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. 01 OF 2023

GUIDANCE ON RISK MANAGEMENT, CUSTOMER DUE DILLIGENCE, DETECTING AND REPORTING OF SUSPICIONS: ADLAs/MONEY SERVICE BUSINESSES

First Issued: 14 April 2023

Table of Contents

DEFINITIONS AND ABBREVIATIONS

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

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

"ADLA" Authorized Dealers in Foreign Exchange with Limited Authority (ADLA) as licensed by the Bank of Namibia to avail money remittance and currency exchange services;

"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 customary meaning and are used interchangeably;

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

"Enhanced Due Diligence" (EDD) means doing more than the conventional simplified due diligence or the basic CDD measures mentioned above and includes, amongst others, taking measures as prescribed by the Centre to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client or beneficial owners whose activities may pose a risk of ML, TF or PF;

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

"FATF" means the Financial Action Task Force;

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

"FIC" means the Financial Intelligence Centre;

"ML" means Money Laundering;

"PEPs" means Political Exposed Persons;

"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 regulations made under the provisions of section 67 of the Act and published by Government Notice No. 3 of 2015 promulgated in Government Gazette No. 5658 dated 28 January 2015;

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

"SAR" refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act;

"SNMA" refers to a Sanction Name Match Activity report. When an actual or potential sanctions match is detected, institutions should file a SNMA with the FIC. With effect from 1 April 2023, such should no longer be reported through SARs, nor STRs;

"STR" refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the Act. With effect from 17 April 2023, only ML suspicions should be reported through STRs. TF and PF suspicions should be reported through

"TF" means Terrorist Financing;

"TPFA" refers to 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” Terrorist & Proliferation Financing Transaction report. Used for reporting any other transaction (actual transaction) which may point to, or be linked to potential terrorism, TF or PF;

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

1. BACKGROUND

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (Act No. 13 of 2012) as amended (hereinafter referred to as the FIA). This document avails guidance on effective implementation of a risk based internal control system that ensure customer diligence and detecting of suspicions transactions/activities, as per the FIA.

Authorized Dealers in Foreign Exchange with Limited Authority (ADLA) are licensed by the Bank of Namibia to primarily avail the following services:

a. acting as a currency exchange office (a bureau de change); and
b. transmitting money or any representation of money by any means (money remittance).

Over the years, these services, in particular the money remittance services have been subject to Money Laundering (ML) abuse domestically. Internationally, there are trends and typologies which suggest abuse to advance Terrorism and Proliferation Financing (TF/PF) activities. To help mitigate ML/TF/PF risks, the Financial Intelligence Centre (FIC) issues this Guidance to help ADLAs implement and enhance their internal Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) controls.

2. COMMENCEMENT

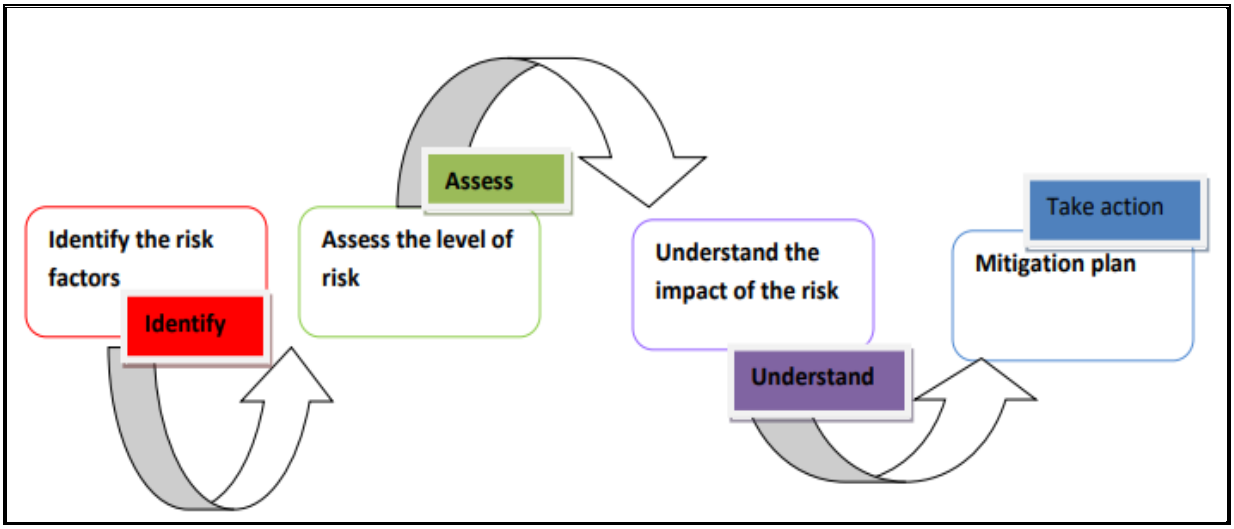
This Guidance Note comes into effect on **17 April 2023**.

PART A

PRACTICAL RISK ASSESSMENTS IN ADLAs

3. RISK BASED APPROACH TO AML/CFT/CPF MANAGEMENT

The Risk-Based Approach (RBA) speaks to a control system premised on an entity's understanding of risks it may be exposed to. As shown in the diagram below, such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (mitigation plan). The key features are *identifying* risks, *assessing* such risks to *understand its levels and impact*, followed by a *mitigation plan* aligned to such risk levels. An effective control implementation is also characterised by documenting ML/TF/PF risk findings (in a risk report) and updating such when the need arises. This enables a platform through which risks are tracked.



Risk Based Approach implementation framework

Money launderers look for cash-based service industries with high turnover rates. ADLAs are cash based high turnover businesses. These features make ADLAs' services attractive to criminals. Money Launderers are equally attracted by the worldwide reach, ease of converting cash into wire transfers and vice-versa, the speed, simplicity and certainty of ADLA transactions.

As a control framework, the RBA ensures efficiency of operations within AML/CFT/CPF activities. If duly implemented, the RBA ensures prudent balancing of compliance costs to business and customers by prioritising and directing controls to where they are most needed, in a prudent manner. This ensures high risk clients and services are accorded

controls which are commensurate to risk while lower risk clients and services are not burdened with unwarranted due diligence.

