Financial Intelligence Centre
Republic of Namibia

PO Box 2882
Windhoek
Namibia

Phone: + 264 61 283 5286
Fax: + 264 61 283 5918
Helpdesk@fic.na

GUIDANCE NOTE NO. 09 OF 2023

GUIDANCE ON THE IMPLEMENTATION OF RISK BASED CONTROLS AND REPORTING SUSPICIONS:

DEALERS IN PRECIOUS METALS AND STONES (DPMS)

First Issued: 12 JUNE 2023

TABLE OF CONTENTS

DEFINITIONS AND ABBREVIATIONS

"Accountable Institution (AI)" means a person or entity listed in Schedule 1 of the Act;

"Beneficial Owner"[1] 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. Care needs to be taken to identify those who control or direct operations, affairs or the management of an entity without their names being written in any formal documents of the entity as would be expected;

"Business relationship" means an arrangement between a client and an accountable or reporting 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;

"DPMS" refers to Dealers in Precious Metals and Stones.

"Enhanced Due Diligence" (EDD) means doing more than the conventional simplified due diligence or the basic CDD measures mentioned above and 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;

[1] FATF RBA on DPMSs, June 2019. file:///C:/Users/ham638/Downloads/RBA-Trust-Company-Service-Providers%20(5).pdf

"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;

"LEAs" means Law Enforcement Authorities such as the Namibian Police, Anti-Corruption Commission or NAMRA;

"ML" means Money Laundering;

"Monitoring" as defined in the FIA, for purposes of Sections 23, 24 and 25 of the Act includes -

a. the monitoring of transactions and activities carried out by the client to ensure that such transactions and activities are consistent with the knowledge that the accountable institution has of the client, the commercial or personal activities and risk profile of the client;
b. the enhanced monitoring of transactions and activities of identified high risk clients in order to timeously identify suspicious transactions and activities; and
c. the screening of the name of a client or potential client, and the names involved in transactions, against the sanctions lists issued by the United Nations Security Council under Chapter VII of the United Nations Charter; for purposes of combating money laundering, the financing of terrorism and the funding of proliferation activities.

"PEPs" means Political Exposed Persons (See FIC Guidance Note 01 of 2019);

"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 the Act;

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

“Shell company” means an incorporated company with no independent operations, significant assets, ongoing business activities or employees;

“Shelf company” means an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established;

“SNMA” refers to a Sanction Name Match Activity Report. When a potential sanctions match is detected, institutions should file a SNMA with the FIC. With effect from 17 April 2023, all sanctions name matches should be reported through SNMA reports and no longer through STRs or SARs;

“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. Reporting any other 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. Reporting any other 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;

"Without delay" means taking required actions within a few hours, as advised in Namibia's September 2022 Mutual Evaluation Report.

1. BACKGROUND

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (FIA). It is applicable to all Accountable Institutions (AIs) who carry on the business of trading in minerals as specified in Schedule 1 of the Minerals (Prospecting and Mining) Act, 1992 (Act No. 33 of 1992), with the exclusion of those dealing in petroleum products. Item 7 of Schedule 1 of the FIA identifies all such persons as Accountable Institutions and they are collectively referred to as Dealers in Precious Metals and Stones (DPMS). Importantly, all DPMS are only required to comply with the FIA when they are involved in cash transactions above the CDD threshold of NAD 5,000.00.

DPMS, like all other sectors are required to align to the Risk Based Approach (RBA) in their overall management of risks. The RBA starts with conducting risk assessments at institutional level with consideration of national and sectoral risk assessment outcomes, amongst others. This Guidance Note is the second part of two sectoral guidance documents for DPMS. While Guidance Note 08 of 2023 speaks to the execution of risk assessments at entity level, the guidance herein helps with the implementation of controls as per the RBA at entity level.

It is common cause that services offered by DPMS have been abused for ML domestically. Internationally, there are trends and typologies which suggest such abuse to advance TF/PF activities. To help mitigate ML/TF/PF risks, the Financial Intelligence Centre (FIC) issues this Guidance to help DPMS implement and enhance their internal Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) measures, at institutional level.

2. COMMENCEMENT

This Guidance Note comes into effect on **12 June 2023**.

3. WHEN TO COMPLY

Section 4 of Guidance Note 08 of 2023 explains when DPMS are required to comply with the FIA. DPMS are only required to comply with FIA obligations when:

a. engaging in any **cash transactions**; and
b. such cash transaction is equal to or **above the prescribed CDD threshold,** which at present is NAD 5,000.00. Note that this threshold is being amended, as discussed in the sectoral workshop in May 2023. Indications are that such will be increased. The final position will be duly communicated.

The above means, a DPMS only becomes an Accountable Institution with compliance obligations when participating in a cash transaction above such threshold. Naturally, for all such cash transactions, the DPMS must comply with all such obligations in the FIA as explained herein.

3.1 Transactions Outside the Compliance Scope

A FATF Study (2013)[2] explained the rationale for limiting application to cash transactions only. It is stated that for transactions not involving cash equal to or above NAD 5,000.00 and where the FIA does not require otherwise, counterparty/customer identification can be accomplished through broader industry practices and associations that already maintain comparable data to which the authorities have ready access, or by reference to government held databases (registered dealer database, VAT related database, etc.).

The above ought to reduce transaction burdens, particularly upon small and mid-size DPMS who already rely upon such industry resources to maintain security and high standards in their business practices. For example, in the diamond industry, transactions for rough diamonds are conducted within the scope of the Kimberley Process. Trading in rough diamonds and polished

[2] FATF and Egmont Study on ML and TF Through Trade in Diamonds, October 2013. Accessed via: https://egmontgroup.org/wp-rcontent/uploads/2021/09/2013_ML_TF_through_Trade_in_Diamonds_and_Precious_Stones_%E2%80%93_Joint_EG_and_FATF_Report_.pdf

diamonds can occur through bourses that are members of the World Federation of Diamond Bourses. DPMS might transparently reference these sources of counterparty/customer identification rather than recreate all identification data in multiple dealer and transaction files, causes unnecessary CDD burdens.

