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. 02 OF 2024

## GUIDANCE ON SANCTIONS SCREENING EFFECTIVENESS: BASED ON THEMATIC REVIEW OF THE EFFECTIVENESS OF CUSTOMER AND TRANSACTION SCREENING SYSTEMS

**First Issued: 25 October 2024**

## DEFINITIONS AND ABBREVIATIONS

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

**"Control test"** testing effectiveness of screening against sanctioned/listed persons' details as they appear on the sanction source. The opposite of this is 'manipulated tests' defined herein below;

**"Customer Screening"** – The process of verifying or confirming if customers of the institution are listed on a sanctions watchlist. This takes place upon account opening and on a continuous basis thereafter as sanctions watchlists are updated;

**"Effectiveness"** the degree to which the matching of sanction names is successful in producing a desired alert;

**"Efficiency"** This is the measurement of the number of alerts that generate for analysts to review. It is an indication of the levels of staff needed to clear alerts generated by screening systems in identifying sanctions risks;

**"Efficiency Score"** in sanction testing, is the ratio or the average number of returns per alert;

**"Enhanced Due Diligence" (EDD)** means doing more than the conventional simplified due diligence or the basic CDD measures and includes, amongst others, taking measures as per the Financial Intelligence Act 2012 (as amended, herein referred to as FIA) to identify, as far as reasonably possible, the source of wealth, income, 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 official documentation issued by a recognised government;

**"Freeze"** means the prohibition of the use, transfer, conversion, disposition or movement of any funds, economic resources, property or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of an action initiated by the United Nations Security Council (UNSC) in accordance with applicable Security Council resolutions (as per PACOTPAA[1]);

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

**"Freezing of economic resources"**, includes preventing their use to obtain funds, goods, or services in any way, including the selling, hiring or mortgaging them (as per PACOTPAA);

**"Fuzzy logic"** Fuzzy matching relates to the rules used in screening solutions which allow for non-exact matches to be identified. The parameters of the systems need to be wide enough to detect slight differences in sanction names but not too wide so that there are large amounts of false positive alerts;

**"Listed"** means any natural or legal person listed or designated by the relevant authorities (including the UNSC, OFAC, EU, etc.). A sanctioned person can be referred to as either 'designated' or 'listed'. These words are used interchangeably with the term 'listed';

**"Manipulation test"** testing effectiveness of screening against sanctioned/listed persons' names and related person/client details that have been manipulated/changed using an algorithmic or any relevant type of manipulation deemed appropriate by the FIC to fulfil assessment objectives. The opposite of this is 'control tests' defined herein above;

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

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

**"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;

**"Single transaction"** means a transaction other than a transaction concluded in the course of a business relationship and includes a cash deposit by a person, other than the client, into a client's account. This means not more than one transaction and within this context of client identification, has the same meaning (or attracts similar compliance obligations) as an "Occasional transaction";

**"SAR"** refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act. When a potential ML *activity* is noted, institutions should file a SAR with the FIC;

**"SNMA"** refers to a Sanction Name Match Activity Report. When a potential sanctions match is detected, institutions should file a SNMA report 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. When a potential ML transaction is noted, institutions should file a STR with the FIC;

**"Targeted Financial Sanctions (TFS)"** means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities or beneficiaries;

**"Transaction screening"** relates to identifying the potential involvement of sanctioned individuals and entities within a transaction in a domestic or international payment;

**"United Nations Security Council Resolutions (UNSCRs)"** These are formal expressions of the UN Security Council. The Resolutions are issued as individual documents. At a minimum, the sanctions database and system configuration should include the following UN Resolutions and their successor resolutions:

- ✓ UNSC Consolidated List that includes UNSC Resolutions 1267/1989 (Al Qaeda), 1988 (Taliban) and 2253 (ISIL Daesh) for Targeted Financial Sanctions on terrorism and terrorist financing; and
- ✓ UNSC Consolidated List that includes UNSC Resolution Numbers 1718 of 2006 (DPRK) and 2231 of 2015 (Iran) for TFS on Proliferation Financing;

**"Whitelisting"** Instead of alerting on all names on sanction lists, whitelisting allows only specific names on sanction lists to not generate any alerts. This is usually done by creating a rule in the configuration of the system to not let any customer name generate a match against a name that is whitelisted in the aim of reducing false positives to names that hold no or low sanction risks;

**"Without delay"** means taking required actions *within a matter of hours*, as advised in Namibia's September 2022 Mutual Evaluation Report. For purposes of Resolution 1373 the term without delay seems to require reasonable grounds or reasonable basis to suspect that a person or entity is a terrorist, one who finances terrorism which requires that without delay should be interpreted to prevent the flight and dissipation of funds or other assets related to terrorism and the need to swiftly disrupt the flow of such funds and assets.

**TABLE OF CONTENTS**

## 1. BACKGROUND

Namibia is a United Nations (UN) Member State and has an obligation to comply with United Nations Security Council (UNSC) Resolutions. The sanctions issued by the UN are considered and composed by the Security Council, under the authority of Article 41, Chapter VII of the UN Charter. FATF[2] Recommendations 6[3] and 7[4] require Namibia to implement targeted financial sanctions regimes to ensure risk mitigation and thus compliance with the UNSC Resolutions relating to the prevention and suppression of Terrorism, weapons Proliferation and the financing thereof.

At a practical level, relevant institutions are required to ensure effective Customer Due Diligence[5] that enables screening to detect persons listed by the UNSC, when such persons attempt to transact with or make use of certain designated services. This is in line with the definition of 'Monitoring'[6] as defined in the FIA Regulations. The FIC conducts periodic tests to gain reasonable assurance that monitoring (screening) mechanisms implemented at the institutional level duly provide effective controls that will not unduly expose designated services to risks of TF, PF.

## 2. PURPOSE AND OBJECTIVES OF SCREENING

The Financial Intelligence Centre (FIC) as part of its continuous efforts to assist the Government of the Republic of Namibia in combatting Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF), hereby issues this Guidance Note in terms of Sections 9(2)(e) of the FIA. It builds on Directive 01 of 2022 and Directive No. 01 of 2023. Institutions are encouraged to read this Guidance along with contents in the said Directives.

