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. 11 OF 2023

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

## VIRTUAL ASSETS SERVICE PROVIDERS (VASPs) AND INITIAL TOKEN OFFERINGS (ITOs) PROVIDERS

## First Issued: 30 JUNE 2023

**TABLE OF CONTENTS**

## A. DEFINITIONS AND ABBREVIATIONS

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

**"Administrator"** is a person or entity engaged as a business in issuing (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to redeem (withdraw from circulation) the virtual currency;

**"Anonymiser"** (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. [Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)];

**"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. 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;

**"Cold Storage"** refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft. It is commonly referred to as an unhosted wallet;

**"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;

**“Dark Wallet”** is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road;

**“Distributed Ledger Technology” (DLT)** is the technological infrastructure and protocols that allow simultaneous access, validation, and record updating across a networked database. DLT is the technology blockchains are created from, and the infrastructure allows users to view any changes and who made them, reduces the need to audit data, ensures data is reliable, and only provides access to those that need it;

**“Decentralized finance (or DeFi)”** uses emerging technology to remove third parties and centralized institutions from financial transactions. Functions by enabling direct or P2P engagements by eliminating intermediaries and thus allowing people, merchants, and businesses to conduct financial transactions through emerging technology. Through peer-to-peer financial networks, DeFi uses security protocols, connectivity, software, and hardware advancements. The components of DeFi are stablecoins, software, and hardware that enables the development of applications;

**“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;

**"FATF"** means the Financial Action Task Force. The FATF is an organization that develops policies to prevent and combat money laundering, terrorist and proliferation financing activities. Like most countries, Namibia’s AML/CFT/CPF regime is aligned to the FATF standards;

**“FIA”** refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012);

**“FIC”** means the Financial Intelligence Centre;

**"Hot Storage"** refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage. It is hosted by a service provider or entities that provide custodial services;

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

**"ML"** means Money Laundering;

**"Mixer (laundry service, tumbler)**" is a type of anonymizer that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address;

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

- 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;
- the enhanced monitoring of transactions and activities of identified high risk clients in order to timeously identify suspicious transactions and activities; and
- 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;

**"Tor"** (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network;

**"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;

**"Virtual Asset (VA)"** VAs must be digital and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes. That is, they cannot be merely digital representations of fiat currencies, securities and other financial assets without an inherent ability themselves to be electronically traded or transferred and the possibility to be used for payment or investment purposes;

**"VASPs"** refers to Virtual Assets Service Providers. A VASP is a person who carries out one or more of the five categories of activity or operation described in the VASP definition below (i.e "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an issuer's offer and/or sale")

**"Virtual Asset Service Provider (VASP)"** The definition of a VASP is broadly defined by the Financial Action Task Force (FATF), owing to the nature of virtual asset operations. Along such guidance, Namibia has adopted[1] a functional approach and applies the following concepts underlying the definition to determine whether an entity is undertaking the functions of a VASP. A VASP is any natural or legal person who, as a business, conducts one or more of the following activities or operations for, or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets;

[1] the proposed FIA amendments and both FIC Directives 01 and 02 of 2021.

iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

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

## B. UNDERSTANDING DIFFERENT TYPES OF VA ACTIVITIES

| VASP Types | Description of virtual asset activities |
|---|---|
| **Virtual Asset Exchanges** | Providing a digital online platform facilitating virtual asset transfers and exchanges. Exchanges may occur between one or more forms of virtual assets, or between virtual assets and fiat currency.<br><br>Issuing own virtual assets in order to facilitate virtual asset transfers and exchanges |
| **Virtual Asset Wallet Providers** | Providing storage for virtual assets or fiat currency on behalf of others and then facilitating exchanges or transfers between one or more virtual assets, or between virtual assets and fiat currency. |
| **Virtual Asset Broking** | Arranging transactions involving virtual assets, or involving virtual assets and fiat currency. |
| **Initial Token/Coin Offering (ITOs/ICOs) Providers** | Issuing and selling virtual assets to the public;<br><br>May involve participating in and providing financial services relating to the ICO. |
| **Providing investment opportunities in virtual assets** | Providing an investment vehicle enabling investment in/ purchase of virtual assets (i.e. via a managed investment scheme or a derivatives issuer providing virtual asset options, or via a private equity vehicle that invests in virtual assets). |