In similar circumstances, other regulatory programs and/or industry associations may provide similar counterparty information and assurances. Transactions with well-known, longstanding counterparties might also be identified by transparent reference to existing information of a dealer, rather than be recreated. Such streamlined counterparty identification practices should, of course, be limited to transactions with standard trading and bank payment practices that do not give rise to suspicion and concern, and do not in any case fully eliminate the need to apply risk based analysis to transactions, customers, or counterparties.

4. THE RISK BASED APPROACH

As explained in section 7 of Guidance Note 08 of 2023 and other FIC publications[3], the RBA speaks to a control system premised on a DPMS' understanding of risks it may be exposed to. Such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (mitigation plan). The key features are identifying risks, assessing such risks to understand its levels and impact, followed by a mitigation plan aligned to such risk levels. An effective control implementation is also characterised by documenting ML/TF/PF risk findings (in a risk report) and updating such when the need arises. This enables a platform through which the evolving of risks and the management thereof is tracked.

The guidance herein focuses on primary controls such as: effecting appropriate CDD[4] measures for customers; on-going and enhanced due diligence of client behaviour[5]; record keeping[6] to assist criminal investigations; monitoring[7] to detect suspicions and reporting[8].

[3] The FIC website contains Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF/PF in terms of the FIA.
[4] FIA Sections 21 and 22
[5] FIA Sections 23 and 24
[6] FIA Sections 26 and 27
[7] FIA Section 24
[8] FIA Section 33

5. AML/CFT POLICY AND PROGRAM/CONTROLS

An AML/CFT Policy, aligned to the FIA, should be approved by management and supported to ensure effective risk mitigation. Such policy should be complemented by risk based controls reflected through procedures and processes. The overall AML/CFT framework consisting of policy and control procedures requires commitment, participation and authority of owners and controlling persons (beneficial owners) to enhance its effectiveness. Further, it should be part of a culture of legal and ethical compliance that these senior management officials should inculcate to all employees, to counterparties, and to other persons associated with the business. To ensure effectiveness thereof, the nature and extent of AML/CFT controls will depend upon a number of factors including:

a. nature, scale and complexity of a dealer's business: there must be alignment between controls implemented and nature or type of risks at hand;
b. diversity of a DPMS' operations, including geographical diversity;
c. DPMS' customer, product and services profile. Where need be, some due diligence around counterparties;
d. volume and size of the transactions;
e. degree of risk associated with each area of the DPMS' operation;
f. extent to which the DPMS is involved directly with the customer or through third parties or non-face-to-face access; and
g. frequency of customer contact (either in person or by other means of communication).

The executive and middle-management, shareholders, directors etc must see to it that the above conditions exist to support the institutional AML/CFT framework.

Care needs to be taken and executive management must see to it that the risk-based AML/CFT framework is designed and driven by persons with relevant specialized expertise about a DPMS' industry, about a DPMS' particular business within that industry and about particular counterparties to does business with. It also requires knowledge of ML/TF techniques and how

they might be used within particular industry transactions and areas of operation. This implies the notion of simply drafting a policy is not helpful in ensuring effectiveness.

6. EXTENT OF CUSTOMER DUE DILIGENCE (CDD) MEASURES

The core of AML/CFT measures is centred around CDD. The nature, extent and type of CDD are thus key to the effective functioning of the AML/CFT framework. The nature and extent of CDD measures a client ought to be subjected to depends on the degree of risk that such individual client, in view of the transaction at hand, presents to the DPMS.

CDD goes beyond simply carrying out identity checks and includes creating an adequate client profile which will help the DPMS monitor such client's transacting behaviour to gain assurance that such client does not unduly expose the DPMS to risks. This is important because even people known to the DPMS may become involved in illegal activities at some point, for example, if their personal circumstances change or they face new financial pressures. The DPMS should be able to demonstrate that the extent of the CDD measures applied for each client are appropriate to mitigate risk exposure related with client.

6.1. Simplified Due Diligence

Simplified Due Diligence in principle suggests reduced or less extensive CDD measures. The below explains simplified CDD for natural persons when they access DPMS services in their personal capacities. Such is also applicable for natural persons when acting on behalf of legal persons such as Close Corporations or Companies and arrangements like Trusts and partnerships.

6.1.1 Extent of Simplified CDD

The extent to which simplified due diligence should be applied is essential to financial inclusion objectives. For this reason, such due diligence should not be extensive if all relevant considerations indicate lower risks. FIA Regulations 6 to 11 provide guidance on the minimum

identification procedures that should be followed for the various types of clients. The guidance herein builds on same. Where ML/TF risks are lower, financial institutions are allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. 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:

a. 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);
b. Reducing the frequency of customer identification updates;
c. Reducing the degree of on-going monitoring and scrutinising transactions, based on the CDD or monetary threshold; and
d. 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.

6.1.2 Ascertainment and Verification of Information

When simplified due diligence is applicable, DPMS 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):

a. Verification: full names;
b. Verification: nationality;
c. Verification: If citizen – national ID no./ passport no./date of birth;
d. Verification: Non-citizen – passport no./national ID no./date of birth;
e. Obtain: Namibia residential address for citizens OR if non-citizen, residential address in his/her country or physical address in Namibia, if any; and
f. Contact particulars.

DPMS need 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. DPMS should use other reliable means to verify identity of clients such as comparing ID documents to passports, driver's license cards, voter's cards, birth certificates and such other reliable mechanisms.

Simplified due diligence for legal persons, trusts and partnerships similarly only require obtaining basic identification information/documents of the legal person or arrangement. Basic verification of company or trust registration information is always essential. 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. Section 8 herein explains simplified due diligence and EDD measures for legal persons, trusts and partnerships.

6.1.3 Tips on simplified CDD

DPMS may:

a. use information already at hand such as client profile, without unduly requesting for more. For example, if you identified your customer as a Manager in a local shop or pensioner, you 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
b. adjust the frequency of CDD reviews when necessary, for example, when a change occurs which may suggest escalation of the low-risk behaviour.

6.1.4 Pre-requisites for Simplified Due Diligence

To apply simplified due diligence, a DPMS must ensure:

a. it is supported by internal customer risk assessment;
b. enhanced due diligence does not apply (there is no high risk in terms of client, geographic considerations, payment method etc.);

c. 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;
d. customer is not from, nor associated with a high risk country;
e. the customer is not a PEP, a family member, or a known close associate of a PEP;
f. the real customer is seen face-to-face (and not having others transact on his/her behalf unduly to evade detection);
g. customer is not dealing through a shell or shelf company;
h. 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;
i. the source of funds or wealth are transparent and understood; and
j. the transaction is not complex or unusually large.