[2] Financial Action Task Force – Global body coordinating the prevention and combatting of ML, TF and PF.
[3] As per Targeted United Nations Financial Sanctions related to the Combatting of Terrorism and Terrorist Financing.
[4] As per Targeted United Nations Financial Sanctions related to the Combatting of Proliferation.
[5] In terms of FIA Regulations 1 and 15, as well as Section 24 of the FIA - read with Section 25 of the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014) (PACOTPAA).
[6] See definitions section of this Guidance for explanation of 'monitoring' activities.

This guidance highlights considerations to enhance the effectiveness of sanctions screening systems, in particular, as part of the greater framework of Targeted Financial Sanctions (TFS) stipulated in the FIA and PACOTPAA.

The primary pillars of an effective TFS framework are:

a) **sanctions screening:** the ability to **detect or identify persons listed/designated** on sanctions lists;
b) **asset freezing:** screening is followed by **freezing of assets of listed/designated persons without delay;** and
c) **Prohibition: prohibition of providing** any funds/other assets/services etc, directly or indirectly, available for the benefit of such sanctioned individuals, entities, or groups.

## 3. SCOPE AND APPLICABILITY

The Guidance Note is aimed at all Accountable Institutions (AIs) and Reporting Institutions (RIs), herein simply referred to as institutions. These are institutions that provide services listed in Schedules 1 and 3 of the FIA. In the same vein, sections 24, 25, and 45 of the PACOTPAA collectively require regulatory and supervisory bodies listed in FIA Schedules 2 and 4 to ensure compliance and contribute to TF and PF risk management efforts. This naturally implies such bodies are to ensure institutions under their regulation and supervision comply with the PACOTPAA, especially when updates to sanctions lists are made. Equally, in their supervisory or regulatory dealings such as licensing and authorising market entry, compliance be ensured with TFS measures as per the PACOTPAA as simplified herein.

It is common cause that services listed in FIA Schedules 1 and 3 have been subjected to ML abuse domestically. The risk that such services can be further abused to advance TF and PF activities is prevalent. Internationally, there are many trends and typologies that suggest how TF and PF threats exploited vulnerabilities within such services. This Guidance Note focuses on effective TFS implementation to combat and prevent TF and PF. In furtherance of such, all institutions providing services listed in Schedules 1 and 3 of the FIA are required to implement effective internal Anti-Money Laundering, Combatting the Financing of Terrorism and

Proliferation (AML/CFT/CFP) measures[7]. The guidance herein should thus be used in enhancing the effectiveness of sanctions screening systems at the institutional level.

## 4. COMMENCEMENT

This Guidance Note comes into effect on **25 October 2024**.

## 5. UNSC SANCTIONS SCREENING

The object of sanctions screening is to ensure effective implementation of TFS against any person or group listed by the UNSC.

Institutions are expected, in terms of Section 24 and Regulation 15(5)[8] of the FIA, to screen clients or potential clients involved in transactions against the relevant sanctions' lists issued by the UNSC. Such a screening should take place before accounts are opened or the client is granted access to services, regardless of whether the client transacts below or above the CDD threshold. If the institution in any way makes use of intermediaries, brokers, or agents to facilitate or provide any services[9] related to sanctions screening, it has an obligation to ensure that such intermediaries, agents, or brokers duly attend to their AML/CFT/CPF responsibilities, if any reliance is placed on the services they provide. This is essential to combat TF and PF activities by ensuring designated persons are identified and no services are provided to them.

[7] Includes both policies and procedures (controls).

[8] 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.

[9] For example, some entities' sanctions screening controls are executed by external parties or external parties provide/manage the operational system which may have an in-built screening operation.

### 5.1 UNSC Sanctions Lists

At a minimum, the sanctions database should include the following UNSC Resolutions and their successor resolutions:

a. UNSC Consolidated List that includes UNSC Resolutions 1267/1989 (Al Qaeda), 1988 (Taliban), and 2253 (ISIL Daesh) for Targeted Financial Sanctions on terrorism and terrorist financing;
b. UNSC Consolidated List that includes UNSC Resolution Numbers 1718 of 2006 (DPRK) and 2231 of 2015 (Iran) for TFS on Proliferation Financing; and
c. Domestic designations [or those that are designated by the National Security Commission (NSC)] pursuant to UNSC Resolution 1373. Locally, the NSC is the body with statutory responsibilities in terms of the PACOTPAA to proscribe persons or entities to the 1267/1989 Committee for designation and for proposing persons or entities to the 1988 Committee for designation. At the time of issuing this Guidance, the NSC has not designated any person(s).

The UNSC Consolidated List and the updates thereto may be downloaded from the UNSC website via https://www.un.org/securitycouncil/content/un-sc-consolidated-list .

### 5.2 Beyond the UNSC sanctions lists

Screening against other designation lists such as OFAC[10], though not mandatorily required by domestic laws, is very helpful in the overall context of risk management effectiveness. For any transactions or currency exchanges in USD, for example, there is an inherent legal obligation to screen involved parties against the OFAC list. Similarly, when dealing in British Pounds or the EURO currencies as a foreign exchange currency, screening against lists issued by His Majesty's Treasury (HMT) and the European Union (EU) is an inherent obligation that, if not complied with, could jeopardise the involved AI or RI's relationship with these institutions and corresponding banking relationships. This could naturally expose Namibia to relevant risks such as:

[10] The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions.

a. institutions being sanctioned, which may include fines or bans from international remittance frameworks;
b. loss of correspondent banking relations, which will undermine the integrity of the financial system and clients' ability to transact; and
c. the natural consequence of sanctioned institutions is a loss of international trading opportunities for the country, and such can adversely impact the economy.