## C. TYPICAL VASPs AND THEIR SERVICES

| | | |
|---|---|---|
| Virtual Asset Wallet Providers | Custodial | Hot Wallet |
| | Non-custodial | Cold Wallet |
| Virtual Asset Exchanges | Transfer Services | P2P |
| | | P2B |
| | Conversion Services | Fiat-to-Virtual |
| | | Virtual-to-Fiat |
| | | Virtual-to-Virtual |
| Virtual Asset Broking/Payment Processing | Payment Gateway | ATMs |
| | | Merchants |
| | | Cards |
| Virtual Asset Management Providers | Funds | Fund Management |
| | | Fund Distribution |
| | | Compliance, Audit, and Risk Management |
| Initial Coin Offering Providers | Fund raising | Fiat-to-Virtual |
| | | Virtual-to-Virtual |
| | Investment | Development of Product and Services |
| | Other offerings | Security Token Offerings (STOs) |
| | | Initial Exchange Offerings (IEOs) |
| Virtual Asset Investment Providers | Trading Platforms | Investment into VA-related commercial activities |
| | | Non-Security Tokens and Hybrid Trading Activities |
| | | Stablecoins |
| | Emerging Products | Crypto Escrow Service |
| | | Crypto-Custodian Services |
| Validators/Miners/Administrators | Proof of Work | Fees<br>New Assets |

## D. THE FOUR MAIN CATEGORIES OF TOKENS

Tokens are digital representations of VAs or rights and obligations, created, stored, and capable of being transferred electronically using DLT or similar technology and sometimes conferred during a sale to raise capital for a business or organization. This is ordinarily achieved through an initial coin offering or security token offering. Tokens are often bought in exchange for existing VAs, such as bitcoin or Ether. Where there is sufficient demand, some tokens are traded on a secondary market (VA exchange platforms) and, consequently, start to carry characteristics of a payment token or VA such as bitcoin rather than to a utility or security token.

| | |
|---|---|
| Payment/exchange-type tokens such as bitcoin and Litecoin | Typically, they do not provide rights (as is the case for investment or utility tokens) but are used as a means of exchange (for example, to enable the buying or selling of a good provided by someone other than the issuer of the token) or for investment purposes or the storage of value. These are largely performed functions similar to a currency.<br><br>“Stablecoins” are a relatively new form of payment/exchange token that is typically asset-backed (by physical collateral or crypto-assets) or is in the form of algorithmic stablecoins (with algorithms being used as a way to stabilize the volatility in the value of the token). |
| Investment/security-type tokens, such as bankera | These tokens typically provide rights (for example, in the form of ownership rights and/or entitlements similar to dividends), such as a share in future company earnings or future capital flows, which makes these tokens analogous to equities, bonds, or derivatives in terms of their economic function. Tokens that enable physical assets to be traded on the blockchain also fall into this category.<br><br>This type of token can be digital; for example, a digital Asset Token is a token that entitles the holder to the smart contract-initiated payout from an escrow account upon the occurrence of an event. In trade finance, a letter of credit paid to the token holder upon a debtor’s default would be a digital Asset Token. |

| | |
|---|---|
| Utility tokens used to access applications or services | Utility tokens typically enable access to a specific product or service often provided using a DLT platform but are not accepted as a means of payment for other products or services. For example, in the context of cloud services, a token may be issued to facilitate access. |
| Hybrid tokens | There are a wide variety of virtual assets with features spanning more than one of the categories identified previously. For example, Ether has the characteristics of an asset token but is also accepted by some persons to exchange goods external to the Ethereum blockchain and as a utility in granting holders access to the computation power of the Ethereum Virtual Machine. |

## 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 are collectively referred to as Virtual Assets Service Providers (VASPs) and those engaged in Initial Token Offerings (ITOs).

VASPs, like all other Accountable Institutions 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 VASPs. While Guidance Note 10 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. These Guidance Notes are issued while the FIA amendments and VAITOs Bill are on the verge of being passed in parliament, to enable expansion of the AML/CFT and prudential supervisory frameworks on VASPs and ITOs.

It is common cause that services offered by VASPs 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 VASPs 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 **03 July 2023**.

## 3. SCOPE OF VASP COMPLIANCE

A P2P DeFi transaction is where two parties agree to exchange cryptocurrency for goods or services without a third party involved. In DeFi, P2P can meet an individual's loan needs, and an algorithm would match peers that agree on the lender's terms, and a loan is issued. Payments from P2P are made via a decentralized application, or dApp, and follow the same process in the blockchain.[2]

VASP activities that are covered are as defined herein under the definitions section and the FIA VAITOs. It is however important to note that some activities in the VA space, such as P2P and DeFis are excluded from the FIA compliance framework as explained below:

a. **P2P transactions:** These transactions are conducted without using the involvement of VASPs or other conventional Accountable Institution, such as VA transfers between two unhosted wallets. P2P transactions are not explicitly subject to the FIA (in line with the FATF Recommendations), but the obligations are on the intermediary between the individual and the financial system. Globally (including the FATF), it is accepted that P2P transactions could pose heightened ML/TF risks[3], as they can potentially be used to avoid AML/CFT controls imposed on VASPs and conventional Accountable Institutions;

b. **Decentralized Finance (DeFi):** The DeFi application is not a VASP but the creators, owners, and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements may be VASPs should they avail services within the VASP

[2] Why are DeFis attractive? Using DeFi allows for:
   a. **Accessibility:** Anyone with an internet connection can access a DeFi platform and transactions occur without any geographic restriction;
   b. **Low fees and high-interest rates:** DeFi enables any two parties to directly negotiate interest rates and lend money via DeFi networks; and
   c. **Security and Transparency:** Smart contracts published on a blockchain and records of completed transactions are available for anyone to review but do not reveal your identity. Blockchains are immutable, meaning they cannot be changed.

