution for the purpose of concluding transactions on a regular basis.

"CDD" means Customer Due Diligence.

"Client and Customer" have their ordinary meaning and are used interchangeably herein.

"Customer Due Diligence" (CDD) means a process which involves establishing the identity of a client, the identity of the client's beneficial owners in respect of legal persons and monitoring all transactions of the client against the client's profile.

"Enhanced Due Diligence" (EDD) means doing more than the basic CDD which includes, amongst others, taking measures as per the FIA to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client or beneficial owners whose activities may pose a risk of ML, TF or PF.

"Establish Identity" means a two-tier process consisting of *ascertainment or collecting* of certain identification information, and *verification* of some of the information against reliable documentation or information.

"FATF" means the Financial Action Task Force.

"FIA" refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012).

“FIC” means the Financial Intelligence Centre.

“ML” means Money Laundering.

“Monitoring” as defined in the FIA.

“PIPs” means Prominently Influential Persons as envisaged in FIA amendments.

“PF” means proliferation financing.

“Records” means any material on which information is recorded or marked and which is capable of being read or understood by a person, or by an electronic system or other device.

“Regulations” refer to the FIA Regulations unless otherwise specified.

“RBA” refers to the Risk Based Approach. An approach for managing risks based on prioritization of such risks as per the occurrence/frequency/probability and potential impacts/consequences of each identified risk.

“SAR” refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of FIA.

“Single Transaction” means a transaction other than a transaction concluded in the course of a business relationship.

“STR” refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the FIA.

“TF” means Terrorist Financing.

"TPFA" means Terrorist & Proliferation Financing Activity report. Activity (or attempted transaction which was not completed) which may point to, or be linked to potential terrorism, TF or PF.

"TPFT" means Terrorist & Proliferation Financing Transaction report. Transaction (actual transaction that has taken place) which may point to, or be linked to potential terrorism, TF or PF.

"Transaction" means a transaction concluded between a client and an accountable or reporting institution in accordance with the type of business carried on by that institution and includes attempted transactions.

2. BACKGROUND

2.1 NAMFISA in terms of schedule 2 of FIA read with section 35(2) of FIA has a statutory obligation to supervise, monitor, and enforce compliance with the provisions of FIA or any regulation, order, circular, notice, determination or directive issued in terms of FIA, in respect of all AIs supervised by it.

2.2 Furthermore, section 35(15) (d) of FIA confers the mandate upon NAMFISA to,

> *"issue guidelines to assist accountable and reporting institutions in detecting suspicious patterns of behaviour in their clients and these guidelines shall be developed taking into account modern and secure techniques of money management and will serve as an educational tool for accountable and reporting institutions' personnel".*

2.3 In light of the above, NAMFISA issues these guidelines to AIs under its purview to –

2.3.1 assess and maintain understanding of the ML/TF/PF risks they are exposed to in terms of the nature of business they conduct, the type of clients they serve, the delivery channels and the geographical area where their clients and clients' businesses originate;

2.3.2 effectively apply a risk-based approach by applying measures commensurate with the level of the ML/TF/PF risks identified; and

2.3.3 effectively identify suspicious patterns of behavior in their clients

2.4 It is expected that the assessment of ML/TF/PF risks considers all the prescribed risk factors namely, client, products/services, delivery channels, geography, as well as the recent national and sectoral risk assessments.

2.5 These guidelines will assist AIs to mitigate ML/TF/PF risks on a risk-sensitive basis.

3. APPLICATION OF A RISK-BASED APPROACH

3.1 The application of a Risk-based approach is premised on the AI's understanding of ML/TF/PF risks emerging from the nature of business it conducts, the type of clients it serves, the channel used for product offering or delivery of a financial service, the geographical nature of its business and origin of its clients and their businesses.

3.2 The aforementioned understanding forms the basis of the AI's internal policy, procedures and controls, and the extent of application thereof to mitigate ML/TF/PF risks identified.

3.3 The application of a risk-based approach is preceded by risk identification and assessment to determine the extent of the exposure (risk levels) and the consequences should the identified risks materialized.

3.4 The process of identification and assessment of the risks is followed by the application of internal AML/CFT/CPF measures commensurate with the level of the risk exposure. This is what is called a risk-based approach, and it is central to the effective application of AML/CFT/CPF measures designed to

mitigate ML/TF/PF risks so identified. These measures are universally harmonized to avoid arbitrage across jurisdictions.

3.5 Every risk assessment should be based on a particular risk assessment methodology. There is no single (universal) risk assessment methodology that is the best methodology. Any risk assessment methodology that leads to identification of risk events, threats and consequences is a good methodology.