### 5.3 Principles of effective TFS (and Sanctions Screening in particular)

The FIC issued Directive No. 01 of 2023[11] on Mandatory Implementation of Targeted Financial Sanctions (TFS). Amongst others, the said directive provides overall expectations on actions before sanctions screening and after sanctions screening if sanctions name matches are found.

In order to effectively implement TFS, institutions must ensure:

a. sanctions screening is performed on all clients before providing 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** providing services or facilitating transactions, unless such screening is done in the course of a business relationship when the sanctions lists are updated. **This enables proactive detection of sanctioned or designated persons.** If such sanctioned or designated persons are detected, they 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 transactions cancelled, 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 the client is listed, eventual freezing of the assets or funds that the client attempted to transact with (can be made). The freezing is then followed by a complete prohibition to transact any further.**

[11] Directive 01 of 2023 - Mandatory Implementation of Targeted Financial.pdf (fic.na)

## 6. OBJECTIVES OF FIC's THEMATIC REVIEWS

The FIC has conducted thematic reviews on the sanctions screening systems of some financial institutions in 2021, 2022, and 2024. The aim remains to understand the effectiveness and efficiency of the primary client and transaction screening systems, with particular attention placed on four key considerations:

a. Does the system generate an alert when an 'unmanipulated' sanctioned name is screened?
b. Are the 'fuzzy logic' matching rules, configuration, and threshold settings effective, such that a 'manipulated' sanctioned name generates an alert?
c. Are the levels of 'false positives' or 'noise' within operable/manageable levels?
d. Is the system's performance in line with the regulator's expectations?

### 6.1 Scoring thresholds

As a reference point for system performance metrics, the table below highlights the expected Customer and Transaction Screening thresholds, in terms of thematic review scoring, as per Directive 01 of 2022.

| Test | Expected score/Level of ability to match |
|---|---|
| Control | 100% at all times |
| Manipulation | Between 95% and 100% |

In 2021, the FIC engaged the services of AML Analytics[12] to conduct tests (thematic reviews) on the effective functioning of sanctions screening systems deployed by institutions. The outcomes of the 2021 tests were not encouraging. Given that this was the country's first thematic review, institutions were encouraged to enhance their systems' level of effectiveness. In late 2021, consultations commenced with the financial sector on setting thresholds. This culminated in the eventual publication of Directive 01 of 2022 in March of the next year.

[12] A private consulting firm with technical capabilities suitable for thematic reviews.

### 6.1.1 Reconciling thresholds with UNSC obligations

a. With the UNSC, whose principled position is reflected in FATF Recommendations 5, 6, and 7, TF/PF risks do not have the same tolerance level for non-compliance as ML;

b. The UNSC has zero tolerance for non-compliance with sanctions screening obligations, and thus, our country's thresholds should ideally be aligned to such zero tolerance as much as possible. In fact, the UNSC Resolutions and the PACOTPAA do not create room or allowance for a 1-5% compliance failure. Any level of non-compliance, no matter how small, poses a risk worth addressing. Despite this, the threshold level for manipulated data was reduced to 95%, creating room for tolerance to practical challenges;

c. The law of averages: the FIC is aware of the global averages and freely shares such information with the sector within the thematic review reports. With averages, the best performing institutions typically attain higher scores than the said averages, while the poor-performing institutions naturally score lower. The scores from poor performing institutions thus inherently reduce the global averages to where they are. Benchmarking[13] exercises of any nature take cognisant of *'best-in-class'* performances if the objective is to enhance overall effectiveness.

### 6.1.2 Screening domestic transactions

a. Amongst a host of provisions which may be cited, the 2012 FIA Regulations define monitoring, amongst others, as follows: *"... the screening of the name of a client or potential client, and the names involved in transactions..."* There is no provision that limits sanctions screening requirements to cross-border remittances[14]; and

b. When the International Monetary Fund (IMF) was in Namibia[15] to help guide the implementation of the FATF Joint Group's Action Items, the FIC again asked the IMF to

[13] The FIC acknowledges that the balancing act required is challenging, however protecting the integrity of our financial system remains paramount. Therefore, lowering the standard to the current global averages does not seem logical from a risk management or compliance perspective.
[14] Additionally, AML Analytics who have conducted the thematic reviews so far have also reiterated this position.
[15] In the first quarter of 2024.

re-emphasise this international obligation to the banks, and such clarity was provided. Banks attended the IMF session. The IMF went further to cite examples of sanctions screening at the jurisdictional level in the European Union (EU) and across the EU member countries.

### 6.2 Common trends and observations

The FIC's thematic reviews undertaken in the past have identified several common trends and findings. Some of these are:

a. Overall underperformance against most sanctions screening testing metrics versus global benchmark data;
b. Significant weaknesses seen in the ability of institutions to identify manipulated names in their screening system and processes;
c. Reliance on manual processes with limited automation across the sanctions screening process. This becomes challenging when volumes are enormous;
d. Lack of understanding into how sanctions screening systems operate and potential risks they bring;
e. Where there was no prior testing of sanctions screening systems, there was limited understanding of system configuration, resulting in poor performance;
f. Over-reliance on manual systems and processes along with an over-reliance on technology and data vendors;
g. Average returns per hit (efficiency indicators) also remain relatively high in comparison to resources to process or review such hits. This shows system inefficiencies, generating significant numbers of false positives;
h. Vendors have been tasked with managing financial institution risk without financial institution understanding or awareness of system settings and the impact thereof;
i. In some instances where systems have been tuned, alerting levels are tuned to current resource capacity *as opposed to being turned to risk appetite*;
j. A limited number of institutions have testing and auditing programs in place;
k. New systems are not being tested before implementation;

l. Screening systems are not generating alerts to potential matches to sanction names where systems have not been tuned in any way for more than a year;
m. Senior management is not being adequately briefed on sanctions risk and programs; and
n. In some instances, there was a misunderstanding between the differences of transaction screening and transaction monitoring by institutions and the usages of identifying risks through a combination of customer screening, transaction screening, and transaction monitoring technologies.