Annexure A attached hereto avails a detailed list of potential indicators of ML and TF activities. ADLAs are encouraged to consider such in their risk assessments and the entire RBAs.

3.1 Conducting Risk Assessments and Implementing Effective Controls

ADLAs, like all other Accountable Institutions are best placed to understand their risk exposure and thus implement controls to manage same. In advancement of the RBA, an ADLA must:

3.1.1 Undertake a ML/TF/PF risk assessment[1], the comprehensiveness of which should be aligned to the nature, complexity and risk exposure of their proposed products (or amendments). The main elements institutions are required to consider, in addition to others that may arise are:

a. *the **risk profiles of customers** who will make use of your products and services. Section 23 of the FIA prescribes obligations with regards to the treatment of "Risk clients". Where a client has been identified as high risk, ADLAs must apply EDD measures. Inherently, Politically Exposed Persons (PEPs)*[2]*, foreign nationals or other such type of persons whose Customer Due Diligence (CDD) information cannot be effectively or readily verified may present enhanced risk exposure. PEPs need to be subjected to Enhanced Customer Due Diligence (EDD). See FIC's 2019*

[1] FIA section 39(1) [Read with FIA section 23]: An accountable institution, on a regular basis, must conduct ML/TF/PF activities risk assessments taking into account the scope and nature of its clients, products and services, as well as the geographical area from where its clients and business dealings originate. Persons much measure, rank or rate (e.g low, medium and high) their level of risk for relevant elements of the services they aim to provide. You could rank each service as low, medium or high risk. The control measures should describe how the entity will reduce each level of risk, especially the medium and higher risk rated levels. The FIC may, in its interpretation however disagree with ratings not duly informed and request reconsiderations accordingly.

[2] Annexure B of this document lists persons who meet the definition of a PEP. Also see FIC Revised Directive No. 02 of 2020 on PEPs as well as Revised Guidance Note No. 01 of 2019 on the definition and due diligence required for PEPs: Both documents are available on the FIC Website under the "Publications" folder.

Guidance on PEPs. In the case of foreign customers, the periodic risk assessment should indicate the inherent risk level of countries in order to aid risk considerations. The reliability of national identification systems in foreign countries and the effectiveness of AML/CFT/CPF controls in such country should always be considered;

b. ***Vulnerability of products and services:*** *typically, and from an inherent risk view, the FIC's assessment is that currency exchange services have generally been exposed to lower ML risk levels than conventional money remittance services. Note that ADLA's remittances services are for use by natural persons only, as per Exchange Control Rulings and Regulations. If proposed remittances appear to be for potential business purposes, care needs to be taken to reduce risks of abuse as some STRs in the FIC have shown that persons advancing tax evasion and capital flight abuse ADLA remittances to advance same;*

Profile mismatch

At times, the profile of the client might not match the values of funds client transactions in. In the single case of potential terrorism and TF investigated by NamPol, it was found that the primary suspect, a local Namibian, formerly Christian, who converted to Islam some years ago and became radicalized was sending funds to various high risk jurisdictions. Upon investigations, it was found that the suspect who send such via ADLAs/Money Service Businesses (MSBs), did not have the means to earn such funds, judging by his lifestyle audit revelations. He was granted minority stake in two CCs. In one, he has shareholding of 5% and in another, he has shareholding of 10%. One entity is a 'car wash' and the other is a used car dealership. He appears to be a front man for foreign nationals from Kenya and Somalia, who are also closely associated with his faith.

He appears to have been used by others to remit funds on their behalf as his earning and lifestyle did not suggest all the funds he was sending was his. The said primary suspect openly supports extremism and his activities on social media revealed same. (Observations from the 2023 NRA update on TF)

c. ***Product delivery channels*** *(how you provide those services): for example, face-to-face, remittances in partnership with other stakeholders etc. Cross border*

delivery channels could enhance domestic and foreign ML/TF/PF risk exposure, especially if ADLA does not gain assurance that relevant AML/CFT/CPF frameworks in such other foreign jurisdictions are effective and reliable, relative to the risks at hand.

Practical tip:

In practice, the overall risk is assessed periodically and client profile types are identified, which can for example be: Foreign PEP, Domestic PEP, Self-Employed businessman, Government Employee, Teacher, Bank Employee, Domestic Worker, etc. Inherent risk levels (high, medium, low) are then assigned to each such group/profile. When a client is onboarded, he or she is placed in one of such profiles and then subjected to due diligence relevant for such profile. Such due diligence must then include reviewing information which may be specific to such individual client.

3.1.2 If any, role of key stakeholders in the service provision or product delivery: ADLAs should duly understand the nature and effectiveness of AML/CFT/CPF controls that are implemented by its partners or stakeholders in the value chain, especially for money remittance activities. Ensure that there has capacity and is willing to play their part in ensuring effective risk mitigation and thus FIA compliance. Controls such as availability of records[3], as and when where required by the institution (for timely and effective due diligence) or competent authorities[4] are worth considering;

3.1.3 The type, nature and extend of controls to reduce inherent[5] risks to tolerable or acceptable residual[6] levels. ADLAs have a responsibility to implement such and duly demonstrate their effectiveness to authorities such as the FIC. The FIC must be satisfied, upon such presentation, that such residual risk levels are tolerable or acceptable to the national AML/CFT/CPF framework. The entirety of controls

[3] As per FIA record keeping obligations.
[4] As defined by the FIA.
[5] Inherent risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.
[6] The remaining risk level after due controls have been implemented.

should be documented in an **AML/CFT/CPF Program or Policy document which needs management approval**;

3.1.4 New innovations, products and services: for institutions already operating in the AML/CFT/CPF framework and are launching or introducing new products, it is essential to ensure aligning the approved AML/CFT/CPF Program or Policies to speak to the new products or innovations. The existing program may be amended if introduction of new innovations or proposed amendments so require;

3.1.5 External Risk Assessments: The considerations and indicators herein are not extensive. Real Estate Agents are required to consider observations from Sectoral Risk Assessment Reports and National Risk Assessments issued by the FIC. Local[7] and international trends and typology reports issued by bodies such as ESAAMLG[8] and FATF[9] (available on their websites) equally help highlight changing risks broadly and related to the sector. To the extent possible, this guidance has incorporated lessons and best practices from such local and international publications. ML and TF trends are dynamic, it is thus essential to keep abreast of updated publications in this regard; and

3.1.6 Risk Management Reports: All identified risks as far as products, services, delivery channels, types of clients etc., should be documented in Risk Management Reports. Such report should be periodically updated when material changes arise in risks and controls.