Guidance Note 08 of 2023 avails detailed guidance on how to assess the risk level emanating from transactions or clients and equally lists indications of high risk.

6.1.5 When to cease Simplified Due Diligence and commence EDD:

a. If suspicions of ML, TF or PF arise;
b. doubt whether documents obtained for identification are genuine;
c. doubt whether the customer is indeed the one demonstrated in the documentation;
d. 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);
e. The structure or nature of the entity or relationship makes it difficult to identify the true owner. 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 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 you cannot identify the ultimate beneficial owner, you should:
    - keep records in writing of all the actions taken to identify the ultimate beneficial owner of the corporate; and

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

f. suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired. Impact of identity theft is rife especially with online activities;
g. circumstances change and your risk assessment no longer considers the customer, transactions, or location as low risk; and
h. Any other considerations that do not maintain the low risk of client or specific transaction(s).

Guidance Note 08 of 2023, in particular section 8.1.1 to 8.1.3, avails detailed guidance on transactions or clients who may present higher risks. Such should be duly considered.

7. ENHANCED DUE DILIGENCE (EDD)

It is critical that a DPMS 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. 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.

The EDD in this section apply to DPMS clients who are natural persons, unless otherwise indicated (section 8 deals with legal persons and arrangements). The section below expands on EDD measures, with the below listing a high level summary of such:

a. General training for appropriate personnel on ML/TF methods and risks relevant to DPMS;
b. Targeted training for appropriate personnel to increase awareness of higher risk customers or transactions;

c. Increased levels of KYC/counterparty or EDD;
d. Escalation within DPMS management required for approval;
e. Increased monitoring of transactions; and
f. Increased controls and frequency of review of relationships.

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

There are **significant vulnerabilities** that enhance ML/TF risks with **online trading platforms**. These are internet or web-based operations which encourage non-face-to-face dealer-client and counterparty engagements. Since such platforms have generally reduced overhead, they proclaim to sell at better rates. The FATF Study (2013) cited herein above indicated that some online based DPMS in the United States enable consumers to save up to 40% from retail prices. The registration procedures have very minimal identifying requirements, with almost not reliable mechanisms for verifications, if any. This makes trading platforms vulnerable for one to easily move very high value stones internationally without either establishing the identity of the buyer or the identity of the seller.

Given the above, if a DPMS encounters increased risks such as online trading platforms, cryptocurrencies/assets, or any such similar frameworks with non-face-to-face engagements and limited verification opportunities, DPMS must subject transactions and clients to EDD.

7.1 Nature and Type of EDD Measures

It is essential to keep in mind that identification procedures as per FIA Regulations 6 to 11 regulate obtaining the minimum identification information or simplified due diligence while Regulation 12 provides for EDD or obtaining additional information[9]. As stated above, EDD means building onto the basic identification information obtained as per simplified due diligence

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

measures in part 6 above. Such EDD information primarily includes the following and is useful in monitoring transactional behaviour:

Type of EDD Information	Usefulness of Such
Nature & location of business activities	Creating client financial profile: Helps DPMS 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 DPMS) and to be invested in their business	Enables a comparison of transacting behaviour 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 DPMS.

7.2 When to undertake EDD

i. As per internal risk assessment, a DPMS has determined that there is a high risk of ML, TF or PF associated with the client or transaction;
ii. FIC or another supervisory or law enforcement authority provides information that a particular transaction, situation or client is high risk;
iii. a customer originates from or has ties to a high risk country;
iv. client is evasive, has given the DPMS false or stolen documents to identify themselves (immediately consider reporting this as suspicious transaction/activity to the FIC);
v. a customer is a Politically Exposed Person (PEP), an immediate family member or a close associate of a PEP;
vi. the transaction is complex, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose;
vii. client deposits or introduces funds into the DPMS and soon thereafter, without logical explanation, chooses to withdraw from transaction and asks for a transfer/refund;

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

ix. Any other considerations enhancing client or transaction risk.

Guidance Note 08 of 2023 avails detailed guidance on clients, activities, transactions, delivery channels and circumstances that present high risks. Such should be duly considered.

7.3 The Additional EDD Measures

For EDD to be duly undertaken, the DPMS must do more to verify, identify and scrutinise 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 DPMS' AML/CFT/CPF policies and procedures. For example, the DPMS should make provision to:

a. 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;
b. 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 by a bank, financial institution, lawyer or notary who is competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust;
c. take actions to understand the **true sources of funds**;
d. when receiving funds for the transaction or to manage on behalf of counterparty in view of a pending deal, ensure such **funds are being introduced by the client and not another person** merely using a client to introduce funds in the deal;
e. the following measures must be taken when the transaction relates to a PEP, a family member or known close associate of a PEP (See Guidance Note 01 of 2019 on PEPs):
    - obtain **senior management approval before** establishing a business relationship with that person;

- take adequate steps to **establish their nature of business activities, source of wealth and actual source of funds** introduced; and
- conduct **enhanced ongoing monitoring** if transactions are frequent or appear structured.

f. 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 profile**;

g. measures which must be taken when a client/counterparty originates from, or has ties to a high-risk main or third country[10]:

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

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

iii. 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.

8. CDD RELATED TO LEGAL PERSONS, TRUSTS AND OTHER ARRANGEMENTS

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

8.1. Ascertainment of information: Companies and Close Corporations (CCs)

DPMS 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

[10] (a business is established in a country if they are incorporated there, is their principal place of business, or they are regulated there as a financial or credit institution; an individual is established in a country if they are resident there)

companies may not be as highly exposed to risks as CCs, their vulnerability is still very high for comfort. 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:

a) its **registered name;**
b) the **name under which it conducts business** in the country in which it is incorporated;
c) 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);
d) **the name used in Namibia**;
e) its **registration number**;
f) 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;
g) **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:
    i. 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;
    ii. each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the DPMS on behalf of the CC or company; and
    iii. 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. **DPMS 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.**

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. A DPMS' AML/CFT/CPF policies and procedures must outline all such deliberate measures aimed at identifying the UBOs. See expanded explanations on EDD for UBOs in sections 8.1.1 - 8.1.2 below.