Most screening tools use similar technology and work in the same way. The key to optimum effectiveness and efficiency is how it is being used. Normally, when a screening system is not performing as expected, it is because of one, or a combination of these things:

a. Poor configuration;
b. It is being used with 'out of the box' or factory settings;
c. The rules and settings have not been updated to suit the changing risk appetite of the institution;
d. It is an old version of the vendor solution that has not been updated;
e. Poor list management – too many sanction sources are being screened;
f. The list provider is not fully up to date; and
g. Problems with the institutions' list feed in keeping up with list providers updates.

Throughout the thematic review, the FIC has identified that it is how a system is used by the institution and not the actual system itself that provided outstanding results against their peers.

## 7. SUPERVISORY EXPECTATIONS: SANCTIONS SCREENING

### 7.1 General considerations

Institutions can minimize their risk of non-compliance via the following considerations:

a. Ensuring that senior management is committed to promoting sanctions compliance;
b. Undertaking ongoing sanctions-based risk assessments to assess the likelihood of dealing with an individual or entity on a sanctions list;

c. Ensuring that all employees have been adequately trained to recognize any potential sanctions issues;
d. Ensuring adequate policies and procedures are in place and approved by senior management;
e. Appointing a responsible person with the appropriate skills and experience to deal with sanctions-related issues and take ownership of the sanctions regime;
f. Using technology as a tool to identify financial crime risk through real-time and ongoing screening methods;
g. Ensuring that there are proper internal escalation processes in the event of an actual match;
h. Conducting independent, ongoing, and regular screening tests to assess the effectiveness and efficiency of the systems. Institutions should naturally conduct risk assessments on the effectiveness of sanctions screening systems to identify potential shortcomings. The FIC's thematic review results and approach taken in such tests can also serve as guidance on how institutions may approach such internal screening tests;
i. Where possible and provided there is agreement amongst entities, consider conducting, testing, utilizing peer comparative[16] data and tuning to improve configuration of sanctions screening systems to drive greater effectiveness and efficiency. This is especially relevant in Namibia where some entities use different sanctions screening systems but are different levels of effectiveness as per FIC's thematic review outcomes. This is mere best practices noted in a few entities and can only work with consent of participating parties; and
j. Ensuring that appropriate supervision is in place in key client facing/money transmitting departments.

### 7.2 Senior management oversight and commitment

#### 7.2.1 Culture of compliance (tone-at-the-top)

[16] This should be risk and governance data related to sanctions screening systems and not data that have a bearing on competitiveness.

Senior management and the Board of Directors set the tone at the-top around risk management and tolerance for non-compliance institutionally. This impacts organisational culture around compliance and risk management. As per Section 20A(4) of the FIA, senior management remains charged with the obligation to ensure the TFS and sanctions screening risk management framework[17] remains relevant, updated, and effective in mitigating TF and PF risks.

Relevant senior management should have a reasonable appreciation and understanding of sanctions screening processes, procedures, frameworks, and technology with the capability to act should sanctions risk arise. Senior management should actively assess, review, and approve the organizations sanctions compliance program, including policies, procedures, resourcing, data, and technology practices. Senior management should own the sanctions regime, as they will be accountable in the event of non-compliance.

A clear whistleblower policy and culture of compliance that does not penalise active reporting of potential sanctions violations or misconduct and ensures senior management acts when misconduct or violations are identified.

### 7.2.2 Adequate resourcing

Senior management needs not only provide oversight and maintain governance protocols. They should also ensure adequate resources are provided to the compliance function. Resources including suitable and proper staffing, technology, data, and training to ensure sanctions screening can be undertaken in an appropriate matter aligned to the organizations risk-based approach. In this context, there ought to be adequate balance in the nature of the system, its outputs, and human resources able to process the volume of outputs from the system.

### 7.2.3 Management reporting

Reporting on all relevant elements of the sanctions screening program should be provided to senior management on a frequent basis in a risk-based manner. Given the low tolerance level and adverse impact of TF and PF risks, the frequency to the Board of Directors should be no

[17] This is a component of the entire AML/CFT Compliance Program.

less than quarterly if system ineffectiveness arises. Reporting should include but not be limited to the alignment to this guidance document (and FIC Directive 01 of 2022) and be focused on being able to identify, assess, and act on sanctions risk. Compliance leaders should have a direct reporting capability to the Managing Director/Board of Directors to escalate critical sanctions risk information generated from the sanctions screening process.

### 7.3 Risk assessment

In February 2019, the Wolfsberg Group published guidance on sanctions screening. They stated that screening *"requires a programmatic approach through which each financial institution must assess its own risks in order to define the manner, extent, and circumstances in which screening is employed."*[18]

That process is built around four core principles summarized as follows:

a. *Articulate the specific sanctions risk the institution is trying to prevent or detect within its products, services, and operations.*
b. *Identify and evaluate the inherent potential exposure to sanctions risk presented by the institution's products, services, and customer relationships.*
c. *A well-documented understanding of the risks and how they are managed through the set-up and calibration of the screening tool.*
d. *Assess where, within the institution, the information is available in a format conducive to screening.*

Being able to effectively identify potential threats and vulnerabilities within the sanction's compliance context will enable organizations to enhance their programs. A regular, periodic risk assessment of the sanctions screening program and associated policies, procedures, and frameworks will produce effective compliance programs. Organizations should construct, if they do not have one in place, a risk assessment methodology based on its ability to identify, assess, and manage those risks.

[18] Wolfsberg Group 2019, Wolfsberg Sanctions Screening Guidance, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

### 7.3.1 Emergent risk typologies

Due to the evolution of crime and continued usage of evasive techniques undertaken by sanctioned individuals and entities, there is a need to constantly monitor new emergent risks as well as test against the new typologies on an ongoing basis. Institutions should be constantly monitoring guidelines and alerts published by competent supervisory authorities and international bodies (e.g., FATF, ESAAMLG, UNSC, etc.), as well as through continuous training and skill advancements. They should be able to enhance system effectiveness through the updating of policy and system configurations to meet new and emergent risks posed by sanctioned individuals and entities.