3.6 Therefore, a risk assessment methodology adopted by the AI ought to be approved by senior management of that AI before the AI commences with the identification and assessment of ML/TF/PF risks.

3.7 Similarly, the findings of the ML/TF/PF risk assessment are to be documented and approved by senior management of the AI. Risks are not static; therefore, the risk assessment is to be conducted periodically, taking into account new developments.

4. AML/CFT/CPF POLICIES, PROCEDURES AND CONTROLS

4.1 The AI's AML/CFT/CPF Policy outlines the procedures/internal rules and controls aligned to the requirements under FIA, and ought to be approved by senior management. The application of internal procedures/rules and controls should be done on a risk-sensitive basis.

4.2 To ensure effectiveness thereof, the nature and extent of AML/CFT/CPF controls will depend upon a number of factors including:

4.2.1 nature, scale and complexity of the AI's business: there must be alignment between controls implemented and nature or type of risks at hand;
4.2.2 diversity of the AIs' operations, including geographical diversity;
4.2.3 the nature of the AIs' product(s)/services;
4.2.4 volume and value of transactions;
4.2.5 risk exposure/risk level;
4.2.6 solicited and unsolicited clients;

4.2.7 non-face-to-face or walk-ins; and

4.2.8 frequency of customer contact.

4.3 Executive management should see to it that the risk-based AML/CFT/CPF framework is designed and driven by people with relevant specialized expertise.

5. CUSTOMER DUE DILIGENCE (CDD) MEASURES

5.1 The nature, extent and type of CDD are key to the effective functioning of the AML/CFT/CPF framework, and the application thereof depends on the risk level an individual client poses to the AI.

5.2 CDD measures include ascertaining clients' profiles which will help the AI to monitor transactional behavior of clients to be able to identify any unusual or suspicious activities. This is important because even people known to AIs may become involved in illegal activities at some point, for example, if their personal circumstances change or they face new financial pressures.

5.3 The AI should be able to demonstrate that the extent of the CDD measures applied for each client are appropriate to mitigate ML/TF/PF risks posed by clients.

5.3.1 ***Simplified Due Diligence of natural persons:***

5.3.1.1 Simplified Due Diligence in principle suggests reduced or less extensive CDD measures.

5.3.1.2 It is also applicable to natural persons when acting on behalf of legal persons such as Close Corporations or Companies and legal arrangements such as Trusts and Partnerships. Simplified CDD for natural persons when they access AIs' services in their personal capacities is explained below.

5.3.2 ***Extent of Simplified CDD***

5.3.2.1 FIA Regulations 6 to 11 provide guidance on the basic identification procedures that should be followed for the various types of clients. However, where ML/TF/PF risks are lower, financial institutions are allowed to conduct simplified CDD measures.

5.3.2.2 The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

5.3.2.2.1 Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g if account transactions rise above the CDD monetary threshold);

5.3.2.2.2 Reducing the frequency of customer identification updates;

5.3.2.2.3 Reducing the degree of on-going monitoring and scrutinizing transactions, based on the CDD or monetary threshold;

5.3.2.2.4 Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established; and

5.3.2.2.5 Previously, AIs could rely on the exemption order issued under the Government Notice No. 75 of 2009 which initially made provision for a degree of

simplified CDD for certain types of clients i.e. public companies listed on a recognized stock exchange, NAMFISA regulated institutions or state-owned / public enterprises. Although this exemption order has been retracted, AIs can rely on the guidelines provided herein to perform simplified CDD.

5.3.3 ***Ascertainment and Verification of Information***

5.3.3.1 When simplified due diligence is applicable, AIs are still required to identify and verify or ascertain customers' identification information. Below is a list of the type of information for natural persons which needs to be ascertained/verified and that which simply needs to be obtained (primarily from client):

5.3.3.1.1 Verification: full names;
5.3.3.1.2 Verification: nationality;
5.3.3.1.3 Verification: If citizen – national ID no./ passport no./date of birth;
5.3.3.1.4 Verification: Non-citizen – passport no./national ID no./date of birth;
5.3.3.1.5 Obtain: Namibia residential address for citizens OR if non-citizen, residential address in his/her country or physical address in Namibia, if any; and
5.3.3.1.6 Contact particulars.

5.3.3.2 AIs to ensure due verification of identification information before availing any services. Verification for natural persons should ideally be done with the Ministry of Home Affairs' National Identification Database. However, such is not possible at the time of issuing this guidance. Therefore, in the interim AIs should use other reliable means to verify identity of clients such as comparing ID documents to passports, voter's cards, birth certificates and such other reliable mechanisms.

5.3.4 ***Simplified due diligence for legal persons, and legal arrangements***

5.3.4.1 Similarly, AIs are only required to obtain basic identification information/documents of the legal person or arrangement. Basic verification of company or trust registration information is always essential.