[3] The FATF latest guidance acknowledges that unhosted wallets lack VASP oversight, thus bringing certain risks by not having an obliged entity as an intermediary. Still, the FATF explains that regulators need to study the nature and extent of the risks around unhosted wallets in their jurisdictions and manage those risks accordingly. The proposed FIA amendments are accordingly aligned.

definition. Even if those arrangements seem decentralized, they may still fall under the FATF definition of a VASP when they are providing or actively facilitating VASP services;

c. **Validators/miners:** Though in some countries, miners or validators are classified as VASPs, this is not the case in Namibia unless they avail the defined VASP services to others. Some would classify validators/miners as VASPs when the user engages as a business in issuing (putting into circulation) a VA and redeeming (withdrawing from circulation) such VA. A user is a person who obtains VAs to purchase goods or services on his or her own behalf. To the extent that a user mines the VA and uses the VA solely for the user's own purposes and not for the benefit of another, the user is not a VASP because these activities involve neither "acceptance" nor "transmission" of the convertible VAs and are not the transmission of funds. This is the reason for such exclusion as per FIA amendments.

## 4. WHEN TO COMPLY

VASPs are required to comply with FIA obligations when facilitating transactions equal to or **above the prescribed CDD threshold,** which at present is **NAD 5,000.00**. At the time of issuing this Guidance, national review activities are considering increasing such threshold. The final position will be communicated with all sectors when taken.

## 5. THE RISK BASED APPROACH

As explained in section 7 of Guidance Note 10 of 2023 and other FIC publications[4], the RBA speaks to a control system premised on a VASPs' 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

[4] 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.

(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[5] measures for customers; monitoring: on-going and enhanced due diligence of client behaviour[6]; record keeping[7] to assist criminal investigations; monitoring[8] to detect suspicions and reporting[9].

## 6. 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 VASP's business: there must be alignment between controls implemented and nature or type of risks at hand;
b. diversity of a VASPs' operations, including geographical diversity;
c. VASPs' 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 VASPs' operation;
f. extent to which the VASPS is involved directly with the customer or through third parties or non-face-to-face access; and

[5] FIA Sections 21 and 22
[6] FIA Sections 23 and 24
[7] FIA Sections 26 and 27
[8] FIA Section 24
[9] FIA Section 33

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 VASPs' industry, about a VASPs' particular business within that industry and about particular counterparties the VASP is doing 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.

## 7. 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 risks that such individual client, in view of the transaction at hand, presents to the VASP.

CDD goes beyond simply carrying out identity checks and includes creating an adequate client profile which will help the VASP monitor such client's transacting behaviour to gain assurance that such client does not unduly expose the VASP to risks. This is important because even people known to the VASP may become involved in illegal activities at some point, for example, if their personal circumstances change or they face new financial pressures. The VASPs 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.

### 7.1 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 VASP 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.

### 7.1.1 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. Current 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 transaction value rises 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.

### 7.1.2 Ascertainment and Verification of Information

When simplified due diligence is applicable, VASPs 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;
f. Contact particulars;
g. Such additional, non-core identity information, which VASPs are recommended to collect, could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; VA wallet addresses; and transaction hashes; and
h. In addition to the above:
   a VASP should ensure screening its customer's and counterparty's wallet addresses with the aim of understanding their links or engagements with high risk elements/threats such as mixers.

Where there is a suspicion of ML/TF, or when the VASP doubts the veracity or adequacy of previously obtained customer identification data, VASPs should conduct the necessary CDD, regardless of any CDD threshold.

VASPs 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. VASPS 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.

### 7.1.3 Tips on simplified CDD

VASPs 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.

### 7.1.4 Pre-requisites for Simplified Due Diligence

To apply simplified due diligence, a VASPs 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 10 of 2023 avails detailed guidance on how to assess the risk level emanating from transactions or clients and equally lists indications of high risk.

### 7.1.5 When to cease Simplified Due Diligence and commence EDD:

i. If suspicions of ML, TF or PF arise;
ii. doubt whether documents obtained for identification are genuine;
iii. doubt whether the customer is indeed the one demonstrated in the documentation;
iv. 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);
v. 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 10 of 2023 and various other publications.
vi. suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired. Impact of identity theft is rife especially with online activities;
vii. circumstances change and your risk assessment no longer considers the customer, transactions, or location as low risk; and
viii. Any other considerations that do not maintain the low risk of client or specific transaction(s).