8.1.1 Ultimate Beneficial Ownership in CCs

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 DPMS being abused to advance ML/TF/PF.

The ideal expectation is that all UBO information should be verified with relevant authorities such as Business and Intellectual Authority (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.

DPMS 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. 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 DPMS should understand why such person(s) is not listed on the CC incorporation documents as a Member. If there are no logical explanations, the DPMS 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:

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

Some of the information listed under 8.1.2 below as sources for verification can also be used for CCs.

8.1.2 UBO in Companies (including section 21 companies)

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. DPMS, like all other Accountable Institutions need to access the company incorporation documents and request of 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 DPMS, Accountants and Auditors of such companies, or any other independent registries/bodies etc.

To verify the information listed above in 8.1(g), DPMS may use the below measures:

a. **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;
b. obtaining information on the **reasons for intended or performed transactions** carried out by the company or other legal entity administered by the DPMS

constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);

c. details from **company registries**;
d. shareholder **agreements** or other agreements between shareholders concerning control of the legal person;
e. 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;
f. looking **further than simply holdings of equity shares**, to understand the **voting rights** of each party who holds an interest in the entity; and
g. filed audited accounts/reports.

8.1.3 Nominee Directors and Shareholders

The Mutual Evaluation report of Namibia observed as follows:

"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, ML included. 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 that if there are any risks associated with the use of nominee shareholders and directors, these are assessed, understood and monitored as they evolve."

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 DPMS.

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.

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.

The nominee relationships described above should be disclosed to the company and to any relevant registry. DPMS must subject the UBOs behind nominee directors and shareholders to EDD measures as per the FIA. DPMS should have measures to detect the possibility that undisclosed nominee arrangements may exist. Guidance Note 08 of 2023 avail some indicators of possible nominee arrangements. Policies, procedures and controls of the DPMS must ensure detecting undisclosed nominee arrangements will be identified and addressed as part of the CDD process and ongoing monitoring by the DPMS. The object is to request the nominee shareholder or director to avail identity of the UBO and subjecting both nominee and UBO to EDD measures as per sections 6.1, 8.1(g) and 8.1.2 above. If nominee or relevant parties are evasive, give misleading information or do not cooperate, the DPMS should file a suspicious activity report with the FIC as per section 33 of the FIA, without delay.

8.1.4 Bearer shares[11]

Similar to risks arising from nominee shareholder or directorship and shelf companies as per above, the Mutual Evaluation on Namibia[12] observed that *"the use of bearer shares is permitted in Namibia, however, no mechanisms have been implemented to guard against them being abused for ML or TF."* The risk emanating from bearer shares is further exacerbated by the lack of mechanisms to prevent the misuse of nominee shareholding and directorship.

DPMS needs to identify the use or involvement of bearer shares (especially when nominee arrangements exist) and ensure, to the extent possible, that the UBO can be subjected to EDD as the FIA. Sections 6.1, 8.1(g) and 8.1.2 above avails EDD measures which ought to be undertaken. If the holders of bearer share certificates (or those in whose custody it is merely placed), nominees or relevant parties are evasive, give misleading information or do not cooperate, the DPMS should file a suspicious activity report with FIC as per section 33 of the FIA, without delay.

8.2. Ascertainment of information: Associations and other Entities

Though DPMS do not always do business with associations or non-governmental organizations (NGOs), the risks with such entities is notable and they therefore ought to be subjected to the necessary CDD. DPMS 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 -

a) the **registered name** of the entity, if so registered;
b) the **office or place of business**, if any, from which it operates;
c) the **registration number**, if any;

[11] Simply put, bearer shares are negotiable instruments that accord ownership of a company to the person who possesses the share certificates, which are not registered and do not contain the name of the shareholder. Bearer shares permit ownership of the corporation to be transferred by simply handing over physical possession of the shares. Because ownership is never recorded in the share certificates, bearer shares are beyond the reach of the regulations and controls typically associated with registered shares.
[12] as per paragraph 405, page 120.

d) its **principal activities**; and
e) 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 authorised (Part of Management or Director etc) to establish a business relationship or to enter into a transaction through the DPMS on behalf of such entity and each beneficial owner. Persons who **exercise such effective control** of a legal person or arrangement should be identified as per section 8.1(g), 8.1.2 and 8.1.3 above.

8.2.1 NPOs

It is generally accepted that Specified Non-Profit Organisations (NPOs) are highly vulnerable to TF. Not all NPOs are thus highly vulnerable. It is thus not risk based, nor required in law to subject all NPOs to EDD. The 2020 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. This naturally also exposes Namibia to enhanced TF risks associated with charities, especially given the global reach of some. DPMS are therefore reminded that FBOs and charities, being Specified NPOs, generally present increased TF risks. Worth noting is that domestically, FBOs have also been greatly abused to advance ML activities. The DPMS shall, in addition to the CDD measures in 8.2 (and some elements in 8.1.2) above, ensure that FBOs and charities are subjected to the following:

a) conduct EDD of the customer (NPO and those acting on its behalf);
b) obtain **senior management's approval** while establishing business relationship but before availing any services;
c) gain assurance that the business relationship may **not be used for unlawful objects**;
d) 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;
e) subject the authorized agents or **representatives** of the customer to comprehensive CDD as stated herein (section 8.1(g) and 8.2 above); and

f) 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.

8.3. Ascertainment of Information: Partnerships

DPMS must ascertain, in respect of a partnership, the following:

a) its name, or where applicable its registered name;
b) its office or place of business, if any, or, where applicable, its registered address;
c) where applicable, its registration number; and
d) 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 DPMS on behalf of the partnership. Persons who **exercise such effective control** of a partnership, legal person or arrangement should be identified as per section 8.1(g) (and some elements in 8.1.2) above. **DPMS 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.**

8.4. Ascertainment of Information: Trusts

A DPMS must ascertain the following in respect of a trust:

a) its **registered name**, if any;
b) the **registration number**, if any;
c) the **country where it was set up**, if the trust was set up in a country other than Namibia;

d) the **management company of the trust**, if any;

e) 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 **authorised to establish a business relationship** or to enter into a transaction or transact with the DPMS on behalf of the trust; and

f) 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 –

- ✓ each **trustee of the trust**;
- ✓ 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;
- ✓ the **founder of the trust**;
- ✓ each **person authorised to act on behalf of the trust**; and
- ✓ each person **exercising ultimate effective control** over the trust or/and each beneficial owner.

g) 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 DPMS must follow the natural person identification procedure stated herein above [section 8.1(g) and some elements of 8.1.2] to ascertain the names of the beneficiaries and document the method of determining such beneficiaries. **DPMS 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.**

8.4.1 Risks with trusts

In Namibia, a trust can either be a private trust or a public charitable trust. The 2023 NRA update suggests only *inter-vivo trusts*[13] may have been abused in advancing ML. Such trusts were all

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

(100%) Namibian initiated or founded (owned). Also, none of them are charitable trusts. 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.