5.3.4.2 The nature of business, source of funds and such additional information around legal person's financial profile can be assumed from the information at hand. Paragraph 8 herein explains simplified due diligence and EDD measures for legal persons, and legal arrangements.

5.3.5 ***Tips on simplified CDD***

5.3.5.1 AIs may:

5.3.5.1.1 use information already at hand such as client profile, without unduly requesting for more. For example, if the AI identified its customer as a Manager in a local shop or pensioner, the AI can assume what the source of funds is, unless other factors exist (such as higher financial values which may be beyond reasonable earnings of such person); and

5.3.5.1.2 adjust the frequency of ODD, when necessary, for example, when a change occurs which may suggest escalation of the low-risk rating to a higher one.

5.3.6 ***Pre-requisites for Simplified Due Diligence***

5.3.6.1 To apply simplified due diligence, an AI must ensure that:

5.3.6.1.1 it is supported by internal customer risk assessment;

5.3.6.1.2 enhanced due diligence does not apply (there is no high risk in terms of client, geographic considerations, payment method etc.);

5.3.6.1.3 monitoring the business relationship or transactions (e.g with frequent transactions of similar client) to ensure that there is nothing unusual or suspicious from the outset;

5.3.6.1.4 customer is not from, nor associated with a high risk country;

5.3.6.1.5 the customer is not a Prominently Influential Person (PIP), a family member, or a known close associate of a PIP as envisaged in FIA amendments;

5.3.6.1.6 the real customer is seen face-to-face (and not having others transact on his/her behalf unduly to evade detection);

5.3.6.1.7 customer is not dealing through a shell or shelf company;

5.3.6.1.8 client is not dealing through a complex legal structure to hide the identification of true beneficial owners or those who will ultimately control the company or trust;

5.3.6.1.9 the source of funds or wealth are apparent and understood; and

5.3.6.1.10 the transaction is not complex or unusually large.

5.3.7 When to cease Simplified Due Diligence and commence EDD:

5.3.7.1 If suspicions of ML, TF or PF arise;

5.3.7.2 doubt whether documents obtained for identification are genuine;

5.3.7.3 doubt whether the customer is indeed the one demonstrated in the documentation;

5.3.7.4 indications that client may be transacting on behalf of another unduly (or when there are attempts to hide identification of some or all beneficial owners);

5.3.7.5 The structure or nature of the entity or relationship makes it difficult to identify the true owner. The AI to be careful of controllers or ultimate beneficial (true) owners who do not wish to be recorded on company or trust documents. They usually present high ML/TF/PF risks. For example, checks can be done via the Business and Intellectual Property Authority (BIPA), relevant registries, local authorities, Deeds offices etc., to verify certain information. If a customer seeking to do business (cash transaction) is a corporate person and the AI cannot identify the ultimate beneficial owner, the AI should:

5.3.7.5.1 keep records in writing of all the actions taken to identify the ultimate beneficial owner of the corporate;

5.3.7.5.2 take reasonable measures to verify the identity of the senior person in (or associated with) the entity responsible for managing it and keep records in

writing of the actions taken to do so, and any difficulties encountered; and

5.3.7.5.3 consider carefully the risks associated with beneficial owners as per Guidance 08 of 2023 and various other publications.

5.3.7.6 suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired;

5.3.7.7 circumstances change and the risk assessment no longer considers the customer, transactions, or location as low risk; and

5.3.7.8 Any other considerations that do not render the client or specific transaction(s) low risk.

5.3.8 ***Enhanced Due Diligence (EDD)***

5.3.8.1 It is critical that an AI has measures to identify circumstances that require escalating controls from simplified due diligence to EDD, for example identifying that a client or company/counterparty is from a high-risk jurisdiction and thus a high-risk client.

5.3.8.2 EDD applies when a client's risk profile or transaction is not low. EDD builds on simplified due diligence by taking additional measures to identify and verify customer identity, creating a client's financial profile including the source of funds and conducting additional ongoing monitoring.

5.3.8.3 The EDD in this section applies to AIs' clients who are natural persons, unless otherwise indicated (section 8 deals with legal persons and arrangements). The below

high-level summary expands on EDD measures and requirements:

5.3.8.3.1 General training for appropriate personnel on ML/TF methods and risks relevant to an AI;

5.3.8.3.2 Targeted training for appropriate personnel to increase awareness of higher risk customers or transactions;

5.3.8.3.3 Increased levels of KYC/counterparty or EDD;

5.3.8.3.4 Escalation within AI management required for approval;

5.3.8.3.5 Increased monitoring of transactions; and

5.3.8.3.6 Increased controls and frequency of review of relationships.

5.3.8.4 The same measures and controls may often address more than one of the risk criteria identified and it is not necessarily expected that AIs establish specific controls that target each criteria.