Guidance Note 10 of 2023, in particular sections 8.1.1 to 8.1.3, avails detailed guidance on transactions or clients who may present higher risks. Such should be duly considered.

## 8. ENHANCED DUE DILIGENCE (EDD)

**It is critical that a VASPs 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 VASPs 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 VASPS;
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 VASPS 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 VASPS 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 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 VAs internationally without either establishing the identity of the buyer or the identity of the seller.

Given the above, if a VASP 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, VASPs must subject transactions and clients to EDD.

### 8.1 Monitoring: Nature and Type of CDD/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[10]. As stated above, EDD means building onto the basic identification information obtained as per simplified due diligence 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 VASPs 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 VASPs) 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 VASP as the foundation for monitoring activities.

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

### 8.1.1 Monitoring framework

Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. Where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions, and flagged transactions should go through human/expert analysis to determine if such transactions are suspicious. VASPs should understand their own internal policies/controls, verify their integrity on a regular basis, and check that they account for the identified ML/TF risks associated with VAs, products or services or VA financial activities.

In essence, the above suggests VASPs, like all other Accountable Institutions should adjust the extent and depth of their monitoring in line with their institutional risk assessment and their individual customer risk profiles including the type of transactions that they allow (e.g. transactions to/from unhosted wallets). If a VASP assess/finds the risks of transfers to/from unhosted wallets or other higher risks to be unacceptably high, the VASP may consider choosing to subject such wallets to enhanced monitoring or to limit or not accept transactions with such wallets. Enhanced monitoring should be required for higher-risk situations and extend beyond the immediate transaction between the VASP or its customer or counterparty. The adequacy of monitoring systems and the factors that lead VASPs to adjust the level of monitoring should be reviewed regularly for continued relevance to the internal AML/CFT risk exposure.

Monitoring under the RBA allows VASPs to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. VASPs should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers, where applicable. The criteria applied to decide the frequency and intensity of the monitoring of different customer (or even VA product) segments should also be transparent. To this end, VASPs and should properly document, retain and communicate to the FIC the results of their monitoring as well as any queries raised and resolved.

## 8.2 When to undertake EDD

i. As per internal risk assessment, a VASP 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 VASP 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 with the VASP 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 10 of 2023 avails detailed guidance on clients, activities, transactions, delivery channels and circumstances that present high risks. Such should be duly considered.

## 8.3 The Additional EDD Measures

For EDD to be duly undertaken, the VASP 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 VASP's AML/CFT/CPF policies and procedures. For example, the VASP should make provision to:

i. 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;

ii. identify and monitor **high risk wallet addresses**: If a VASP uncovers VA addresses (wallets) that it has decided not to establish or continue business relations with or transact with due to suspicions of ML/TF, the VASP should consider making availing its list of "blacklisted wallet addresses to the FIC," subject to the FIA. A VASP should **screen its customer's and counterparty's wallet addresses** against such available blacklisted wallet addresses as part of its ongoing monitoring. A VASP should make its own risk-based assessment and determine whether additional mitigating or preventive actions are warranted if there is a positive hit;

iii. 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;

iv. take actions to understand the **true sources of funds**;

v. 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;

vi. 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.

vii. 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**;

viii. measures which must be taken when a client/counterparty originates from, or has ties to a high-risk main or third country[11]:

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.

## 8.4 Compliance with the Travel Rule

### 8.4.1 What is the Travel Rule?

The FIA amendments are aligned to the so-called FATF Travel Rule. The Travel Rule requires financial institutions and VASPs to collect personal data on participants exceeding the prescribed threshold in transaction value. VASPs must comply with such rule which includes the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities. The requirements apply to both VASPs and other Accountable Institutions such as banks when they send or receive VA transfers on behalf of a customer.

VASPs are required to ensure that all remittances facilitated for their clients are always accompanied by the following:

a. Required and accurate originator information:

i. the name of the originator;

[11] (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)

ii. the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and
iii. the originator's address, or national identity number, or customer identification number, or date and place of birth.

b. Required beneficiary information:
   i. the name of the beneficiary; and
   ii. the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

Further it is essential that VASPs submit the required information immediately—that is, simultaneously or concurrent with the transfer itself—particularly given the cross-border nature, global reach, and transaction speed of VA activities.

### 8.4.2 Who are subject to FATF Travel Rule?

Currently, this FATF Recommendation only covers VASP-to-VASP transfers, while VASP-to-private wallets are not yet part of this rule. However, to enhance risk mitigation, VASPs and Accountable Institutions may undertake transfers to non-obliged entities (i.e., unhosted wallets). In such circumstances, a VASP should obtain the required originator and beneficiary information from their customer, because they cannot obtain the relevant information from another VASP. Such transfers would fall within scope of the VASP's broader AML/CFT obligations, such as transaction monitoring and targeted financial sanctions compliance.