## 7.4 Ownership, skills and training

### 7.4.1 Responsible persons

Responsible persons (e.g., the AML/CFT/CFP compliance function) need to be accountable within the organization for the overall effectiveness of the sanctions screening program. Responsible persons should be adequately skilled with the requisite experience and be provided with ongoing training. Responsible persons should be knowledgeable across all elements of the sanctions screening process and be accountable to the areas that they oversee.

### 7.4.2 Risk-based training program

Training of responsible persons and associated personnel needs to be undertaken in a risk-based manner that is ongoing, frequent, and helps develop appropriate expertise across all components of the sanctions screening program. Training should be across all functions linked to the sanctions program and should include accessible resources for all stakeholders to continue to drive understanding of sanctions risks, driving greater execution.

## 7.5 Policies and procedures

### 7.5.1 Documented methodology

All configurations of the sanctions screening program, including processes, policies, procedures, frameworks, and technology configurations, need to be adequately documented. Documentation should be securely stored and reviewed on an ongoing basis with continued updates in line with improvement programs. Documentation should have ownership by Responsible Persons and be accessible and understood by senior management.

### 7.5.2 Processes and procedures

Clear and appropriate processes and procedures should be instituted and followed by all persons in the sanctions screening process as well as the wider organization. Clear processes need to be defined and approved by senior management. Processes and procedures should be accurately documented and validated by Responsible Persons aligning to the risk-based approach of the organization.

### 7.5.3 Record keeping

In line with the FIA, all risk-relevant records need to be properly documented and securely stored. Such may be physical and/or digital, depending on the nature of the document and aligned with the organization’s business practices.

## 7.6 Technology

### 7.6.1 Balancing effectiveness and efficiency

Institutions should first ensure that they have the correct AML/CFT/CPF technologies in place to detect financial crime indicators. This should include a robust sanction screening system that is set up to alert against names on globally important sanctions lists and tuned to flag sanctioned names even when they have been altered using algorithms to assess the fuzzy logic matching capabilities of a screening system. Algorithmic manipulation will stress test a screening system and make it harder for a system to identify and alert against sanctions records. Sanctions screening systems should be tested regularly to ensure they are working as expected and that the number of false positives generated by the system is manageable and does not overwhelm available resources.

Sanctions screening system testing will help an institution understand a system's configuration whilst determining its weaknesses within pre-defined detection parameters. Testing and the ongoing monitoring of the screening system will facilitate improvement and enhancement of systems' performance through ongoing iterative tuning to optimize the efficiency and effectiveness thereof.

All AML/CFT/CFP technologies should be monitored on an ongoing basis to ensure they remain correctly calibrated and that the number of false positives generated by the system remain at a manageable level. A highly tuned AML/CFT/CFP system that is fit-for-purpose leads to relevant and valid alerts without the interference of excess system noise caused by numerous irrelevant false positives.

### 7.6.2 Manual and automated systems

Within the FIC's thematic review, many organizations were utilizing manual screening systems, including those of substantial scale and with potential risks and vulnerabilities to sanctions. The choice between the implementation of manual and automated screening systems should be risk-based.

Whether systems are commercially sourced or in-house developed, institutions should understand their capabilities and limitations in an effort to ensure such systems are aligned to meet risk management expectations, data requirements, and risk profiles. Institutions should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used, institutions should be satisfied that they have adequate contingency arrangements should the software fail and should periodically gain assurance that the software is working as expected.

Automated screening systems provide batch screening system capabilities that enable more efficient screening due to delta screening capabilities, more effective use of data segmentation, the ability to utilize secondary identifiers with greater effectiveness, and typically have far greater ability to customise configurations based on risk.

Delta Screening is the process of screening customer accounts whenever a change occurs in either the customer accounts or the watchlists used in the screening process. This limits the unnecessary process of a full list of customers screened against the full list of sanction parties every day. After the full list of customers is screened against the full list of sanction parties once, then the full list of customers can be screened only against *new sanction names* thereafter. Then only new customers can be screened against the full list of sanction parties daily, without screening the full list of customers against the full list of sanction parties daily.

Below are some considerations around practices relating to the determination of the level of automatization of sanction screening systems.

| **Determining the level of automatization of sanction screening system** | |
|---|---|
| **Good Practice** | **Poor Practice** |
| The institution has carried out a sanction risk assessment and has evaluated its provided services and products, the daily/monthly number of customers' transactions, the number of existing customers, and the intensity of new customer onboarding. It has determined that to ensure adequate sanction risk management, it is necessary to implement an automatic IT system solution for screening of both transactions and customers. Considering the limited technical capabilities of the institution, the institution | The institution used to provide limited products and therefore was performing only manual sanction checks on publicly available sources, which were appropriate for managing its sanction risks. The institution has started to offer a new product. However, before implementing the new product, the institution in its targeted risk assessment for the product, did not assess whether the existing sanction screening measures would be effective to ensure management of risks inherent to the new product. |

| | |
|---|---|
| decides to use a third-party service-provided IT tool for sanction screening.<br><br>The management of the institution understands the importance of effective sanction screening and has allocated sufficient resources necessary for the new IT tool. The institution's sanctions officer/compliance officer and IT specialists are involved in cooperation with the third-party vendor and in the implementation of the new IT solution to ensure that all the institution's determined requirements are met and that the new IT tool is properly integrated with other institution's IT systems and is tested before implementation. | In practice, after the new product was introduced, the institution's employees responsible for carrying out the manual sanction checks cannot perform the necessary tasks within the time frame determined in the internal procedures of the institution, therefore creating backlogs for both transaction monitoring and know-your-customer processes and leading to increased sanctions risks and customer complaints. |
| The institution has carried out a risk assessment and has concluded that, considering the provided services, it would be disproportionate to implement automatic sanction screening for incoming/outgoing payments. The institution only offers a limited range of products that have been assessed as low-to-medium-low-risk products, and its customer base is comparatively small.<br><br>The institution has implemented additional controls, namely, its product limitations foresee that only residents of Namibia may receive the institution's services. To receiving the service, the customer shall use only an account in another credit institution that is licensed and/or registered in Namibia, and the institution is not accepting third-party payments. Additionally, the institution regularly assesses the actual payment flow to determine whether the determined product limitations have been met in practice and sanctions risks are being managed effectively. | The institution has implemented an automated sanctions screening tool; however, its functionalities have not been evaluated in sufficient detail. For example, the institution is not aware that the screening tool has very limited fuzzy matching algorithms, which will not ensure effective and efficient identification of manipulated sanctioned records. Thus, the functionalities of the screening tool are insufficient to ensure effective management of sanctions risks, considering the type and scale of the institution's services and customer base. |