5.3.8.5 Given the above, if the AI encounters increased risks such as online platforms, cryptocurrencies/assets, or any platform on non-face-to-face engagements and limited verification opportunities, the AI must subject transactions and clients to EDD.

5.3.9 Nature and Type of EDD Measures

It is essential to keep in mind that Regulation 12 provides for EDD or obtaining additional information[1].

Type of EDD Information	Usefulness of such
Nature & location of business activities	Creating client financial profile: Helps AIs create context around magnitude of clients' earning capabilities, sources of funds etc.
Occupation or source of income	
Source of funds involved in transaction (as payment to AI) and to be invested in their business	Enables a comparison of transacting behavior in terms of funds to be used vs the financial profile of the customers.

The above should be clearly outlined in the AML/CTF/CPF policies, procedures and internal controls of the AI.

5.3.10 When to undertake EDD

5.3.10.1 As per internal risk assessment, the AI has determined that there is a high risk of ML, TF or PF associated with the client or transaction;

5.3.10.2 FIC, NAMFISA or another regulatory or law enforcement authority provides information that a particular transaction, situation or client is high risk;

5.3.10.3 a customer originates from or has ties to a high risk country;

5.3.10.4 client is evasive, has given the AI false or stolen documents to identify themselves (immediately consider

[1] the extent of which is dependent on the risk the client/transaction may pose to the AIs.

reporting this as suspicious transaction/activity to the FIC);

5.3.10.5 a customer is a PIP, an immediate family member or a close associate of a PIP;

5.3.10.6 the transaction is complex, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose;

5.3.10.7 client deposits or introduces funds into the AI and soon thereafter, without logical explanation, chooses to withdraw from transaction and asks for a transfer/refund;

5.3.10.8 client unreasonably refusing to continue with transaction when asked to avail EDD information; and

5.3.10.9 Any other considerations enhancing client or transaction risk.

5.3.11 Additional EDD Measures

In order for EDD to be duly undertaken, the AIs must do more to identify, verify and scrutinize the background and nature of clients and their relevant conduct. This is usually more extensive than simplified due diligence measures. The extent to which EDD goes beyond simplified due diligence must be clearly stated in the AI's AML/CFT/CPF policies and procedures. For example, the AI should make provision to:

5.3.11.1 obtain additional information or evidence to establish the identity from independent sources, such as supporting documentation on identity or address or electronic verification alongside manual checks;

5.3.11.2 take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified;

5.3.11.3 take actions to understand the true sources of funds;

5.3.11.4 the following measures must be taken when the transaction relates to a PIP, a family member or known close associate of a PIP:

5.3.11.4.1 obtain senior management approval before establishing a business relationship with that person;

5.3.11.4.2 take adequate steps to establish their nature of business activities, source of wealth and actual source of funds introduced; and

5.3.11.4.3 conduct enhanced ongoing monitoring if transactions are frequent or appear structured.

5.3.11.5 carry out more scrutiny of the client's known (or accessible record of) transactions/conduct and satisfy yourself that it is consistent with the client's profile;

5.3.11.6 measures which must be taken when a client/counterparty originates from, or has ties to a high-risk:

5.3.11.6.1 Obtain additional information on the customer and the customer's beneficial owner(s), if they identify themselves as associated with a high risk entity;

5.3.11.6.2 Obtain the approval of senior management for establishing or continuing the business relationship; and

5.3.11.6.3 Where possible, e.g for ongoing relationships, enhance monitoring of the business relationship by increasing the number and timing of controls applied and select patterns of transactions which require further examination.

5.3.12 CDD Related to Legal Persons, and Legal Arrangements

5.3.12.1 This section outlines considerations as per the FIA when identifying legal persons and legal arrangements. It is common cause that most stakeholders, clients or counterparties of local AIs are foreign or have foreign interests.

5.3.12.2 Local AIs are required to obtain and when need be, verify CDD and EDD information relating to such foreign clients along the guidance provided herein as per the FIA, to the extent possible.