### 8.4.3 Why is it important?

Since the intention of the FATF Travel Rule is to share information between VASPs, its aim is enable the ease with which these entities easily:

a. Identify and prevent payments to sanctioned individuals, entities, countries, and wallet addresses;
b. Block terrorist financing especially with the use of VASP services;
c. Detect suspicious users; and
d. Prevent money laundering and avoid fraud.

### 8.4.4 P2P risk exposure: The world is responding

It goes without saying that P2P transactions are still out of scope, however with the 2021/22 FATF updates, the previously proposed threshold of 1,000 EUR[12] for VASP transactions have been removed. This means the Namibian CDD threshold is also done away with. Traceability is now required for all transactions regardless of amount, as an international policy position to which Namibia must align. Further, when conducting transactions with unhosted wallets, VASPs will soon be required to verify the identity of the respective beneficial owner, and VASPs report incoming transactions from unhosted wallets above given thresholds to the FIC. This updated position suggests the direction the FATF is headed in terms of addressing risks with P2P transactions.

VASPs should have mechanisms to deliberately identify unhosted wallets or risks posed by VA transfers to/from unhosted wallets and related P2P transactions. Such transactions may be attractive to criminals due to anonymity, the lack of limits on portability, mobility, transaction speed, and usability. Therefore, VASPs should collect data on their unhosted wallet transfers, monitor and assess that information as necessary to determine to what extent a transaction is within their risk appetite, and the appropriate risk-based controls to apply to such a transaction/individual customer, and to meet STR obligations. VASPs that are not yet licensed/registered and supervised for AML/CFT purposes pose a higher risk as they may be based in a jurisdiction that has not yet implemented the FATF Standards for VAs/VASPs.

In practice, VASPs must assess the financial crime risks in all transactions with unhosted wallets by, amongst others, identifying the source of funds and determining appropriate due diligence

[12] Namibia's would thus have been the current NAD 5,000.00 threshold until amended.

measures. VASPs must take steps to ensure the unhosted wallet is controlled by their customer for transactions over the minimum identification threshold.

In terms of best practices, the United Kingdom (UK) has updates on this matter. For transfers below their threshold, only names and accounts (of both parties) are required by the Authorities (HMT) while for transfers where all service providers are within the UK, only the accounts of the parties are needed. On the other hand, for unhosted (or cold) wallets, such information only need to be collected for high-risk transfers. A 12-month grace period from 1 September 2022 to 1 September 2023 has been given by UK HMT to implement this Travel Rule.

### 8.4.5 Managing third party risks

VASPs have responsibilities similar to banks in correspondent banking relationships. “Correspondent banking” does not include one-off transactions[13], but is rather characterised by its on-going, repetitive nature. VASPs should establish their control framework, by defining and assessing the characteristics of their counterparty VASP relationships and whether they are undertaking activities similar to correspondent banking. This should include considering the FIC’s guidance (as per FIA section 25) on any identified high risk counterparty VASP relationships. Below are minimum requirements when considering the risks associated with third parties:

a. identify and verify the identification of the third party with which it conducts relationship similar to correspondent banking relationships;
b. collect information on the nature of the third party’s activities;
c. based on publicly-available information[14], evaluate the third party’s reputation and the nature of supervision to which it is subject;

[13] see FATF Recommendation 13 in part III.

[14] Examples of potential reliable, independent sources of information for the verification of the identity and beneficial ownership of legal persons and arrangements include: corporate registries, registries maintained by competent authorities on the creation or regulated institutions list (e.g. VASP lists maintained by each jurisdictions where available), registries of beneficial ownership and other examples. Some examples of potential sources of information on level of risks include, but are not limited to: the AML/CFT laws and regulations of the home country or the host country where the third party institution is doing business and how they apply, public databases of legal decisions and/or regulatory or enforcement actions, annual reports that have been filed with a stock exchange, country assessment reports or other information published by international bodies which measure compliance and address ML/TF risks (including the FATF, FSRBs, BCBS, IMF and World Bank), lists issued by the FATF in the context of its International Co-operation Review Group process, reputable newspapers, journals or other open source electronic

d. obtain approval from the directors, partners or senior management of that VASP before establishing a third party relationship similar to a correspondent banking relationship;
e. evaluate the controls implemented by the third party with respect to anti-money laundering and combating the financing of terrorism; and
f. establish an agreement on the respective anti-money laundering and combating the financing of terrorism responsibilities of each party under the relationship.

Not all VASPs are the same. They vary in size from small independent businesses to large multinational corporations. Similarly, no country's AML/CFT regime for VASPs is exactly the same and countries are introducing their measures at different paces. Different entities within a sector will pose higher or lower risks depending on a variety of factors, including products, services, customers, geography, the AML/CFT regime in the VASP's jurisdiction and the strength of the entity's compliance program. VASPs should analyse and seek to understand how the ML/TF risks they identify affect them and take appropriate measures to mitigate and manage those risks. **Such risk assessments should be revised periodically** to see if risk positions change. The risk assessment, therefore, provides the basis for the risk-based application of AML/CFT measures. Guidance Note 10 of 2023 avails detailed guidance on considerations of such risk assessment.