[7] Published on the FIC website under Risk Assessments folder while trends and typology reports are under Publications folder.
[8] https://www.esaamlg.org/index.php/methods_trends
[9] https://www.fatf-gafi.org/en/publications.html

PART B

IMPLEMENTING A RISK-BASED PREVENTATIVE FRAMEWORK

4. IMPLEMENTING A RISK BASK APPROACH

4.1 Customer Due Diligence (CDD)

Sections 21 and 22 of the Act ADLAs to identify their clients. For ADLAs to effectively mitigate the risk of ML/TF and PF, client identification and record keeping measures need to be complemented by other measures as prescribed by the FIA including: implementing AML Programs and Policies; adopting a risk based approach; on-going and enhanced due diligence of client behaviour; measures to aid detecting and reporting of suspicious transactions and activities; training of staff members on how to mitigate these risks etc. The FIC website contains Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF and PF in terms of the Act.

4.1.1 Extent of Customer Due Diligence Measures

The extent of customer due diligence measures depends on the degree of risk a proposed transaction presents to the ADLA. It depends on the type of client/customer, business relationship, product, transaction destination country or country of origin and delivery channels.

CDD goes beyond simply carrying out identity checks to understanding who one is dealing with. This is important because even people known to the ADLA may become involved in illegal activity at some time, for example if their personal circumstances change or they face new financial pressure. An ADLA’s due diligence measures should reduce this inherent risk and the opportunities for staff to be corrupted. In practice, ADLAs must consider the level of identification, verification and ongoing monitoring that is necessary, depending on the assessed risk. An ADLA should be able to demonstrate that the extent of these procedures is appropriate to mitigate risk exposure.

4.2 Simplified Due Diligence

4.2.1 Extend of Simplified CDD

The extent to which simplified due diligence should be applied is essential to financial inclusion objectives. For this reason, identification in terms of the FIA should only be applied when so required. Given this, it is important to note that identification of clients is required when a business relationship is established or when a single transaction that exceeds the following thresholds is entered into:

CDD Threshold	Extend of CDD
Less than or equal to NAD 4,999.99	Below simplified CDD threshold. The normal business identification for general operational purposes should suffice. Only apply EDD if risk is assessed as high.
Above NAD 4,999.99	Simplified CDD as a minimum, and escalation to EDD if risk is high.

An ADLA may apply simplified due diligence measures where the business relationship or transaction is considered low risk in terms of ML, TF or PF. In practice, simplified due diligence only applies to a client when the ADLA assess such as being low risk. Transactional risk exposure such as destination of or origin of funds should be equally considered and if risk is higher, EDD should be considered. FIA Regulations 6 to 11 provide guidance on the minimum identification procedures that should be followed for the various types of clients.

4.2.2 Ascertainment and Verification of Information

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

a. Verification: full names;
b. Verification: nationality;

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

4.2.3 Tips on simplified CDD

ADLA may:

a. use information already at hand to determine the nature or purpose of a business relationship without requiring further information. For example, if your customer is a student or pensioner, you can assume what the source of funds is, unless other factors exists such as too frequent transactions which may be beyond reasonable student or pensioner earnings; and
b. adjust the frequency of CDD reviews, for example, to when a change occurs which escalates the low risk behaviour.

4.2.4 Pre-requisites for Simplified Due Diligence

To apply simplified due diligence, an ADLA 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 or delivery channel of the remittance);
c. there is no structuring to reduce amounts below EDD levels;
d. 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;
e. neither party to the transaction is established in or operates in a high risk country;
f. the customer is not a politically exposed person, a family member, or a known close associate of a politically exposed person;
g. the real customer is seen face to face (and not sending people to transact on his/hr behalf);
h. the source of funds or wealth are transparent and understood by your business;

i. transactions are clearly within the mandate of an ADLA (not business transactions disguised as those of natural persons);
j. the transaction is not complex or unusually large.

4.2.5 When to cease Simplified Due Diligence and commence EDD:

a. If suspicions of ML, TF or PF arise;
b. doubt whether documents obtained for identification are genuine;
c. doubt whether the person is the one demonstrated by the documentation;
d. indications that client may be transacting on behalf of another unduly;
e. suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired;
f. circumstances change and your risk assessment no longer considers the customer, transactions, or location as low risk; and
g. Any other considerations that do not maintain the low risk of client or transaction(s).

5. Enhanced Due Diligence (EDD)

5.1 Nature and Type of EDD Measures

It is critical that an ADLA has measures that can identify when to escalate from simplified due diligence to EDD, e.g identifying that a client meets the definition of a PEP. EDD applies when a client's risk profile or transaction is not low. It includes 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.

It is essential to keep in mind that identification procedures as per FIA Regulations 6 to 11 regulate obtaining the minimum identification information (as per 4.2.1 and 4.2.2 above) while Regulation 12 provides for EDD or obtaining additional information[10]. Given

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

the nature of once-off transactions facilitated by ADLAs, it is necessary to ensure obtaining all relevant information before finalisation of transactions.

EDD means building onto the basic identification information obtained as per simplified due diligence measures in parts 4.2.1 and 4.2.2 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: Help ADLA create context around magnitude of clients earning levels, especially for self-employed or business people.
Occupation or source of income	
Source of funds involved in transaction	Enables a comparison of transacting behaviour through funds being moved/remitted/exchanged and the financial profile of client

5.2 When to undertake EDD:

a. As per internal risk assessment, ADLA has determined that there is a high risk of ML, TF or PF associated with the client or transaction;
b. FIC or another supervisory or law enforcement authority provide information that a particular situation is high risk;
c. a customer or other party is established in, or operates in a high risk country;
d. client has given you false or stolen documents to identify themselves (immediately consider reporting this as suspicious transaction/activity);
e. a customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person;
f. the transaction is complex, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose; and
g. Any other considerations enhancing client or transaction risk.