5.3.13 Ascertainment of information: Companies and Close Corporations (CCs)

5.3.13.1 AIs are encouraged to keep in mind that CCs are the most abused entities in the advancement of ML and TF locally, as per the 2023 National Risk Assessment Update. While companies may not be as highly exposed to risks as CCs, their vulnerability is still very high. This context is helpful when considering the risk exposure of clients. It is essential that the following information is obtained, as a minimum, for CC identification purposes:

5.3.13.1.1 its registered name;

5.3.13.1.2 the name under which it conducts business in the country in which it is incorporated;

5.3.13.1.3 if the CC (or company) is incorporated outside of Namibia and conducts business in Namibia using a name other than the name specified under paragraph (a) or (b);

5.3.13.1.4 the name used in Namibia;

5.3.13.1.5 its registration number;

5.3.13.1.6 the registered address from which it operates in the country where it is incorporated, or if it operates from multiple addresses in that country the address of its head office;

5.3.13.1.7 Ultimate Beneficial Owners (UBOs): the identification particulars for natural persons who exercise effective control of the company or CC, as referred to in 3.2. The following are indications of such persons:

5.3.13.1.7.1 the executive manager/s chief executive officer and beneficial owners of the company or, in the case of a close corporation, each executive manager/s, each member/s who individually or collectively holds a controlling interest and the beneficial owners;

5.3.13.1.7.2 each natural person who purports to be authorised to establish a business

relationship or to enter into a transaction with the AIs on behalf of the CC or company; and

5.3.13.1.7.3 the identity of shareholders and their percentage ownership: from such, each natural person (member/shareholder) holding 20% or more of the voting rights at a general meeting of the company concerned or acting or purporting to act on behalf of such holder of such voting rights. AIs need to deliberately make efforts to identify any other persons, other than the stated owners/members, who may be exercising effective control or 'directing affairs' of the CC in the background, as stated in the next section below. Usually, the risk is higher when such persons are not recorded on relevant company or CC documents.

5.3.13.2 The obligation to identify beneficial ownership does not end with identifying the first level of ownership but requires reasonable steps to be taken to identify the ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

5.3.13.3 The AIs' AML/CFT/CPF policies and procedures must outline all the measures aimed at identifying the UBOs. See expanded explanations on EDD for UBOs below.

5.3.14 Ultimate Beneficial Ownership in CCs

5.3.14.1 Understanding the **ownership and control structure** of the client and gaining an understanding of the client's source of wealth and source of funds helps reduce risks of AIs being abused to advance ML/TF/PF.

5.3.14.2 The ideal expectation is that all UBO information should be verified with relevant authorities such as BIPA. At the time of publishing this guidance, BIPA is in the process of sourcing all relevant ultimate beneficial ownership (UBO) information not in its possession and uploading same on an accessible portal which can be used by Accountable Institutions for verification as per the FIA.

5.3.14.3 AIs should understand who the UBOs are from accessing CC incorporation documents. UBO includes not only interest holders/shareholders but importantly those who exercise effective control such as Executive Management. CC incorporation documents reflect Members as the UBOs.

5.3.14.4 If it becomes apparent, at any stage in the deal that other persons not listed as such, exercise control which is ideally expected of Members or owners, such person(s) should be duly identified and the AIs should understand why such person(s) is not listed on the CC incorporation documents as a Member. If there are no logical explanations, the AIs should file a STR/SAR with the FIC if ML is a possibility and TPFA or TPFT when TF or PF is suspected. The following can help indicate UBOs not listed on relevant incorporation documents:

5.3.14.4.1 profile of Members may not be consistent with the nature of such business activities (e.g the Members on incorporation documents may not appear to have an understanding of the nature of business activities they are involved in or may not

have the required capital to invest in such business); and

5.3.14.4.2 when the AIs avails services, if it becomes apparent that Members or those purporting to be such have to consult or seek permission for matters they (as Members) should be able to explain or take decisions on.

5.3.14.5 Some of the information listed below as sources for verification can also be used for CCs.

5.3.15 UBO in Companies (including section 21 companies)

5.3.15.1 BIPA currently obtains information around the directors of companies. It was found that BIPA has not been obtaining adequate information about the identification of UBOs such as shareholders. This creates challenges with verification requirements as per the FIA.

5.3.15.2 AIs need to access the company incorporation documents and request the relevant parties to the transaction to avail information such as share certificates which may confirm shareholder information. Other verification exercises can also be considered, such as enquiries with relevant AIs, Accountants and Auditors of such companies, or any other independent registries/bodies etc.

5.3.15.3 To verify the information listed above, AIs may use the below measures:

5.3.15.3.1 Financial profile of UBOs: obtaining additional information on the beneficial owner or natural person exercising effective control of the trust,

company or other legal entity (e.g. occupation, overall wealth, information available through public databases, internet), and updating more regularly the identification data of such persons and sources which can be regarded as credible;

5.3.15.3.2 obtaining information on the reasons for intended or performed transactions carried out by the company or other legal entity administered by the AIs constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);

5.3.15.3.3 details from company registries;

5.3.15.3.4 shareholder agreements or other agreements between shareholders concerning control of the legal person;

5.3.15.3.5 EDD may also include lowering the threshold of ownership (e.g. below the stated 20%), to ensure complete understanding of the control structure of the entity involved;

5.3.15.3.6 looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity; and

5.3.15.3.7 filed audited accounts/reports.