### 8.4.6 Data submission technology

The FIC does not prescribe a preferred technology, application, programme or software for submission of travel rule information as required. Any technology or software solution is acceptable, so long as it enables the ordering and beneficiary institution (where present in the transaction) to comply with its FIA obligations. For example, a solution for obtaining, holding, and transmitting the required information (in addition to complying with the various other requirements of FATF Recommendation 16) could be code that is built into the VA transfer's underlying DLT transaction protocol or that runs on top of the DLT platform (e.g., using a smart

media, third party databases, national or supranational risk assessments, information from the respondent institution's management and compliance officer(s) and public information from the regulator and supervisor.

contract, multiple-signature, or any other technology); an independent (i.e., non-DLT) messaging platform or application program interface (API).

The selected technological solution should enable VASPs to comply with the travel rule in an effective and efficient manner and enable a VASP to carry out the following main actions:

a. enable a VASP to locate counterparty VASPs for VA transfers;
b. enable the submission of required and accurate originator and required beneficiary information immediately when a VA transfer is conducted on a DLT platform;
c. enable VASPs to submit a reasonably large volume of transactions to multiple destinations in an effectively stable manner;
d. enable a VASP to securely transmit data, i.e. protect the integrity and availability of the required information to facilitate record-keeping;
e. protect the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure in line with national privacy and data protection laws;
f. provide a VASP with a communication channel to support further follow-up with a counterparty VASP for the purpose of:
    - due diligence on the counterparty VASP; and
    - requesting information on a certain transaction to determine if the transaction involves high risk or prohibited activities.

When selecting a technological solution, it is helpful to consider sanctions screening or ML monitoring capabilities of systems as described herein so as to implement one system that can enhance efficiency on all such risk management obligations.

## 9. CDD RELATED TO LEGAL PERSONS, TRUSTS AND OTHER ARRANGEMENTS

**Section only applies to legal persons and might not be relevant to current domestic VASPs. At the time of issuing this guidance, there are no indications that local VASPs are providing services directly to legal persons. The local VASPs only avail over the counter or broking services to natural persons (limited to exchange of VAs for fiat and vice-versa, with no custodial services either). Their clients remain natural persons but nothing in law restricts them from availing services to legal persons.**

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

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

VASPs 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 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 per section 7.1.2 herein. 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 VASP 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. **VASPs 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 VASPs' 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 9.1.1 – 9.1.2 below.**

### 9.1.1 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 VASPs 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.

VASPs 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 transaction/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 VASPs should understand why such person(s) is not listed on the CC incorporation documents as a Member. If there are no logical explanations, the VASPS 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 VASPs avails services, if it becomes apparent that Members or those purporting to be such are 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 9.1.2 below as sources for verification can also be used for CCs.

### 9.1.2 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. VASPs, 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 VASPs, Accountants and Auditors of such companies, or any other independent registries/bodies etc.

To verify the information listed above in 9.1(g), VASPs 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 VASPs 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.

### 9.1.3 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 VASPs.

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 were 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. VASPs must subject the UBOs behind nominee directors and shareholders to EDD measures as per the FIA. VASPs should have measures to detect the possibility that undisclosed nominee arrangements may exist. Guidance Note 10 of 2023 avail some indicators of possible nominee arrangements. Policies, procedures and controls of the VASPs must ensure detecting undisclosed nominee arrangements will be identified and addressed as part of the CDD process and ongoing monitoring by the VASPs. 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 7.1, 9.1(g) and 9.1.2 above. If nominee or relevant parties are evasive, give misleading information or do not cooperate, the VASPs should file a suspicious activity report with the FIC as per section 33 of the FIA, without delay.

### 9.2. Ascertainment of information: Associations and other Entities

The FIC has not yet seen record of VASPs doing business with associations or non-governmental organizations (NGOs). The risk exposure from such entities is notable and they therefore ought to be subjected to the necessary CDD. VASPs 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;
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 VASPs 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 9.1(g), 9.1.2 and 9.1.3 above.

### 9.2.1 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. VASPs 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 VASPs shall, in addition to the CDD measures in 9.2 (and some elements in 9.1.2) 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 9.1(g) and 9.2 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.

### 9.3. Ascertainment of Information: Partnerships

VASPs 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 VASPs on behalf of the partnership. Persons who **exercise such effective control** of a partnership, legal person or arrangement should be identified as per section 9.1(g) (and some elements in 9.1.2) above. **VASPs 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.**

### 9.4. Ascertainment of Information: Trusts

VASPs 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 7.1 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 VASPs 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 VASPs must follow the natural person identification procedure stated herein above [section 9.1(g) and some elements of 9.1.2] to ascertain the names of the beneficiaries and document the method of determining such beneficiaries. **VASPs 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.**

### 9.4.1 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*[15] may have been abused in advancing ML. Such trusts were all

[15] 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.