8.4.2 Founder[14]

a) 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);

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

c) 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

d) 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.

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

8.4.3 Identifying natural person exercising effective control

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

a. A DPMS providing services to the trust should have **procedures in place to identify any natural person** exercising effective control over the trust;
b. 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:
    i. dispose of or invest (other than as an investment manager or adviser) trust property;
    ii. direct, make or approve trust distributions;
    iii. vary or terminate the trust;
    iv. add or remove a person as a beneficiary or to or from a class of beneficiaries and/or; and
    v. appoint or remove trustees.

c. DPMSs 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;

d. 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 DPMS 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.

8.4.4 Identifying beneficiaries

a. In the case of a **beneficiary which is an entity** (e.g. a charitable trust or company), the DPMS 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 DPMS should satisfy itself that it has sufficient information to identify the individual beneficial owner;

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

c. 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 a DPMS should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed), the DPMS 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

d. 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, DPMS 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.

8.4.5 Identifying Individual and Corporate trustees

a. 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 DPMS should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A DPMS 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

b. 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 licence 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 DPMS 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 DPMS 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.

8.5 EXTENT AND NATURE OF EDD

The EDD measures explained herein are extensive but not exhaustive at all. The extent to which a DPMS may go in carrying out EDD cannot be fully prescribed. Circumstances of each scenario should ideally dictate the nature and extent of relevant EDD measures. Generally, DPMS are not obliged to obtain other information about UBOs other than to enable the DPMS to satisfy itself that it knows who the UBOs are or identify whether any named beneficiary or beneficiary who has received a distribution from a trust/legal entity is a high risk client (e.g PEP, sanctioned person etc.).

9. SUSPICIOUS TRANSACTION OR ACTIVITY REPORTS (“STRs/SARs”)

The primary reason for due diligence and monitoring transactions carried out by clients is to ensure that such transactions are consistent with the DPMS knowledge of the client, the client’s commercial or personal activities and risk profile. Suspicions are often detected from client

behaviour or activities outside the known client profile. Thus, understanding client profile is essential as it places the DPMS in positions to effectively detect and report suspicions when they arise. Guidance Note 08 of 2023 helps detail high risk situations, clients and activities that may be suspicious.

New report types have been introduced to enhance effectiveness. With effect from 17 April 2023, TF and PF suspicions, as well as sanctions screening name matches shall no longer be reported through STRs and SARs on goAML. TF and PF suspicions shall only be reported through TPFA and TPFT reports, as explained in section 11 herein below. Similarly, sanctions screening name matches shall only be reported through Sanctions Name Match Activity reports (SNMAs). Only ML suspicions shall be reported through conventional STRs and SARs.

STRs are reports that explain **suspicious transactions** for ML. The term suspicion is meant to be applied in its everyday, normal sense. The suspicion, as an example, could be the funds involved in the transaction are the proceeds of any crime or linked to terrorist activity. The DPMS does not need to know what sort of crime may have been committed, but one or more red flags or warning signs of potential ML, which cannot be reasonably explained by the customer, should be adequate to reach the standard of what constitutes a suspicion worth reporting to the FIC.

SARs are reports which, under normal circumstances explain potential **suspicious activity** related to clients but may not necessarily be transactions whereas STRs refer to actual suspicious transactions. For example, if a client attempts to transact and after EDD enquiries does not proceed with finalizing the transaction, and the activities or his/her behaviour around such is suspicious, then the appropriate report to file with the FIC is a SAR and not a STR (because no transaction occurred).

9.1 Practical controls

Operating frameworks or controls in the DPMS must enable the following:

a) Staff must be able to raise internal reports where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion that persons involved in the transaction could be engaged in ML, TF or PF;
b) The DPMS' AML Compliance Officer, or their appointed alternative, must consider all such internal reports. The Compliance Officer must submit the relevant report to the FIC via GoAML;
c) Such relevant report should be reported **without delay** (within a few hours of detecting the suspicion) to enhance the effectiveness of combatting activities;
d) After filing such report, the DPMS should consider all risk exposure and whether it is prudent to continue availing services to such client;
e) It is a criminal offence for anyone, following a disclosure to a Compliance Officer or to the FIC, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation. A DPMS' policies should clearly state this;
f) Important actions required:
   - ✓ enquiries made in respect of internal reports (red flags) must be recorded;
   - ✓ the reasons why a report was, or was not submitted should be recorded;
   - ✓ keep a record of any communications to or from the FIC about a suspicious transaction or activity report.

The requirement to report to the FIC should be supported by the following (within the DPMS' AML/CFT Procedures):