5.3.16 Nominee Directors and Shareholders

5.3.16.1 Namibia's Mutual Evaluation revealed that:

"Based on the circumstances of the Fishrot case, one area of huge risk which has not been determined to what extent it is prevalent is the abuse of shelf companies in the commission of serious crimes, including ML. BIPA did not demonstrate that after the Fishrot case, it had proceeded to take reasonable steps to determine to what extent shelf companies were being abused to facilitate commission of serious crimes.

Connected to the risks posed by shelf companies, are the risks associated with the use of nominee shareholders and nominee directors which still have not been assessed nor are they understood by the authorities. Further, the authorities did not demonstrate the measures which have been put in place to mitigate any risks associated with the use of nominee shareholders and directors, and that such risks are assessed, understood and monitored as they evolve."

5.3.16.2 Whilst the cited Fishrot case was predominantly in the fishing sector, the principal observation is around high risks associated with shelf companies and nominee directors. Such risk is equally relevant to AIs.

5.3.16.3 A nominee director is a person who has been appointed to the Board of Directors of the legal person who represents the interests and acts in accordance with instructions issued by another person, usually the UBO. A nominee shareholder is a natural or legal person who is officially recorded in the Register of shareholders (Members) of a company as the holder of a certain number of specified shares, which are held on behalf of another person who is the UBO. The shares may be held on trust or through a custodial agreement.

5.3.16.4 There are legitimate reasons for a company to have a nominee shareholder including for the settlement and safekeeping of

shares in listed companies where post-traded specialists act as nominee shareholders. However, in the AML/CFT/CPF framework, these nominee director and nominee shareholder arrangements can be misused to hide the identity of the UBOs of the legal person. There may be individuals prepared to lend their names as directors or shareholders of a legal person on behalf of another without disclosing the identity of, or from whom, they will take instructions or whom they represent. They are sometimes referred to as “strawmen” and present higher risks.

5.3.16.5 The nominee relationships described above should be disclosed to the company. AIs must subject the UBOs behind nominee directors and shareholders to EDD measures as per the FIA. AIs should have measures to detect the possibility that undisclosed nominee arrangements may exist. Policies, procedures and controls of the AIs must enable the AIs to detect undisclosed nominee arrangements. The identification of nominees should be done through the CDD process and ongoing monitoring by the AIs. The object is to request the nominee shareholder or director to avail the identity of the UBO and subjecting both nominee and UBO to EDD measures reflected above. If a nominee or relevant parties are evasive, give misleading information or do not cooperate, the AIs should promptly file a suspicious activity report with the FIC as per section 33 of the FIA.

5.3.17 CDD on Associations

5.3.17.1 The risks posed by associations cannot be ignored. Therefore, associations ought to be subjected to the necessary CDD. AIs must ascertain, in respect of an entity such as an association, a government organ/department, a representative office of a government, a non-governmental organisation (NGO), an

international organisation, an intergovernmental organisation as well as a legal person, or a foreign company or foreign close corporation –

5.3.17.1 the registered name of the entity, if so registered;

5.3.17.1.1 the office or place of business, if any, from which it operates;

5.3.17.1.2 the registration number, if any;

5.3.17.1.3 its principal activities; and

5.3.17.1.4 the full name, residential address, and one of the following, listed in the order of preference – the national identity number; the passport number; or date of birth, of the natural person purporting to be authorized (Part of Management or Director etc) to establish a business relationship or to enter into a transaction through the AIs on behalf of such entity and each beneficial owner. Persons who exercise effective control of a legal person or arrangement should be identified as per the procedures set out above on UBOs.

5.3.18 NPOs

5.3.18.1 It is generally accepted that Specified Non-Profit Organisations (NPOs) are highly vulnerable to TF. Not all NPOs are thus highly vulnerable. The 2020 National Risk Assessment (NRA) found Faith Based Organisations (FBOs) to be most vulnerable to TF domestically. Internationally, trends and typologies also indicate that charity organisations are most vulnerable to TF abuse.

5.3.18.2 This naturally also exposes Namibia to enhanced TF risks associated with charities, especially given the global reach of some. AIs are therefore reminded that FBOs and charities, being Specified NPOs, generally present increased TF risks.