5.3 Factors which escalate risks

ADLAs should consider several factors in risk assessments when deciding if EDD needs to be applied. Such should be considered along with the indicators as per Annexure A of this report. The following are some examples of factors to take into account.

5.3.1 Customer related factors based on information the ADLA has or behaviours indicating higher risk, such as:

a. unusual aspects of a business relationship;
b. a client/person is resident in a high-risk area/country;
c. a client with an abundance of cash;
d. too frequent transacting/remittances without reasonable explanations;
e. searches on a person or associates show, for example, adverse media attention, disqualification as a director or convictions for dishonesty;
f. structuring or smurfing: *The 2020 NRA FIC observed after the closure of the bank accounts of Mansudae Overseas Project Architectural and Technical Services (Pty) Ltd (MOP)[11], that MOP's employees appeared to use ADLAs to remit funds offshore. Given the manner in which such remittances appeared structured and the financial values in many transactions, such could have been funds remitted on behalf of the business and may not necessarily be employee salaries.* The risk that ADLAs may have been abused to advance potential PF is worth noting. The due diligence measures explained herein, though they may seem ML focused, can help ADLAs mitigate risks arising from potential TF and PF, if duly applied; and
g. any other relevant considerations.

5.3.2 Geographical factors indicating higher country risk

Countries identified by a credible source as:

[11] In April 2009, the UNSC 1718 Committee designated a DPRK entity named KOMID for targeted sanctions, noting it to be the DPRK's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. Another DPRK entity, commonly known as MOP, was operating in Namibia for many years, primarily servicing Government contracts in the Ministry of Defense. Unlike KOMID, MOP was not designated under any UNSC Resolution at the time, but listed on the OFAC list.

a. has been assessed by organisations such as FATF, World Bank, Organisation for Economic Cooperation and Development and the International Monetary Fund as having in place *ineffective* AML/CFT/CPF measures;
b. not subject to equivalent AML/CFT/CPF measures;
c. with a significant level of corruption, terrorism, or supply of illicit drugs;
d. subject to sanctions or embargoes issued by United Nations Security Council (UNSC) and others such as OFAC[12] etc; and
e. providing funding or support for terrorism.

In addition to the above, when the client or transaction (as per information at hand or in the media) can be linked to or is related to any of the following, an ADLA must consider EDD:

a. oil;
b. arms and weapons;
c. precious metals and stones;
d. tobacco products;
e. cultural artefacts; and
f. ivory and other items related to protected species.

5.3.3 Understanding the concept of additional measures

For EDD to be undertaken duly, the ADLA must do more to verify, identify and scrutinise the background and nature of the transactions. 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 an ADLA's AML/CFT/CPF control procedures. For example, the ADLA should:

[12] The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. Can be accessed at: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information

a. obtain additional information or evidence to establish the identity from independent sources, such as more documentation on identity or address or electronic verification alongside manual checks;
b. take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust;
c. if receiving payment ensure it is made through a bank account in the name of the person you are dealing with;
d. The following measures must be taken when the transaction relates to a PEP, a family member or known close associate of a PEP:
    - obtain senior management approval before establishing a business relationship with that person;
    - take adequate steps to establish the source of wealth and source of funds that are involved in the proposed business relationship or transaction; and
    - conduct enhanced ongoing monitoring if transactions are frequent.
e. Carry out more scrutiny of the business relationship and satisfy yourself that it is consistent with the stated purpose;
f. measures which must be taken when either party to a business relationship, or relevant transaction is established in a high-risk main or third country[13]:
    - Obtain any additional information which may support the legitimacy of the customer's information and/or identification;
    - Obtain additional information on the intended nature of the business relationship (prosed money remittance including intended recipient or sender);
    - Obtain supporting information around the source of funds;
    - Obtain information on the reasons for the transaction;
    - Obtain the approval of senior management for establishing or continuing the business relationship; and

[13] (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)

- Enhance monitoring of the business relationship by increasing the number and timing of controls applied and select patterns of transactions which require further examination.

6. SUSPICIOUS TRANSACTION OR ACTIVITY REPORTS ("STRs/SARs")

The primary reason for monitoring transactions carried out by clients is to ensure that such transactions are consistent with the ADLA's 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 ADLAs in a position to effectively detect and report suspicions when they arise. Indicators, especially such listed in Annexure A of this Guidance, are helpful in identifying potential suspicious activities or transactions.

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 8 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 STRs and SARs.

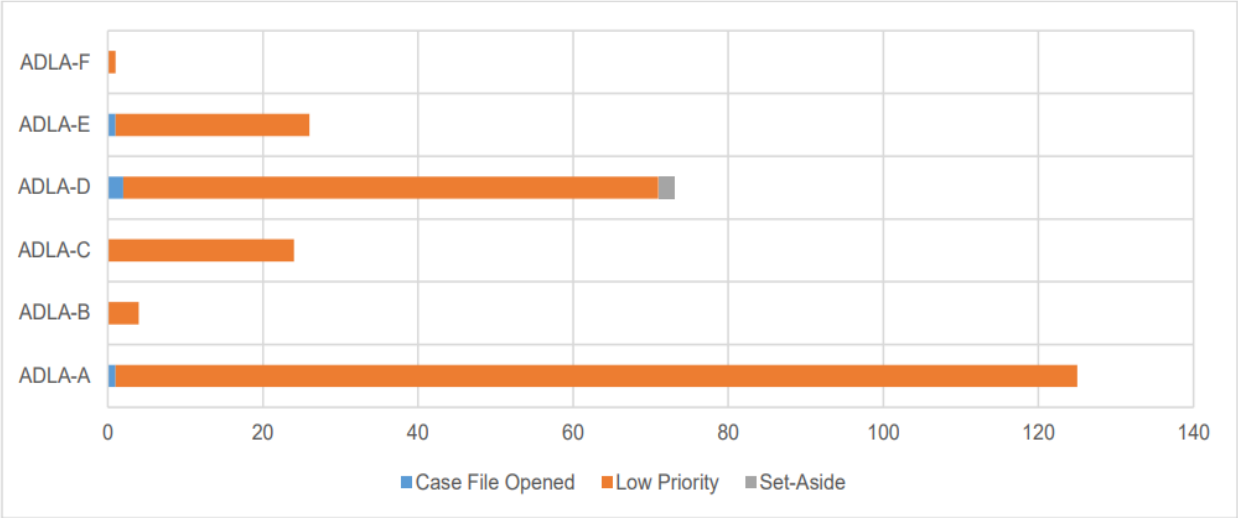
STRs are reports that explain suspicious transactions for ML. The term suspicion is meant to be applied in its everyday, normal sense. The suspicion, as an example, could be the funds involved in the transaction are the proceeds of any crime or linked to terrorist activity. The ADLA does not need to know what sort of crime may have been committed, but one or more red flags or warning signs of 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.