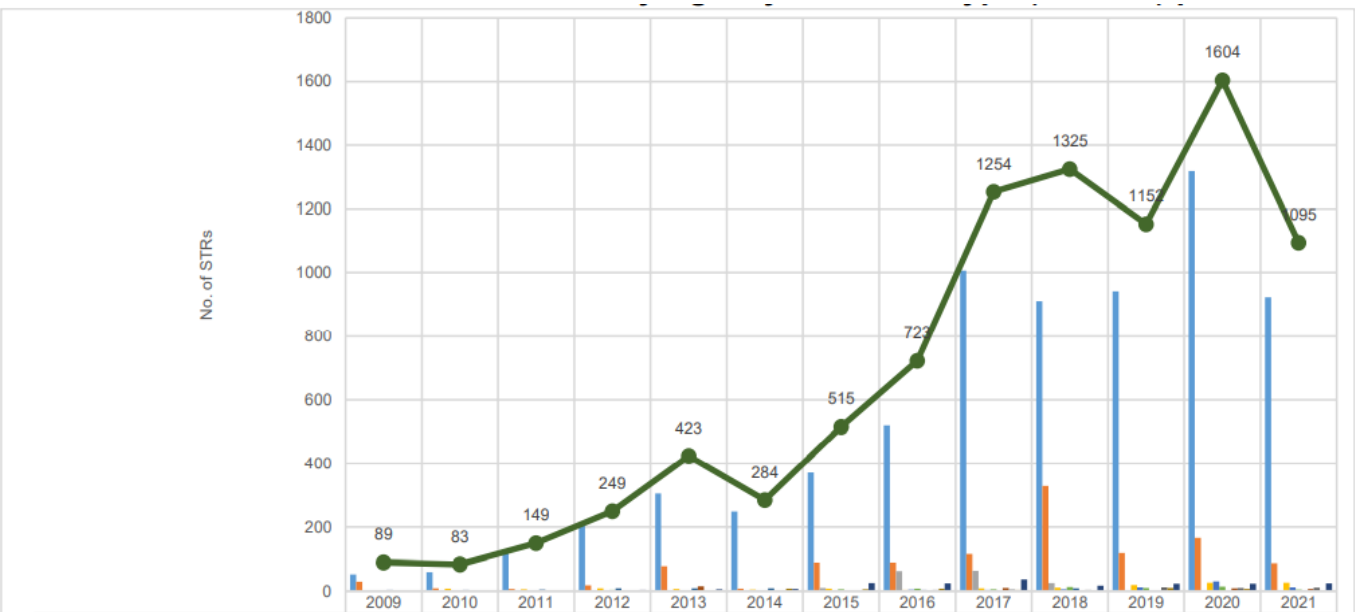
g) Staff internal reporting line to the AML Compliance Officer;
h) Confidentiality of reports, i.e. how to deal with customers, and others involved in a transaction, after an internal or external report has been made.

9.2 Sectoral Reporting Behaviour

The Mutual Evaluation on Namibia[15] found that STR and SAR reporting is not aligned to the country's risk exposure as banks tend to be the only sector detecting and reporting as per their risk exposure. This is an observation we have always known as a country. Overall, 8,945 STRs were received by the FIC since the reporting obligation commenced until 31 December 2021 (see Chart below). The banking sector submitted the most reports in such period, filing 78% (or 6,991) of reports followed by ADLAs[16] who submitted 13% (or 1,140). The high number of reports from the banking sector could be attributed to various factors, including the fact that banks appear to have the most matured AML/CFT/CPF control systems (enhanced ability to detect and report). It can also be argued that banking services are inherently exposed to a higher risk of abuse as almost all other sectors make use of the banking systems. For DPMS however, the reported volumes of STRs are insignificant. Given the vulnerability level of the sector as per the 2020 NRA, the sector's reporting volumes could be enhanced.

[15] Adopted in September 2022: Report available at: https://www.esaamlg.org/reports/MER%20of%20Namibia-September%202022.pdf

[16] Authorised Dealers in Foreign Currency with Limited Authorization often known as Bureaus de Changes.



	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Banks	52	59	129	206	305	248	371	519	1007	911	942	1319	923
ADLAs	29	9	6	18	78	7	89	89	115	329	118	166	87
Insurance/Investment Brokers	2	0	0	1	0	0	10	62	63	25	2	0	0
Legal Practitioners	1	7	5	8	6	4	7	3	8	11	19	26	26
Asset Management Companies	0	1	2	1	2	1	0	4	3	5	12	30	12
Motor Vehicle Dealers	0	1	0	3	2	1	5	7	5	13	10	14	4
Financial Intelligence Units	3	3	1	0	0	8	1	3	0	8	2	2	1
Long Term Insurance Companies	0	0	1	0	15	2	0	2	10	2	2	8	6
Unit Trust Schemes	1	1	1	0	0	0	2	3	4	3	12	10	11
Individual Persons	0	0	0	0	1	7	5	7	3	1	10	6	1
Others	1	2	1	3	5	6	25	24	36	17	23	23	24
Total	89	83	149	249	423	284	515	723	1254	1325	1152	1604	1095

Classification of STRs as received from various sectors

9.2.1 DPMS SAR Reporting

Similar to STRs, record of SARs at hand suggests DPMS can do more to enhance reporting behaviour.

10. RECORD KEEPING

10.1 What Records must be kept?

a. the identity, address and all such client identification records stated in part 6.1 herein;
b. the date, time and involved financial amounts of client's activities/transactions;
c. information relating to all relevant reports escalated to the FIC; and

d. any other information which the FIC may specify in writing.

DPMS should satisfy themselves that the records they obtain would meet the required standard as per the FIA and summarised herein.

10.2 Who must keep records?

The DPMS (as Accountable Institution) ought to keep records as per the FIA. A third party may keep records on behalf of a DPMS but the DPMS remains ultimately accountable for ensuring such records are kept as per the FIA. DPMS must engage the FIC when proposing to outsource record keeping responsibilities as per the FIA. Further, the records of two or more Accountable or Reporting Institutions that are supervised by the same supervisory body can be centralised.

10.3 Manner of Record Keeping

The records must be kept:

a. in a manner that protects the integrity of the transaction;
b. in a manner which permits reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity or civil asset forfeiture procedures. The Golden Rule with record keeping is enabling an effective reconstruction of identification or transacting activities by competent authorities.

Further, records can be kept in hard copy or electronic format as long as a paper copy can be readily produced, especially for law enforcement purposes. DPMS should maintain effective record-keeping systems to enable the FIC and other relevant authorities to access such records in a timely fashion.

10.4 Period for which records must be kept

Records that relate to the establishment of a business relationship (e.g client identification records) must be kept as long as the business relationship exists and for at least five years from

the date on which the business relationship is terminated. Records that relate to single transactions must be kept for five years from the date on which such single transaction was concluded. Records that relate to copies of reports submitted to the FIC must be kept for a period of not less than five years from date of filing such report. However, records must be kept for longer than the 5-year period if the DPMS is requested to do so by the FIC, the Office of the Prosecutor-General or by any other law enforcement body.