5.3.18.3 Worth noting is that domestically, FBOs have also been greatly abused to advance ML activities. The AIs shall, in addition to the CDD measures outlined above, ensure that FBOs and charities are subjected to the following:

5.3.18.3.1 conduct EDD of the customer (NPO and those acting on its behalf);

5.3.18.3.2 obtain senior management's approval while establishing business relationship but before availing any services;

5.3.18.3.3 gain assurance that the business relationship may not be used for unlawful objects;

5.3.18.3.4 issue any instructions, incorporation documents etc., in the name of the relevant NPO or charity, as given in its constituent documents and not other names;

5.3.18.3.5 subject the authorized agents or representatives of the customer to comprehensive CDD as stated herein (section 8.1(g) and 8.2 above); and

5.3.18.3.6 ensure that the NPO itself, its authorized agents or representatives are not listed on any sanctions list nor affiliated directly or indirectly with listed or proscribed persons or entities, whether under the same name or a different name.

5.3.19 ***Ascertainment of Information: Partnerships***

5.3.19.1 AIs must ascertain, in respect of a partnership, the following:

5.3.19.1.1 its name, or where applicable its registered name;

5.3.19.1.2 its office or place of business, if any, or, where applicable, its registered address;

5.3.19.1.3 where applicable, its registration number; and

5.3.19.1.4 the full name, residential address (if available), and one of the following, listed in the order of preference – the national identity number; the passport number; or date of birth, of each partner, including silent partners and partners *en commandite*, beneficial owners and any other natural person who purports to be authorised to establish a business relationship or to enter into a transaction via the AIs on behalf of the partnership. Persons who exercise such effective control of a partnership, legal person or arrangement should be identified as per above. AIs must have measures to identify persons who could be 'directing or managing the affairs" of the partnership without appearing anywhere on any documents as partners or in some logically clear capacity. Beneficial owners or those controlling partnerships without being duly identified increase the ML/TF/PF risk exposure associated with partnerships.

5.3.20 Ascertainment of Information: Trusts

5.3.20.1 AIs must ascertain the following in respect of a trust:

5.3.20.1.1 its registered name, if any;

5.3.20.1.2 the registration number, if any;

5.3.20.1.3 the country where it was set up, if the trust was set up in a country other than Namibia;

5.3.20.1.4 the management company of the trust, if any;

5.3.20.1.5 the full name; the residential address, contact particulars and one of the particulars enumerated, in the order of preference, under section 6.1 above, of each natural person who purports to be authorized to establish a business relationship or to enter into a transaction or transact with the AIs on behalf of the trust; and

5.3.20.1.6 the full name, and one of the following, listed in the order of preference – national identity number; passport number; or date of birth; of the following persons –

5.3.20.1.6.1 each trustee of the trust;

5.3.20.1.6.2 each beneficiary or class of beneficiaries of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust is created;

5.3.20.1.6.3 the founder of the trust;

5.3.20.1.6.4 each person authorized to act on behalf of the trust; and

5.3.20.1.6.5 each person exercising ultimate effective control over the trust or/and each beneficial owner.

5.3.20.2 If the beneficiaries of the trust are not referred to by name in the trust deed or founding instrument in terms of which the trust is created, the AIs must follow the natural person identification procedure stated herein above to ascertain the names of the beneficiaries and document the method of determining such beneficiaries. AIs must have measures to identify persons who could be 'directing or managing the affairs' of the trust without appearing anywhere on any documents as trustees or other beneficial owner or in some logically clear capacity. Beneficial owners or those controlling trusts without being duly identified increase the ML/TF/PF risk exposure of partnerships. The information below helps identify various types of UBOs in trusts.

5.3.21 Risks with trusts

5.3.21.1 In Namibia, a trust can either be a private trust or a public charitable trust. The 2023 NRA update suggests only *inter-vivo trusts*[2] may have been abused in advancing ML. Such trusts were all (100%) Namibian initiated or founded (owned). Also, none of them are charitable trusts.

[2] Trusts created between living persons registered under the Trust Moneys Protection Act 34 of 1934.

5.3.21.2 The NRA further found that about 82% of these trusts have Namibian donors and Namibian trustees. Only 40% of the trusts involved in potential ML cases have foreign nationals listed as beneficiaries, with the majority being South African citizens. For risk mitigation purposes, *inter-vivos* trusts are high risk. With beneficial owners in trusts, Namibian and South African citizens present the highest risks.

5.3.22 Founder[3]

5.3.22.1 A founder is generally any person (or persons) by whom the trust was made. A person is a founder if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. This requires there to be an element of bounty (i.e. the founder must be intending to provide some form of benefit rather than being an independent third party transferring something to the trust for full consideration);

5.3.22.2 A founder may or may not be named in the trust deed. To combat ML/TF/PF risks as per the FIA, AIs should have policies and procedures in place to identify and verify the identity of the real economic founder;

5.3.22.3 When need be, obtain supporting information that may help establish source of funds. It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift, letter of wishes etc.; and

[3] Trust Founder or the person who establishes the trust. Sometimes referred to as the Settlor in other jurisdictions.