6.1 What happens to STRs from the ADLAs Sector?

As seen from the Sectoral Feedback Report issued in October 2022[14], a total of 8,945 STRs were received by the FIC since the reporting obligation commenced until 31 December 2021. The banking sector submitted the most reports in such period, filing 78% (or 6,991) of reports followed by ADLAs who submitted 13% (or 1,140). When reports are received, such undergo a cleansing process which primarily results in categorization of same to determine how such reports would be treated (including setting aside or escalation to case files for further investigation). The chart below speaks to the categorization of STRs from the sector.



Categorization of STRs by Reporting ADLAs

Most STRs from the sector were categorised as Low Priority. This does not however suggest poor reporting but rather emanates from overall FIC priority levels wherein the financial values often carry significant weight in what the FIC's minimal investigative

[14] Report discussed with sector in 2022 and published on the FIC website under Publications.

resources can attend to. Generally, ADLA operations facilitate transactions of low financial values in comparison to other sectors. During the period under review, ADLA-A filed the majority of STRs (a total of 125 STRs or 49%). This was followed by ADLA-D and ADLA-E with 73 and 26 STRs respectively. Worth noting is that ADLA-D also filed the most STRs that were accorded 'high priority' status and escalated for further analysis.

6.1.1 Improving STR/SAR Quality

Below are some areas noted from the sector's STRs/SARs which can be enhanced on to improve report quality.

a. **Lack of ML/TF and/or PF indicators in the reports:** It is helpful that upon reporting, such information is availed. If the internal risk assessment, CDD and ongoing monitoring measures are effective, such should yield indicators which inform the suspicion. The guidance herein plus the list of indicators in Annexure A of this document can further assist in this regard. AML Compliance Officers are encouraged to reach out to the FIC when uncertain;

b. **Poorly articulated "Reasons for Suspicion" in STRs/SARs:** usually, when adequate CDD has been undertaken, it is easier to explain grounds for suspicion when making analysis of flagged transactions. Regardless, attempts should be made to adequately explain why we find transactions or activities suspicious as such helps with FIC analysis of reports;

c. **Duplicate and erroneous filing of reports:** More care needs to be taken, especially by AML Compliance Officers to reduce erroneous and duplicate reporting. The initial cleansing processes take from the valuable time that FIC analysis resources could deploy to other activities; and

d. **Filing of incomplete STRs/SARs:** more could be done to ensure completeness of information shared in STRs. It helps with value addition from such reports. If the internal risk assessment, CDD and ongoing monitoring measures are effective,

such should yield indicators which inform the suspicion. The guidance herein plus the list of indicators in Annexure A of this document can further assist in this regard. AML Compliance Officers are encouraged to reach out to the FIC when uncertain.

6.2 Practical Controls

Platforms or controls in the ADLA must enable the following:

a. Staff, including the staff of the ADLA's agents must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in ML, TF or PF;
b. The ADLA's AML Compliance Officer, or their appointed alternative, must consider all such internal reports. The Compliance Officer must submit the relevant report via GoAML;
c. Such report should be reported promptly and without delay to enhance the effectiveness of combatting activities;
d. After filing such report, the ADLA 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;
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; and
    - keep a record of any communications to or from the FIC about a suspicious transaction or activity report.

7. RECORD KEEPING

7.1 What Records must be kept?

a. the identity, address and all such client identification records as stated in part 4 herein;

b. identification information of all the parties to a transaction in a remittance transaction;
c. the identity of the sending or remitting party;
d. the date, time and amount of the transaction;
e. information relating to all reports escalated to the FIC; and
f. any other information which the FIC may specify in writing.

7.2 Who must keep records?

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

7.3 Manner of Record Keeping

The records must be kept:

a. in a manner that protects the confidentiality of such copy, record or document;
b. in a manner which permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity or civil or criminal asset forfeiture procedures.

Further, records can be kept in hard copy or electronic format as long as a paper copy can be readily produced. ADLAs should maintain effective record-keeping systems to enable the FIC to have access to such records in a timely fashion. The Golden Rule with record keeping is enabling an effective reconstruction of identification or transacting activities by competent authorities.

7.4 Period for which records must be kept

Records that relate to the establishment of a business relationship 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 the 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 ADLA is requested to do so by the FIC, the Office of the Prosecutor-General or by any other law enforcement agency.

8. TF RISK IN ADLAs

8.1 Domestic and International TF risk

Namibia has not confirmed actual TF exposure within the ADLAs sector. The sector is however one of those highly vulnerable to TF due to its cross border remittance services. The 2020 NRA notes that whilst Namibia is not considered high-risk for TF, small-scale financing raised from within Namibia and remitted could expose the country to TF.

As mentioned in section 5.3.1(f) above, the 2020 NRA observed, *after the closure of the bank accounts of MOP, an OFAC listed entity, that the entity's employees appeared to use ADLAs to remit funds offshore. Though this was said to have been their earnings, the methodology of remitting funds in a manner which appeared structured could have easily exposed the country to PF. Such sectoral loopholes within ADLAs could be equally exploited for TF as well, as suspected in one potential TF case under police investigation at the time of publishing this guidance (April 2023). In the said case, the subject appears to be remitting funds on behalf of others to high risk TF jurisdictions. The subject is a registered beneficial owner in a few CCs but his lifestyle may suggest he could be simply used to represent unknown UBOs' interests or persons.* The risk that ADLAs may have been abused to advance potential TF or PF is worth noting and the 2023 NRA update rightly suggests an increased TF risk exposure for ADLAs.