### 9.4.2 Founder[16]

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, VASPs 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.

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

### 9.4.3 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 VASPs 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. VASPs 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 VASPs 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.

### 9.4.4 Identifying beneficiaries

a. In the case of a **beneficiary which is an entity** (e.g. a charitable trust or company), the VASPs 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 VASPs 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 VASPs 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 VASPs should satisfy itself that these are the intended beneficiaries (e.g. by reference to the trust deed), the VASPs 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, VASPs 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.

### 9.4.5 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 VASPs should obtain information to enable it to satisfy itself as to the

identity of the directors or other controlling persons. A VASPs 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 VASPs 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 VASPs 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.

### 9.5. EXTENT AND NATURE OF EDD

The EDD measures explained herein are extensive but not exhaustive at all. The extent to which a VASPs 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, VASPs are not obliged to obtain other information about UBOs other than to enable the VASPs 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.).

## 10. 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 VASPs 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 VASPs in positions to effectively detect and report suspicions when they arise.** Guidance Note 10 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 12 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 VASP 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).

### 10.1. Practical controls

Operating frameworks or controls in the VASP 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. **Suspicions can often be detected if VASPs screen or go back some hobs/blocks (3 - 10 hobs) etc to see the audit trail of transactions/clients. Often, key information about risk levels exposure to mixers/tumblers, dark webs, use of privacy coins etc can be detected.** With many operations, a user gets a new wallet each time they transact. VASPs should follow up until it becomes improbable to follow up or risks are low. Most of the illicit proceeds eventually end up with an exchange or VASP as the criminals would at some point need to cash out;
b) The VASPs' 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 VASP 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 VASPs' 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 VASPs' AML/CFT Procedures):

g) Staff internal reporting line to the AML Compliance Officer; and

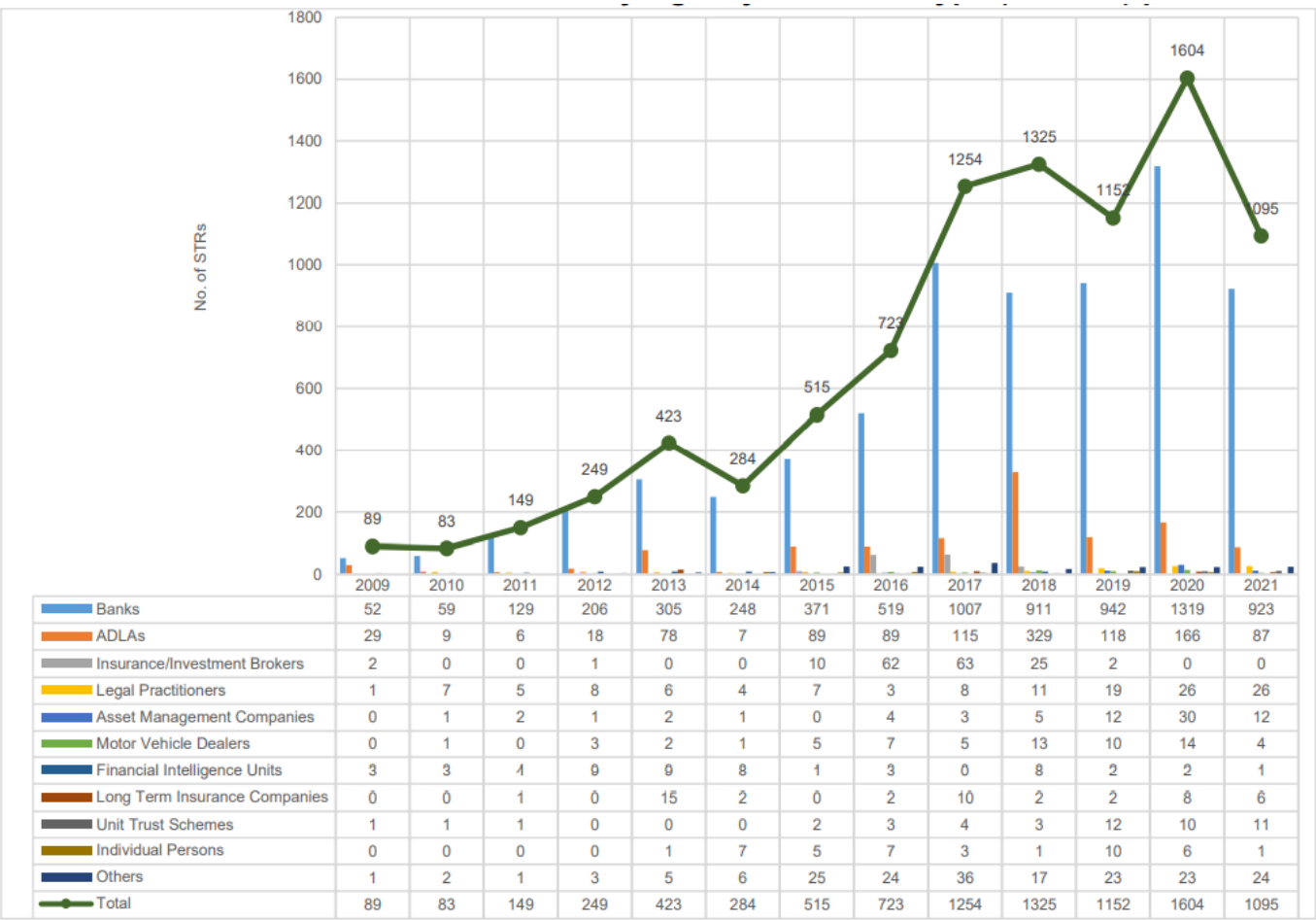
h) Confidentiality of reports, i.e. how to deal with customers, and others involved in a transaction, after an internal or external report has been made.