5.3.22.4 Where assets have been transferred to the trust from another trust, it will be necessary to obtain this information for both transferee and transferor trust.

5.3.23 Identifying natural person exercising effective control

5.3.23.1 Identifying the natural persons exercising effective control of trusts is essential in the UBO related due diligence. The below is essential in such efforts:

5.3.23.1.1 AIs providing services to the trust should have procedures in place to identify any natural person exercising effective control over the trust;

5.3.23.1.2 For these purposes "control" means a power (whether exercisable alone or jointly with another person or with the consent of another person) under the trust instrument or by law to:

5.3.23.1.2.1 dispose of or invest (other than as an investment manager or adviser) trust property;

5.3.23.1.2.2 direct, make or approve trust distributions;

5.3.23.1.2.3 vary or terminate the trust;

5.3.23.1.2.4 add or remove a person as a beneficiary or to or from a class of beneficiaries and/or; and

5.3.23.1.2.5 appoint or remove trustees.

5.3.23.1.3 AIs who administer the trust or otherwise act as trustee must, in addition, also obtain information to satisfy itself that it knows the identity of any other individual who has power to give another individual "control" over the trust; by conferring on such individual powers as described in paragraph (b) above;

5.3.23.1.4 In certain cases, the founder, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, the AIs should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to that entity.

5.3.24 Identifying beneficiaries

5.3.24.1 In the case of a beneficiary which is an entity (e.g. a charitable trust or company), the AIs should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, the AIs should satisfy itself that it has sufficient information to identify the individual beneficial owner;

5.3.24.2 Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), a AIs should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed);

5.3.24.3 Where beneficiaries are identified by reference to a class (e.g. children and issue of a person) or where beneficiaries

are minors under the law governing the trust, although an AI should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed), the AI is not obliged to obtain additional information to verify the identity of the individual beneficiaries referred to in the class unless or until the trustees determine to make a distribution to such beneficiary; and

5.3.24.4 In some trusts, named individuals only become beneficiaries on the happening of a particular contingency (e.g. on attaining a specific age or on the death of another beneficiary or the termination of the trust period). In this case, AIs are not required to obtain additional information to verify the identity of such contingent beneficiaries unless or until the contingency is satisfied or until the trustees decide to make a distribution to such a beneficiary.

5.3.25 Identifying Individual and Corporate trustees

5.3.25.1 Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT/CPF laws, regulations and other measures, the AIs should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. The AI can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the website of the body which regulates the trustee and of the regulated trustee itself); and

5.3.25.2 It is not uncommon for families to set up trust companies to act for trusts for the benefit of that family. These are

sometimes called private trust companies and may have a restricted trust license which enables them to act as trustee for a limited class of trusts. Such private trust companies are often ultimately owned by a fully regulated trust company as trustee of another trust. In such a case, the AI should satisfy itself that it understands how the private trust company operates and the identity of the directors of the private trust company and, where relevant, the owner of the private trust company. Where the private trust company is itself owned by a listed or regulated entity as described above, the AI does not need to obtain detailed information to identify the directors or controlling persons of that entity which acts as shareholder of the private trust company.

5.3.26 Extent and nature of EDD

5.3.26.1 The EDD measures explained herein are extensive but not exhaustive at all. The extent of EDD cannot be fully prescribed. Circumstances of each scenario should ideally dictate the extent of relevant EDD measures. Generally, AIs are not obliged to obtain other information about UBOs other than to enable the AI to satisfy itself of who the UBOs are or identify whether any named beneficiary who has received a distribution from a trust/legal entity is a high-risk client.

6. Consideration of other sources

6.1 The factors, indicators and measures referred to herein may not be exhaustive. AIs are advised to consider the Sectoral Risk Assessment (SRA) and NRA results. Local and international trends and typology reports issued by domestic supervisory bodies or regional and international bodies such as ESAAMLG and FATF (available on their websites) may also be considered.

7. General

7.1 These guidelines are issued without prejudice to the FIA and its complementing Regulations. The information contained in this document is intended to guide AIs on the matters highlighted herein and may not be exhaustive.

The Guidelines can be accessed at: www.namfisa.com.na.

KENNETH S. MATOMOLA
CHIEF EXECUTIVE OFFICER

HOW TO CONTACT NAMFISA:

All correspondence and enquiries must be directed to:

The CEO
NAMFISA
P.O. Box 21250
51-55 Werner List Street,
Gutenberg Plaza,
Windhoek
Republic of Namibia

Tel: +264 (61) 290 5000
Fax: +264 (61) 290 5194
amlinspections@namfisa.com.na; or info@namfisa.com.na;