### 7.6.3 Exact matching and fuzzy logic

In some circumstances, in the name screening process, exact matching may be appropriate, such as in the case of adverse media screening. However, in the instance of sanctions screening, the usage of fuzzy logic or black box technologies powered by algorithms to detect manipulations of sanctioned individuals or entity names are required. This can be provided either

by third-party vendors or built in-house. If the FIC's thematic review or institution's internal review measures, such as audit identified consistent underperformance of the screening system's ability to match against manipulated names across the market and all forms of market segments, the institution must timely address such underperformance.

Advanced name matching technology is essential for an effective sanctions screening system, so that possible matches where data, whether in official lists or in an institution's internal records, is spelled differently due to transliteration, misspelled, incomplete, or missing, could be identified. Sanctions screening systems should be capable of applying fuzzy matching algorithms, i.e., an algorithm-based technique, the purpose of which is to match one name (a string of words), where the content of the information being screened is not identical but its spelling, pattern, or sound is a close match to the contents contained in a data set used for screening. Accordingly, sanctions screening systems should be calibrated in a way, for example, by calibrating the percentage of fuzzy matching, so that the screening system not only will alert an exact match (when an alert is generated if the system is presented with data that exactly matches a data in the screening list), but also in case certain manipulations would have been made.

The institutions should be aware that lowering the fuzzy matching percentage or altering the parameters of the algorithm will result in a higher number of alerts, part of which will be false positives. Evidently, this can negatively affect the efficiency of the screening system. Therefore, the institutions should calibrate the fuzzy matching parameters in a manner that ensures both – that the system is working as effectively as possible (no or minimal number of sanctions records are missed), but at the same time the screening system is working efficiently, i.e., sanction screening system is generating qualitative alerts and the screening system is not generating an extensive number of false positives that could require disproportionate resources for investigation of such alerts, result in backlogs and cause a series of operational risks and customer complaints. Assessment and testing should be carried out by the institutions to determine the appropriate calibration for the sanction screening system.

There are different types of fuzzy matching algorithms that could be applied. When evaluating which algorithms to apply more effectively or which algorithms to focus more on, an appropriate

assessment and testing should be carried out. The table below shows commonly used fuzzy matching algorithms:

| Text Matching | Text Manipulation | Word Manipulation | Date Adjustment |
|---|---|---|---|
| Soundex | Text Character Add | Word Delete | Add Subtract Date |
| Levenshtein Distance | Text Character Delete | Word Swapping | Swap Day and Month Date Valid |
| Metaphone 3 | Text Character Add and Delete | Word Joining | Swap Decade of Year |
| | Text Character Reversing | Word Separating | |
| | Text Contextual Start | Word Moving | |
| | Text Contextual End | Abbreviation Combined | |
| | Text Contextual Complete | Abbreviation Combined Dot | |
| | Fat Finger Replace | Abbreviation Combined Space | |
| | Text Character Add Repetition | Abbreviation Combined Dot Space | |
| | Text Character Remove Repetition | Word Joining with Hyphen | |
| | Text Alphanumeric Swap | Word Reordering | |
| | Text Phonetic Character Replace | Add Initial | |
| | Text Character Add Special Characters | Add Initial Dot | |
| | Initial Letters Change | Name Duplicate | |
| | Add Subtract Number | Duplicated Name Remove | |
| | Number Add | Initial Join Space Delete | |
| | Number Swap | Digit to Text | |
| | Number Remove | Text to Digit | |
| | | Ordinal Number Abbreviate | |
| | | Ordinal Number Expand | |

| Determining fuzzy matching parameters and deciding on additional controls with the aim to improve screening efficiency | |
|---|---|
| **Good Practice** | **Poor Practice** |
| The institution has calibrated the fuzzy matching parameters to a certain level that ensures that the screening system is working both effectively and efficiently. The parameters have been determined and validated based on comprehensive testing, where different models were tested.<br><br>The institution has developed a testing environment that is as close as possible to the institution's production environment. The testing was carried out and documented by the institution before implementing the settings in the production environment. According to the internal regulations of the institution, the institution re-assesses the determined parameters within a certain regularity and makes necessary changes, which are tested and validated before implementation in the production environment. | The institution has decided to change the parameters of the fuzzy matching in order to increase the effectiveness for screening manipulated data. However, the institution has not assessed how such changes will affect the efficiency of the screening system.<br><br>As a result of this decision, the institution's employees are faced with a significantly higher number of alerts per day. The employees cannot manage to investigate the alerts within the determined time frame in a qualitative manner. Therefore, alerts are closed as false positives without proper investigation. |
| The institution has implemented additional measures to increase the efficiency of the sanction screening system, such as the whitelist, where the system suppresses common alerts that are false positives.<br><br>The institution has clear procedures that determine the creation and usage of such lists, including how such lists are reviewed, updated, amended, etc. The institution regularly assesses the effectiveness of this measure, carries out relevant testing, and implements appropriate changes when necessary. | The institution has implemented additional measures to increase the efficiency of the sanction screening system, i.e., whitelist.<br><br>However, as the institution does not have clear procedures that regulate the usage of such lists, the institution has not included the whitelist in the scope of data that the institution should regularly screen against that would allow to identify instances when the list should be reviewed and updated. Therefore, for example, if a new sanction regime has been imposed, the institution is now exposed to the risk that the whitelist contains data that should potentially generate a positive match. |

### 7.6.4 Sanctions screening systems tuning

Tuning screening system parameters needs to be undertaken in an evidence-based manner to ensure configurations are aligned to the institution's risk-based approach. Configurability of the sanctions screening technology in place needs to be addressed at the procurement and implementation stage to enable the ongoing tuning to risk. The ability to continually optimize the technologies and usage of data needs to be undertaken on a periodic basis. Tuning should be undertaken in line with testing frameworks and should be targeted at the tuning stage for effectiveness and efficiency-reducing false positives whilst not sacrificing effectiveness levels. Tuning should be iterative with audit capabilities, and reporting should be established to be escalated internally to stakeholders.