11. UNSC SANCTIONS SCREENING AND TARGETED FINANCIAL SANCTIONS

The object of sanctions screening is to implement Targeted Financial Sanctions (TFS) towards anyone listed by the UNSC.

DPMS are expected in terms of section 24 and Regulation 15(5)[17] of the FIA to screen clients or potential clients involved in transactions against the relevant sanctions lists issued by the United Nations Security Council (UNSC). Such screening should take place before accounts are opened or client is granted access to services, regardless of whether the client transacts below or above the CDD threshold. If the DPMS in any way makes use of third parties, middlemen or brokers/agents to facilitate or avail services, the DPMS needs to ensure that such third parties duly attend to their AML/CFT/CPF responsibilities if any reliance is placed on them. This is essential to combat TF and PF activities by ensuring designated persons, organizations or countries are identified and not unduly availed services, while their assets and funds are accordingly frozen. The term Targeted Financial Sanctions primarily speaks to **asset freezing without delay** and **prohibition** from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

[17] Accountable institution to conduct on-going and enhanced customer due diligence: (5) An accountable institution must also, in the process of monitoring, screen - (a) names of prospective clients, before acceptance of such a client; (b) names of existing clients, during the course of the business relationship; and (c) all the names involved in any transaction, against the sanctions lists issued by the United Nations Security Council under Chapter VII of the United Nations Charter for purposes of combating the financing of terrorism and the funding of proliferation activities.

Locally, the National Security Commission (NSC) is the body with statutory responsibilities in terms of the PACOTPAA[18] to propose persons or entities to the 1267/1989 Committee for designation and for proposing persons or entities to the 1988 Committee for designation. To date, the NSC has not seen the need to designate any person. DPMS are required to continue screening against relevant sanctions lists as explained above.

Screening against other designations lists such as OFAC, though not mandatorily required by domestic laws is very helpful in the overall risk management effectiveness. For any transactions or currency exchanges in USD for example, there is an inherent requirement to screen involved parties against the OFAC list. Similarly, when dealing in British Pounds or the Euro, screening against lists issued by such relevant authorities is an inherent requirement.

This section avails basic guidance on TFS. DPMS are required to further consider the detailed guidance around reporting, sanctions screening and TFS contained in Guidance Note 07 of 2023.

11.1 Effective Client Screening

In order to effectively implement Targeted Financial Sanctions (TFS), DPMS must ensure:

a. sanction screening is performed on all clients before availing them services; and

b. no services are availed to clients before the sanction screening is completed and evidence of same has been documented. Screening should **not be undertaken after** availing services or facilitating transactions. Prior screening **enables proactive detection of sanctioned persons.** If such sanctioned persons are detected, such should not be granted access to any services at all and their attempted transactions should be reported to the FIC promptly and without delay, while the assets (or funds) involved are frozen or further transactions prohibited, as per the FIA and PACOTPAA. **In**

[18] Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014).

practice, policies and operating procedures therefore need to ensure clients are allowed to at least attempt the transaction to ensure due identification, which will enable effective screening and, if client is listed, eventual freezing of the funds which the client attempted to transact with, followed by complete prohibition to transact any further and reporting.

The following databases of the DPMS must be included in the screening process:

a. Existing customer databases. All systems (if any) containing customer data and transactions need to be mapped to the screening system to ensure full compliance;
b. Potential customers before conducting any transactions or entering a business relationship with any person;
c. Names of parties to any transactions (e.g., buyers and sellers; any party or beneficial owner of an entity or trust to be registered etc.[19]);
d. Ultimate beneficial owners, both natural and legal;
e. Names of individuals, entities, or groups with direct or indirect relationships with them; and
f. Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

11.2 Where to find the updated Sanctions Lists?

As mentioned above, DPMS, like all other Accountable and Reporting Institutions are required to access lists of sanctioned persons and screen their clients against such lists before establishing a business relationship and whenever the sanctions lists are updated. Domestically, at the time of issuing this Guidance, the NSC has not designated nor listed any persons yet. At an international level however, the information on designated individuals, entities or groups in

[19] Other sectors such as Banks need to include agents, freight forwarders, vessels etc.

the Sanctions Lists is subject to change. The most recently updated sanctions list of the UNSC[20] can be found on the UNSC website or via the following link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

11.3 Targeted Financial Sanctions (TFS)

As mentioned above, TFS includes **asset freezing without delay** and **prohibition** from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

11.3.1 Asset freezing without delay

In terms of international standards, without delay means **within a matter of hours**. Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. It includes:

a. The freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access; and
b. The freezing of economic resources. Also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, by selling or mortgaging them.

Examples of freezing:

i. ***Financial Institutions:*** *a freezing measure can be suspending listed client's access to bank accounts which have funds or blocking transactions which can deplete such;*
ii. ***DNFBPs like DPMS, Accountants and law firms:*** *a freezing measure can be holding onto any funds, assets the client may have paid/deposited with the DPMS/Accountant/Law Firm (including payment for services). Could be holding onto or blocking the export/transfer of precious metals and stones that client has paid for, bid for or has provided guarantees for in a sale etc.; and*

[20] The UNSC has a UN Consolidated List of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC.

iii. ***VASPs[21]:*** *a freezing measure can be holding onto the funds/value from client (e.g in VASP's custody) to trade and transfer virtual assets, despite client having asked for same.*

11.3.2 Prohibition

The principle is prohibition from making funds or other assets or services available. This means the prohibition to provide funds or other assets to or render financial or other services to any designated individual, entity, or group.

Examples of prohibition:

i. ***Financial institutions:*** *prohibition from offering banking or transactional services;*

ii. ***DNFBPs, like DPMS, Accountants and law firms:*** *prohibiting the provision of any services, such as stopping the shipping of precious stones and metals bought by client or as agreed with client, ceasing services to transfer entity ownership, shares etc.;*

iii. ***VASPs:*** *prohibition from the provision of any services, including but not limited to trading and transferring virtual assets.*

11.3.3 Object of freezing and prohibition

Note however that even when freezing measures are taken or enacted, there should be no restrictions on client introducing or depositing more funds with the DPMS (e.g paying further funds towards a deal), while the making of such additional payments are still possible. Just ensure such are received but not further depleted or released in any way. As long as the service which the listed client so desires cannot be finalised for them, prohibition and asset freezing requirements will be met on condition whatever has already been frozen is not further depleted. The object remains to deprive listed/designated/proscribed persons from as much funds/assets as possible so they can be denied access to resources which may be used to fund terrorist or proliferation activities. This is the essence or primary goal of TFS measures. DPMS need to consider appropriate implementation thereof given the circumstances they may find themselves in, with each transaction/client.