In light of the above, it is prudent for all Accountable Institutions, especially ADLAs, to consider the vulnerabilities and risk factors associated with TF and the potential red flags that may indicate TF activities. Accountable Institutions should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds across borders. The NRA equally found that Namibia's porous border present a significant vulnerability which enhances the ease with which proceeds can be moved around.

TF covers a wide range of terrorism-related activity, including operational funds, equipment, salaries and family compensation, social services, propaganda (e.g radicalization), training, travel, recruitment and corruption. It is not necessary for Accountable Institutions to identify the *purpose* of TF, as a pre-requisite for reporting. Any potential TF-related information or suspicion must be reported to the FIC promptly and without delay. What is helpful is that such report be as accurate as possible, timely and treated with urgency and sensitivity.

As per the various SRAs, NRAs and consideration of TF trends internationally, the FIC highlights the following as primary TF threats ADLAs should consider:

a. *Overseas groups able to inspire support through ideology* – Individuals may be inspired to contribute to overseas terrorist groups by travelling to conflict zones, which requires self or third-party funding. Radicalised individuals may also choose to contribute to terrorism by raising and contributing funds. ADLAs which move funds with ease are at greater risk;

b. *Well-resourced groups with established networks* – This may involve the movement of larger sums of money for terrorism, in particular for or by state-sponsored groups. Again, ADLAs' ability to ensure fast transfer of funds is vulnerable to TF abuse;

c. *Domestic terrorism* – given the low-to-non-existent level of domestic support for terrorist causes and absence of terrorist networks, it is more likely that financiers

of domestic terrorism (if it were to happen domestically) could manifest in Namibia as isolated disaffected individuals or small groups.

8.2 Nature of TF

The characteristics of TF can make it difficult to identify. Transactions can be of low value, they may appear as normal patterns of behaviour and funding can come from legitimate as well as illicit sources. It is important to note that the methods used to monitor ML (as stated herein) can also be used for TF, as the movement of those funds often relies on similar methods to ML. Internationally the TF processes are considered to typically involve three stages:

a. *Raising funds* (through donations, legitimate wages, selling items, criminal activity);
b. *Transferring funds* (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell); and
c. *Using funds* (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses)

The risks associated with TF are highly dynamic. As such, ADLAs need to ensure that their prevention and combatting measures are current, regularly reviewed and flexible. It is important that ADLAs maintain preventative and combatting awareness as well as effective transaction monitoring systems that incorporate dynamic TF risks, along the more static risks associated with ML.

As seen from the 2020 NRA, the value of funds moved through Namibia connected to potential TF is likely to be much lower than other forms of illicit capital flows. However, if funds connected to TF were to be associated with Namibian institutions, it would likely have an adverse effect on Namibia's reputation. Outside of the obvious harm caused as a result of TF, any domestic institution with this activity could see their reputation severely damaged. Further, if such institution's combatting and prevention measures were found

to be inadequate or ineffective, they could also face civil and potentially criminal charges as per the FIA and PACOTPAA[15].

8.3 Namibia as a Conduit for TF

One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist financiers. Overseas groups may seek to exploit Namibia as a source or conduit for funds to capitalise on Namibia's reputation as being a lower risk jurisdiction for TF. For instance, funds originating in or passing through Namibia may be less likely to attract suspicion internationally.

TF through the DNFBs [16] and specifically ADLAs sector can be small-scale and indistinguishable from legitimate transactions. TF could involve structured deposits of cash into bank accounts followed by wire transfers out of Namibia or wire transfers through an ADLA.

The same methods explained above through which ADLAs can be abused to advance TF are similar for PF. The due diligence and RBA, especially screening of clients/parties against sanctions lists is essential in combatting TF and PF within the ADLAs sector.

8.4 UNSC Sanctions Screening

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

ADLAs are expected in terms of section 24 and Regulation 15(5)[17] of the FIA to screen clients or potential clients involved in transactions against the relevant sanctions lists

[15] Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014).
[16] Designated Non-Financial Businesses and Professionals.
[17] Accountable institution to conduct on-going and enhanced customer due diligence: 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.

issued by the United Nations Security Council (UNSC). Note that local ADLAs must gain assurance that all parties to a transaction are duly screened, before transacting. ADLAs need to ensure that their agent(s) or such other stakeholders duly attend to their responsibilities in this regard, if any. This is essential to combat TF and PF activities by ensuring designated persons, organisations or countries are identified and not availed services accordingly.

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 remittances or currency exchanges in USD, 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. ADLAs are required to further consider the detailed guidance around sanctions screening and TFS contained in Guidance Note 07 of 2023.

8.4.1 Effective Client Screening

In order to effectively implement TFS, ADLAs 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 persons should not be granted access to any services at all (prohibited) and their attempted transactions should be reported to the FIC promptly and without delay, while the assets (or funds) involved are frozen, as per the FIA and PACOTPAA.

   In 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.

The following databases of an ADLA 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., sender and beneficiary as well as client who wants currency exchange services[18]);
d. If known, names of individuals with direct or indirect relationships with them; and
e. If known, persons acting on behalf of customers (including those who may have pooled funds or availed funding to others who remit or transact on their behalf).

ADLAs may consider using the screening tool availed by the FIC. It is important to first evaluate same and gain reasonable assurance that the screening mechanism to be employed would address its risk exposure, if not, employ other alternative screening measures to effectively mitigate this risk. Both ad-hoc and batch screening are permitted, with batch screening often preferred to ensure effective screening of voluminous transactions simultaneously. The FIC notes that screening is at times undertaken by the operational system as availed by the ADLA's partner/agent. The need to gain assurance that such screening tool is effective rests on the ADLA as the Accountable Institution.

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

8.4.2 Where to find the updated Sanctions Lists?

ADLAs, 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 or listed any persons yet. At an international level however, the information on designated individuals, entities or groups in the Sanctions Lists is subject to change. The most recently updated sanctions list of the UNSC [19] can be found on the UNSC website or via the following link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

8.4.3 Targeted Financial Sanctions (TFS)

As mentioned above, the term Targeted Financial Sanctions 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.