### 10.2. Sectoral Reporting Behaviour

The Mutual Evaluation on Namibia[17] 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[18] who submitted 13% (or 1,140). This reporting trend has not changed in 2022. 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 VASPs however, the latest information shows that only two STRs were reported from 2020 to 2023. Given the vulnerability level of the sector as per the 2020 NRA, the sector's reporting volumes could be enhanced.

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

[18] 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

### 10.3. VASPs SAR Reporting

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

## 11. RECORD KEEPING

### 11.1. What Records must be kept?

a. the identity, address and all such client identification records stated in part 7.1 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.

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

### 11.2. Who must keep records?

The VASPs (as Accountable Institution) ought to keep records as per the FIA. A third party may keep records on behalf of a VASP but the VASP remains ultimately accountable for ensuring such records are kept as per the FIA. VASPs 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.

### 11.3. 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. VASPs should maintain effective record-keeping systems to enable the FIC and other relevant authorities to access such records in a timely fashion.

### 11.4. 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 VASP is requested to do so by the FIC, the Office of the Prosecutor-General or by any other law enforcement body.

## 12. 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.

VASPS are expected in terms of section 24 and Regulation 15(5)[19] 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 VASP in any way makes use of third parties, middlemen or brokers/agents to facilitate or avail services, the VASP 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.

[19] 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[20] 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. VASPs 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. VASPs are required to further consider the detailed guidance around reporting, sanctions screening and TFS contained in Guidance Note 07 of 2023.

### 12.1 Effective Client Screening

In order to effectively implement Targeted Financial Sanctions (TFS), VASPs 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**

[20] 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 VASP 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.[21]);
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).

### 12.2 Where to find the updated Sanctions Lists?

As mentioned above, VASPs, 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

[21] 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[22] can be found on the UNSC website or via the following link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

### 12.3 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.

#### 12.3.1 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 VASPS, Accountants and law firms:*** *a freezing measure can be holding onto any funds, assets the client may have paid/deposited with the VASPS/Accountant/Law Firm (including payment for services). Could be holding onto or blocking the export/transfer of VAs that client has paid for, bid for or has provided guarantees for in a sale etc.; and*

[22] 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[23]:*** *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.*

### 12.3.2 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 VASPS, Accountants and law firms:*** *prohibiting the provision of any services, such as stopping the shipping of VAs bought by client or as agreed with client, ceasing services to transfer entity ownership, shares etc.*

### 12.3.3 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 VASP (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. VASPs need to consider appropriate implementation thereof given the circumstances they may find themselves in, with each transaction/client.

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

## 12.4 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 VASPs may not release frozen assets or do anything related to such assets without being instructed to do so.

### 12.5 Study Publications on TF Indicators, Trends and Typologies

VASPs 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. The ability of VASPs 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 10 of 2023, along with other FIC publications such as risk assessments and relevant TF related reports on the FIC website[24] and other sources.

## 13. ROLE OF AML COMPLIANCE OFFICER

The effectiveness of the AML Compliance Officer[25] usually impacts a VASPs' overall risk management effectiveness. The AML/CFT/CPF controls within a VASPS 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:

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;

[24] https://www.fic.na/ see under ML/TF/PF Risk Assessments, Trends and Typologies, Publications, amongst others.
[25] Appointed as per Section 39 of the FIA.

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 VASPs operations to lead compliance activities, as per the FIA. With very small or one-man VASPs, 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 VASP, volume of transactions, overall risk etc., regard has to be had with the VASPs' ability to duly attend to all responsibilities as per the FIA. Such factors should guide resourcing of a Compliance function.

## 14. 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.

## 15. 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.

## 16. GENERAL

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

**DATE ISSUED: 30 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**