### 7.6.5 Over reliance on vendors

Technology third-party vendor reliance continues to be prevalent in organizations as they look to rely on the implementation and technologies prescribed by vendors without proper evaluation and assessment. Screening technology providers are heavily relied upon in the configuration of system settings and rules without proper oversight from responsible persons, which can lead to incorrect or erroneous system configurations. Institutions must understand that off-the-shelf solutions from vendors may not meet and combat all their potential risks in which customization and tuning would need to be undertaken after testing is completed.

### 7.6.6 Group-wide system management

If there is a group-wide screening policy, localization measures and controls need to be provided to local offices to meet local regulatory obligations.

## 7.7. Sanctions data

### 7.7.1 Sanctions list selection and management

Appropriate sanctions lists are to be selected in accordance with regulatory agreements in place with other territories, exchange control agreements (e.g., OFAC when dealing in USDs), which enable trade relations, and any separate legislative prescriptions. Internal lists that prohibit

relationships with certain parties can and should be included in screening configuration. Lists are updated by governments and other sanction sources daily (such as OFAC, HMT, and EU). Sanctions lists include individuals, entities, vessels, aircraft, banks that have been sanctioned, and Dual-Use Goods (goods with more than one useful purpose). E.g., uranium can be used for energy generation but also in creating weapons of mass destruction.

Commercial lists are available for procurement and are developed in the format required for screening system use. Commercial list providers retrieve list records from official published sources and provide consolidated list services to institutions in need. List providers are private companies and not the official source of sanction data. Thus, they carry the risk of not updating records immediately, making errors in spelling of names, and incorrectly classifying records. Institutions should show that the selected sanctioned lists from the chosen commercial list vendor are comprehensive and efficient enough to detect all sanctioned parties and are updated with source updates. This can be done by comparing the content and customer support of commercial list vendors.

United Nations Sanctions Lists, as highlighted in Section 5 herein, should mandatorily be included in the screening process as per the FIA and PACOTPAA. Below are some considerations on determining sanctions lists to be screened against and determining and documenting any limitations for screening particular lists.

| **Determining sanctions lists to be screened against and determining and documenting any limitations for screening particular lists** | |
|---|---|
| **Good Practice** | **Poor Practice** |
| | |

| | |
|---|---|
| The institution has carried out a comprehensive risk assessment. The institution has further identified that in addition to transactions in NAD or EURO, a large proportion of transactions are made in USD and GBP currencies. Therefore, in addition to the mandatory sanction's lists – European Union (hereinafter – the EU), United Nations (hereinafter - the UN), the sanctions imposed by the U.S. Office of Foreign Assets Control (hereinafter – OFAC) and United Kingdom HM Treasury (hereinafter – HMT) shall also be screened against.<br><br>Additionally, considering institutions' client base and offered products, which include trade finance products, the institution decides to develop and screen transactions against a Dual-Use[19] Item list. | The institution is screening against the EU, UN, OFAC, and Latvian sanction lists. However, the institution in its sanction risk assessment has not assessed its transaction data, i.e., currency in which transactions are made and transaction flow to different jurisdictions.<br><br>In fact, a significant number of transactions in different currencies are made to the United Kingdom. Therefore, without screening against the HMT list, the institution might be exposed to a risk that the institution could be involved in violation or circumvention of sanctions imposed by the United Kingdom, which, among other things, can cause legal and reputational risks. |
| The institution, after a thorough risk assessment, concluded that due to alternative and demonstrable effective controls, screening against *"Weak Aliases"*[20] is not efficient because the sanction screening system is generating too many false positives, which is negatively affecting the overall efficiency of the sanction screening system. Further, there is a small likelihood that screening against *"Weak Aliases"* would allow the institution to identify a sanctioned individual or entity, considering that there are other demonstrable effective control measures in place to mitigate risks.<br><br>OFAC does not explicitly require screening against *"Weak Aliases"* [21] , however, other authorities (EU and UN) have not made a clear | The institution is not screening against *"Weak Aliases"*; however, the institution has not documented such a decision and has not assessed associated risks with such a decision. Additionally, the institution screens against a sanction list that is provided by a third-party vendor.<br><br>The third-party vendor also categorizes name types of designated individuals/entities in accordance with the official sanction lists, which allows to identify which name type is a *"Weak Aliases"*. However, in addition to the official categorization, the third-party vendor, in order to make the screening more effective, has developed its subjective categorization, where, based on certain principles, the third-party vendor |