8.4.3.1 Asset freezing without delay

In terms of international standards, without delay means **within a matter of hours**[20]. 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.

[19] 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.
[20] See findings on Namibia's 2022 Mutual Evaluation Report.

Examples of freezing:

i. ***Financial Institutions:*** *a freezing measure can be suspending access to a bank account or blocking any further transactions;*

ii. ***DNFBPs like ADLAs:*** *a freezing measure can be blocking or withholding the funds the client attempted to transact with; and*

iii. ***VASPs[21]:*** *a freezing measure includes blocking services to trade and transfer of virtual assets.*

8.4.3.2 Prohibition

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 ADLAs:*** *prohibition from accessing or using any of the ADLAs services upon detecting that a client is listed.;*

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

8.4.4 Object of freezing and prohibition

Note however that even when freezing measures are taken or implemented, there should be no restrictions on client introducing or depositing more funds with the ADLA, provided they do not further gamble or deplete such. 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. ADLAs

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

need to consider appropriate implementation given the circumstances they may find themselves in, with each transaction/client.

8.4.5 Reporting Possible Name Matches

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 or completed transaction) which may point to, or be linked to potential terrorism, TF or PF.	TPFT- Terrorist & Proliferation Financing Transaction report

The mechanism to report any freezing or prohibition 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 process. The following information must be shared when submitting a SNMA report:

a. The full name of the ‘confirmed match’. Attach identification documents of the ‘confirmed match’, such as passport or other ID documents for individual; and
b. Amount of funds or other assets frozen (e.g., value of funds wanted to transact with etc.). Attach proof documents such as internal ADLA record showing the frozen funds, transaction receipts, etc., if such are at hand.

ADLAs are encouraged to familiarise themselves with reporting guidelines and the effective implementation of TFS measures as contained in Guidance Note 07 of 2023.

An ADLA identifies a confirmed match when screening clients upon account opening.

Person A is listed and is a prospective client of an ADLA or approaches the ADLA to access their services. The ADLA must block the transaction immediately, refrain from offering any services to Person A, and submit an SNMA via goAML. The SNMA must include attachments that clarify:

a. The value and location/placement of the funds client want to make use of (e.g in Cash or received and within the control of the ADLA). Such cash should be seized, counted and placed beyond the reach of the client. When reporting, include supporting documents which indicates what was seized and where it is kept;

b. ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

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

9. ROLE OF AML COMPLIANCE OFFICER

The effectiveness of the Compliance Officer [22] usually impacts an Accountable Institution's overall risk management level. The AML/CFT/CPF controls within an Agency 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;
b. the AML/CFT/CPF Controls (policies, procedures etc) are at all times aligned to risk levels;

[22] 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;
e. measures to internally detect and escalate[23] potential ML/TF/PF indicators or red flags are prudent and enable the required level of confidentiality;
f. he/she files external SNMAs, STRs/SARSs 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 an Accountable Institution to lead compliance activities, as per the FIA. With one-man Agencies, the individual Agent has a responsibly to attend to all the responsibilities of a Compliance Officer duly. Depending on the size of the ADLA, volume of transactions, overall risk etc., regard has to be had with the Agent's ability to duly attend to all responsibilities as per the FIA. Such should guide resourcing of a Compliance function.

10. GENERAL

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

11. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of ADLAs. Should an ADLA fail to adhere to the guidance provided herein, it will be such ADLA's responsibility to demonstrate alternative risk management controls implemented which are effective and aligned to the FIA.

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

12. GENERAL

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

DATE ISSUED: 14 APRIL 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

ANNEXURE A: ML/TF INDICATORS

A single indicator may not singularly present potential ML activities but when considered with other indicators and any relevant risk factors or circumstances around the client behaviour, profile, transaction etc., may enhance the chances of detecting potential suspicious transactions.

13.1 Indicators most relevant for ML

The below, though found predominantly relevant for ML, can be equally relevant for detecting TF activities.

13.1.1 ML indicators related to identifying the person

The following are examples of ML indicators that you may observe when identifying persons or entities.

a. There is an inability to properly identify the client or there are questions surrounding the client's identity;
b. The client refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify;
c. The client refuses to provide information regarding the beneficial owners (e.g if transacting on behalf of another person), or provides information that is false, conflicting, misleading or substantially incorrect;
d. The identification document presented by the client cannot be verified/authenticated;
e. There are inconsistencies in the identification documents or different identifiers provided by the client, such as name, address, date of birth or phone number;
f. Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate;

g. Client displays a pattern of name variations from one transaction to another or uses aliases;
h. Client alters the transaction after being asked for identity documents;
i. The client provides only a non-civic address or disguises a post office box as a civic address for the purpose of concealing their physical residence;
j. Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple clients that do not appear to be related;
k. Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple clients conducting similar transactions;
l. Use of the same hotel address by one or more clients;
m. Transactions involve persons or entities identified by the media, law enforcement and/or intelligence agencies as being linked to criminal activities; and
n. Attempts to verify the information provided by a new or prospective client are difficult.

13.1.2 ML indicators related to client behaviour

The contextual information acquired through the Know Your Client (KYC) requirements or the behaviour of a client, particularly surrounding a transaction or a pattern of transactions, may lead an ADLA to conduct an assessment in order to determine if it is necessary to submit a STR to FIC. The following are some examples of ML indicators that are linked to contextual behaviour and may be used in conjunction with an ADLA's assessment client's risk.

a. Client makes statements about involvement in criminal activities;
b. Client conducts transactions at different physical locations, or approaches different tellers/employees;
c. Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information);
d. Client exhibits nervous behaviour;
e. Client refuses to provide information when required, or is reluctant to provide information;

f. Client has a defensive stance to questioning;
g. Client presents confusing details about the transaction or knows few details about its purpose;
h. Client avoids contact with ADLA employees;
i. Client refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect;
j. Client exhibits a lack of concern about higher than normal transaction costs or fees;
k. Client makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the ADLA not to file/maintain required reports; and
l. Insufficient explanation for the source of funds.