[21] Virtual Asset Service Providers such as those dealing in Bitcoin etc.

11.4 Reporting Possible Matches

The mechanism to report any freezing or suspension measures taken upon identifying confirmed or potential matches is through the goAML platform. The use of the goAML platform for TFS reporting purposes eases the burden of reporting and avails the necessary confidentiality required for this sensitive process. As mentioned above, institutions should no longer report sanctions screening matches, TF or PF suspicions via STRs or SARs. New report types have been created to enhance effectiveness, especially around TFS measures. From 17 April 2023, sanctions screening matches as well as TF and PF suspicions or transactions should be reported as per below:

Reportable Activity or Transaction	Type of Report
Detection of a possible **sanctions screening match.**	SNMA - Sanction Name Match Activity report
Reporting any other **Activity** (or attempted transaction which was not completed) which may point to, or be linked to potential terrorism, TF or PF.	TPFA - Terrorist & Proliferation Financing Activity report
Reporting any other **Transaction** (actual transacting) which may point to, or be linked to potential terrorism, TF or PF.	TPFT- Terrorist & Proliferation Financing Transaction report

The following information must be shared when submitting a SNMA report:

a. The full name of the ‘confirmed match’. Attach ID documents of the ‘confirmed match’, such as passport or other ID documents for individuals, and relevant legal person incorporation documents such as CC incorporation forms, articles of association, trust establishing documents etc.; and
b. Amount of funds or other assets frozen (e.g., value of real estate, value of funds in bank accounts, value of transactions, value of securities, etc.). Attach proof documents such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc., if such are at hand.

When a possible match is reported to the FIC, the FIC or such relevant competent authorities will direct all activities related to the frozen assets or funds. The DPMS may not release frozen assets or do anything related to such assets without being instructed to do so.

11.5 Study Publications on TF Indicators, Trends and Typologies

DPMS are encouraged to read FIC and other relevant publications on guidance and TF indicators. TF detection efforts at entity level, absent of specific national/international guidance and typologies may be limited and inadequate. Such is likely to be based on monitoring that only focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available[22]. The ability of DPMS to detect and identify potential TF red flags or suspicions is enhanced with guidance on TF typologies, risk assessment outcomes or acting on specific intelligence provided by authorities. The sector is therefore encouraged to duly consider the TF indicators in Guidance 08 of 2023, along with other FIC publications such as risk assessments and relevant TF related reports on the FIC website[23] and other sources[24].

12. ROLE OF AML COMPLIANCE OFFICER

The effectiveness of the AML Compliance Officer[25] usually impacts a DPMS' overall risk management effectiveness. The AML/CFT/CPF controls within a DPMS should therefore ensure the Compliance Officer is placed in a position to execute his/her FIA responsibilities as required. Such responsibilities primarily include ensuring that:

[22] Many of which are indicative of the same techniques as are used for ML.
[23] https://www.fic.na/ see under ML/TF/PF Risk Assessments, Trends and Typologies, Publications, amongst others.
[24] FATF and Egmont Study, Oct 2013. Also see: FATF Guidance on RBA for Dealers in Precious Metals and Stones, June 2008. Accessed via: file:///C:/Users/ham638/Downloads/RBA%20for%20Dealers%20in%20Precious%20Metal%20and%20Stones%20(2).pdf & ESAAMLG Study in illicit Dealings in Gold, Diamond, Rubies and Associated Money Laundering and Terrorist Financing in the ESAAMLG Region, March 2022. Accessed at: https://www.esaamlg.org/reports/ILLICIT_DEALING_SEPT_2022.pdf
FATF Guidance, June 2008.
[25] Appointed as per Section 39 of the FIA.

a. internal ML/TF/PF risk assessments are undertaken and results thereof duly implemented. Periodically, such risk assessments are duly revised or updated in line with SRAs, NRAs, typology reports locally and internationally;
b. the AML/CFT/CPF Controls (policies, procedures etc) are at all times aligned to risk levels;
c. front-line staff (staff members who directly deal with customers) are duly trained on CDD measures as per the FIA;
d. he/she undertakes monitoring transactions, e.g. routine or spot checks based on risks;
e. measures to internally detect and escalate[26] potential ML/TF/PF indicators or red flags are prudent and enable the required level of confidentiality;
f. he/she files relevant reports to the FIC, without delay;
g. he/she regularly reports to senior management about AML/CFT performance; and
h. he/she attends to any other activities necessary to enhance FIA compliance.

Compliance Officers ought to have adequate managerial authority and capacity within the DPMS operations to lead compliance activities, as per the FIA. With very small or one-man DPMS, Accountants or Law Firms, the single employee/individual (or one of them in management) has a responsibility to attend to all the responsibilities of a Compliance Officer duly. Depending on the size of the DPMS, volume of transactions, overall risk etc., regard has to be had with the DPMS' ability to duly attend to all responsibilities as per the FIA. Such factors should guide resourcing of a Compliance function.

13. GENERAL

This Guidance may contain statements of policy which reflect the FIC's administration of the legislation in carrying out its statutory functions. This guidance is issued without prejudice to the FIA and its complementing Regulations. The information contained herein is intended to only provide a summary on these matters and is not intended to be comprehensively exhaustive.

[26] To the Compliance Officer for analysis and decision on whether to report same to the FIC.

14. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of Accountable and Reporting Institutions. Should an institution fail to adhere to the guidance provided herein, it will be such institution's responsibility to demonstrate alternative risk management controls implemented which are effective to the satisfaction of the FIC as supervisory authority.

15. GENERAL

The Guidance Note can be accessed at www.fic.na

DATE ISSUED: 12 JUNE 2023
DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

FIC CONTACT DETAILS

All correspondence and enquiries must be directed to:
The Director, Financial Intelligence Centre
P.O. Box 2882
No. 71 Robert Mugabe Avenue, Windhoek
helpdesk@fic.na