[19] Termin "Dual-Use Items" in the context of this document means goods, software, and technology that can be used for both civilian and military purposes, especially used for terrorism.
[20] A "weak alias" or "weak also known as" is a term for a broad or generic alias of a sanctioned individual or entity and is included in the official sanction list that may generate a large volume of false hits when such names are run through a computer-based screening system.
[21] OFAC has stated that OFAC's regulations do not explicitly require any specific screening regime. Financial institutions and others must make screening choices based on their circumstances and compliance approach. As a general matter, though, OFAC does not expect that persons will screen for weak AKAs but expects that such AKAs may be used to help determine whether a "hit" arising from other information is accurate. Office of Foreign Assets Control (treasury.gov)

| | |
|---|---|
| statement about the mentioned aspect. In Namibia, **institutions are cautioned to not establish or create *weak aliases* with the UNSC sanctions as the UNSC does not make provision for the same.**<br><br>Considering all the above-mentioned and taking into account various alternative controls - an institution may decide not to screen against *"Weak Aliases"* (on non-UNSC lists). It is essential to document such decisions and reasons for them. The reasons for the decision should be clearly stated and justified (including with testing, where appropriate) and relevant risks that arise from such decision outlined. | can decide to re-categorize a name type, e.g., what in the official sanction list is referred to as *"Strong"*, the third-party vendor can categorize as "Weak".<br><br>However, the institution is not aware that the third-party vendor is performing such re-categorization of name types. Therefore, the institution is not aware of the risks that are associated with such a decision not to screen against such name types that, according to official lists, are *"Strong"*, but according to the third-party vendor, are identified as "Weak Aliases". |

### 7.7.2 Segmentation

Segmentation is the process of segmenting lists within data sets to screen at appropriate configurations depending on the risk. Sanctions, Politically Exposed Persons (PEP), and adverse media data should be segmented in the screening process to ensure that a risk-based approach is implemented. Segmentation allows for the ability to tune to different thresholds for screening based on risk and enables the ability to tune for greater efficiency utilizing exact matching versus fuzzy logic. The guidance in the table below is worth noting.

| **Determining relevant data categories to be screened against** | |
|---|---|
| **Good Practice** | **Poor Practice** |
| Upon onboarding a customer, the institution carries out a comprehensive know your customer | Upon onboarding a customer, the institution carries out a comprehensive know your customer |

| | |
|---|---|
| process, during which, amongst others, the ownership structure, beneficial owner, individuals who have the power to represent the customer, and other persons connected to the customer, such as natural and legal persons within the management or ownership structure, who may be controlling or exercising a dominant influence, are identified. The institution regularly screens its customer base, including the customer itself, the customer's representatives, the beneficial owner, and other related persons who could be capable of exercising control or dominant influence over the customer. The institution has determined and documented which data categories shall be screened against, for example, name and surname/company title, date of birth, registration number, nationality, address, etc., to ensure that the screening results provide the most accurate results.<br><br>The institution ensures that the know your customer information remains up-to-date and ensures that, in case of changes, the customer and its related persons are screened. | process, during which all the necessary information is acquired. However, the institution regularly screens only its customers, its representatives, and customers' beneficial owners. Therefore, when a legal entity that owns the majority of the customer's capital shares is designated, the institution fails to identify that the customer's funds must be immediately frozen because this information has been excluded from the screening system. |
| For transaction screening, the institution has identified which data categories shall be screened against, e.g., names of parties involved in the transaction, financial institutions, including correspondent banks involved in the transaction, free text field, address field, IP address (that is relevant to ensure compliance with sectoral sanctions applying to certain regions).<br><br>The institution has taken into consideration the differences in different types of transaction messages (e.g., for SEPA and SWIFT payments). | The institution provides trade finance services and has implemented certain controls to manage risks related to sanctions. However, the institution has not defined clear procedures that would outline all data categories that should be screened against when trade finance services are provided.<br><br>Employees, who are responsible for carrying out manual checks of the presented trade finance documentation, fail to screen information about the vessel involved in the transaction (including International Maritime Organisation (IMO) numbers). Thereby, the institution fails to identify that the vessel involved in the trade finance deal has been sanctioned. |

### 7.7.3 Whitelisting

Whitelisting, or ‘Good guy’ list usage, is the implementation of rules and configurations to automatically eliminate potential hits from screening. Whitelisting enables organizations to drive greater efficiency in screening practices.

## 7.8. Testing and audit

### 7.8.1 Independent and objective

Testing of sanctions screening systems and validation should be independent of the compliance function and executed either by third parties or internal audit. The assessment and testing need to be objective and carried out by skilled practitioners with detailed metrics and analytics. Reporting should be provided to the organization that aligns with overall effectiveness and efficiency goals set out by senior management. Testing should utilize dummy/synthetic data, fit-for-purpose, and clean identification for further efficiency testing. Testing is a mandatory requirement for all institutions to ensure they understand their TFS requirements and implementation of a program to identify any potential sanctions risks.

### 7.8.2 Frequent testing and validation

Testing of sanctions screening systems and the assessment and validation of sanctions screening processes and frameworks should be undertaken in a frequent and ongoing manner. Frequency should be risk-based, with the frequency thereof depending on the scale and risk assessment undertaken by the institution. Testing should be iterative and should utilize a consistent methodology with reporting to senior management of results on a regular basis with the overall effectiveness of the sanctions screening compliance program to be reported to senior management. Peer comparative data should be utilized in testing to ensure system performance is meeting industry benchmarks.

### 7.8.3 Pre and post implementation testing

Thorough, rigorous, and robust testing at pre- and post-implementation of new or updated systems needs to be undertaken before systems go live to ensure relevant controls are in place to identify potential sanctioned individuals and entities. Testing should be undertaken on all parts of the technology with a clear audit trail of testing.

### 7.8.4 Testing frameworks

Testing frameworks should be defined within the organization's policy and utilized by Responsible Persons. Testing frameworks should be based upon evidence and documented tuning practices. Testing should enable institutions to understand system performance, diagnose deficiencies and weaknesses within the technologies or data, and allow for configuration support and a clearly documented methodology.

### 7.8.5 Ongoing supervisory testing and reporting

The FIC may request institutions to provide ongoing testing results of their sanctions screening systems[22] and program as well as continue to undertake the TFS thematic review of the effectiveness and efficiency of sanctions screening systems, selecting, and testing accountable and reporting institutions.

## 8. 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 an institution's responsibility to demonstrate alternative risk management controls implemented that are as effective.

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

**DATE ISSUED: 25 OCTOBER 2024**
**DIRECTOR: FINANCIAL INTELLIGENCE CENTRE**

[22] In terms of the FIA section 9 and section 20A(6)('c) of the 2023 FIA amendments

## 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