13.1.3 ML indicators surrounding the financial transactions in relation to the person/entity profile

Clearly understanding the expected activity of a person or entity will allow an ADLA to assess their financial activity effectively. For example, an entity involved in an industry that is not normally cash intensive conducting excessive cash transactions or a person conducting financial transactions atypical of their financial profile. The following are some examples of ML indicators surrounding the financial transactions related to the person/entity profile.

a. The transactional activity far exceeds the projected activity at the beginning of the relationship;
b. The transactional activity (level or volume) is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.);
c. The transactional activity is inconsistent with what is expected from declared nature of transactions/activities;
d. The volume of transactional activity exceeds the norm for client profile or geographical area;
e. Client appears to be living beyond their declared means;

f. Large and/or rapid movement of funds not commensurate with the client's financial profile;
g. Rounded sum transactions atypical of what would be expected from the client;
h. Size or type of transactions atypical of what is expected from the client;
i. Conducting transactions when the client's address or employment address is outside the local service area without a reasonable explanation;
j. There is a sudden change in the client's financial profile, pattern of activity or transactions; and
k. Client uses notes, monetary instruments, or products and/or services that are unusual for such a client.

13.1.4 ML indicators based on atypical transactional activity

There are certain transactions that are outside the normal conduct of an ADLA's everyday business. These transactions may be indicative of a suspicious transaction and would require additional assessment. Some examples of ML indicators based on atypical transactional activity are listed below.

a. A series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds;
b. Transactions displaying financial connections between persons or entities that are not usually connected;
c. Transaction is unnecessarily complex for its stated purpose;
d. Client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way;
e. Client's transactions have no apparent business or economic purpose;
f. Transaction is consistent with a publicly known trend in criminal activity;
g. Client uses musty, odd smelling or extremely dirty bills;
h. Through natural persons transacting, transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist);
i. Client frequently exchanges small bills for larger bills;

j. Suspicious pattern emerges from a client's transactions (e.g. transactions take place at the same time of day);
k. Atypical transfers by client on an in-and-out basis, or other methods of moving funds quickly, such as a currency exchange followed immediately by a wire transfer of the funds out;
l. Funds transferred in and out on the same day or within a relatively short period of time; and
m. Unusual amount of self-use by agent/owner.

13.1.5 ML indicators related to transactions structured below the reporting or identification requirements

Structuring of transactions to avoid reporting or identification requirements is a common method for committing or attempting to commit an ML offence. There are multiple thresholds which trigger reporting/identification requirements by an Accountable Institution. Some examples of ML indicators which may be indicative of a person attempting to evade identification and/or reporting thresholds are listed below.

a. ADLA becomes aware of the structuring of wire transfers at multiple locations;
b. Client appears to be structuring amounts to avoid client identification or reporting thresholds;
c. Client appears to be collaborating with others (e.g sending others to transact on his/her behalf) to avoid client identification or reporting thresholds;
d. The structuring of wire transfers through multiple locations of the same ADLA or by groups of persons who enter a single location at the same time;
e. Multiple transactions conducted below the reporting threshold within a short period;
f. Client makes inquiries that would indicate a desire to avoid reporting or understand certain AML related thresholds;
g. Client exhibits knowledge or keen interest in reporting thresholds; and
h. Client conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.

13.2 Indicators specifically related to TF

This section is focused on examples that are specific to the possible commission of a TF offence. However, it is important to emphasize that the other ML indicators listed in this Guidance Note above may also prove relevant in determining when you have reasonable grounds to suspect the commission of TF as the methods used by criminals to evade detection are similar.

The indicators below are some examples of indicators that are specific to TF:

a. Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls;
b. Transactions linked with or can be traced to the name of non-profit organization (NPO), an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization. Note that locally, Faith Based Organisations, especially those that can be associated with encouraging certain extremist behaviour are found to present higher TF risks;
c. The use of funds by a NPO is not consistent with the purpose for which it was established;
d. Raising donations in an unofficial or unregistered manner, or remittances which may appear to support or advance such donations;
e. Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations;
f. Transactions involve persons or entities identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities;
g. Law enforcement information published or provided which indicates persons or entities may be linked to a terrorist organization or terrorist activities;
h. Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of

concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations;

i. Client is associated with NPOs, persons or entities with an online presence which supports violent extremism or radicalization; and

j. Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, NPO, etc.).

ANNEXURE B: IDENTIFYING PEPs[24]

Below is a list of persons who meet the description of a PEP, amongst others:

a) heads of state, heads of government, ministers and deputies, assistant ministers or senior politicians;
b) members of parliament or of similar legislative bodies;
c) secretary to cabinet or those holding such similar position;
d) members of the governing bodies of political parties;
e) significant, senior or important political party officials;
f) executive directors and their deputies (former Permanent Secretaries);
g) directors and their deputies in line ministries;
h) regional authority councillors as well as directors and their deputies;
i) local authority councillors as well as the executive management of local authorities;
j) senior executives of state-owned entities;
k) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
l) members of the boards of domestic or international banks and central banks;
m) ambassadors and members of management of embassies or similar bodies;
n) high-ranking officers in the armed forces and law enforcement, including prosecutorial services;
o) members of the management of supervisory bodies; and
p) directors, deputy directors and members of boards or equivalent function of an international organisation.

The following are included in the broader scope of PEPs:

[24] See Revised Guidance Note 01 of 2019

i. **Foreign PEPs:** individuals who are or have been entrusted with prominent public functions by a foreign country;

ii. **Domestic PEPs:** individuals who are or have been entrusted domestically with prominent public functions;

iii. **International organisation PEPs:** persons who are or have been entrusted with a prominent function by an international organisation;

iv. **Family members:** individuals who are related to a PEP either directly or through marriage or similar (civil) forms of partnership; and

v. **Close associates:** individuals who are closely connected to a PEP, either socially or professionally. Close associates of PEPs means individuals who are closely connected to a PEP, either socially or professionally, and include but not limited to: individuals known to have any close business relationships with a PEP, such as the PEP's business partners or identified as the owners and/or beneficial owners of a legal person or legal arrangement which is associated with a PEP.