

Financial Intelligence Centre Republic of Namibia

> PO Box 2882 Windhoek Namibia

Phone: + 264 61 283 5100 Fax: + 264 61 283 5259 helpdesk@fic.na

GUIDANCE NOTE NO 5 OF 2015

REVISED GUIDANCE NOTE ON INTERVENTION ORDERS ISSUED IN TERMS OF SECTION 42 OF THE FINANCIAL INTELLIGENCE ACT OF 2012 (ACT NO. 13 OF 2012)

First issued: November 2011

Revised and issued in: December 2015

Safeguarding Financial Integrity

TABLE OF CONTENTS

- A. DEFINITIONS
- 1. Introduction
- 1.1 General
- 1.2 Background
- 1.3 Commencement
- 2. The Financial Intelligence Centre (FIC)
- 2.1 Functions of the FIC
- 3. Understanding money laundering, terrorism and proliferation financing activities
- 3.1 Money Laundering
- 3.2 Terrorism financing
- 3.3 Proliferation financing
- 4. Understanding the intervention: Section 42 of the FIA
- 4.1 Key notable compliance deficiencies
- 4.2 Recommended best practices
- 5. Tipping off
- 5.1 Understanding the offence of tipping off
- 5.2 Protection of confidential information (s49): May you tell a client(s) that the FIC had frozen their accounts(s) and/or transaction(s)?
- 5.3 The FATF position on disclosure of information and "tipping off"
- 5.4 What may an accountable or reporting institution tell an irate client if his or her transaction(s) and/or account(s) had been frozen by the FIC?
- 6. Penalties for non compliance

6.1 Penalties for non-compliance with intervention directives by the Centre as per section 42 of the Act

6.2 Penalties for offences of tipping off or providing confidential information (s46 and s49)

6.3 Non-compliance with the provisions of this Guidance Note

7. Comments

8. How to contact the FIC

A. DEFINITIONS

"Accountable or reporting institution" means a person or entity listed in schedule 1 and 3 of the Act;

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

"CDD" means Customer Due Diligence;

"Client and Customer" have their customary meaning and are used interchangeably;

"**Customer due diligence**" 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 customer due diligence" means doing more than the conventional customer due diligence 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;

"FATF" means the Financial Action Task Force. The Financial Action Task Force (FATF) is an inter-governmental body established to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FIA is aligned to the FATF Recommendations;

4

"FIA" the Financial Intelligence Act, 2012 (Act No. 13 of 2012), as amended (also referred to as the Act);

"FIC" means the Financial Intelligence Centre (Referred to as the Centre in the Act);

"ML" refers to Money Laundering;

"**POCA**" refers to the Prevention of Organized Crime Act, 2004 (Act No.29 of 2004), as amended;

"**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 activities report submitted to the FIC in terms of sections 33 (1)(b) of the Act;

"STR" refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1)(b) of the Act;

"TF and PF" refers to Terrorism and Proliferation Financing activities

"**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. INTRODUCTION

This Guidance Note is applicable to all accountable and reporting institutions as set out in schedules 1 and 3 of the Act and is issued and published by the FIC in terms of section 9(h) of the Act. The Guidance Note has been prepared to help all accountable and reporting institutions implement measures to enhance compliance with obligations under section 42 of the Act.

Guidance provided by the FIC is the only form of guidance formally recognized in terms of the Act and its complementing regulations. Viewed from this perspective, guidance emanating from industry associations or other organizations, except Supervisory Bodies (SBs), does not necessarily have a bearing on assessing compliance with the obligations imposed by the Act or the interpretation of its provisions.

1.1 General

The Act empowers the FIC, to provide guidance to accountable and reporting institutions regarding obligations set forth in the Act. This Guidance Note provides guidance that accountable and reporting institutions may apply when dealing with Interventions by the FIC, as per Section 42 of the Act. Accordingly, this Guidance Note is primarily directed at accountable and reporting institutions, but can be used by SBs as listed in Schedule II of the Act in their supervisory capacities over accountable and reporting institutions.

This Guidance Note is intended to explain, but not to replace the language of the Act and the regulations issued under the Act. Accountable and reporting institutions' internal compliance rules may cover situations other than the ones described in this Guidance Note for purposes other than accountable and reporting institutions requirements under the Act.

1.2 Background

This Guidance Note has been issued to help accountable and reporting institutions to develop and put systems in place that will assist in complying with the sections of the Act on Interventions by the FIC. For the purposes of this Guidance Note, where reference is made to a specific category of accountable or reporting institutions, e.g. banks, the guidance that is part of that reference applies to that category of accountable or reporting institutions only.

The principal objective of the FIC, under the Act is to help various stakeholders (including accountable or reporting institutions) meet their obligations in combatting money laundering (ML), terrorism financing (TF) and proliferation financing (PF) activities. In furtherance of this objective, the Act requires accountable and reporting institutions to take certain measures to mitigate the risk of ML/TF and PF Activities. This Guidance Note focuses on one such obligation, which is the obligation to comply with Interventions by the FIC, as set out in Section 42 of the Act. In summary, the section empowers the FIC to intervene by directing an accountable or reporting institution in possession of suspected proceeds of unlawful activities or proceeds which may constitute money laundering or the financing of terrorism or proliferation activities; in writing not to proceed with the carrying out of that transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period determined by the FIC, which will not be more than 12 working days at a time. The purpose of this intervention would be to hold such proceeds beyond the reach of suspected criminals or terrorists pending investigations to establish their true source or purpose.

This guidance note was developed to:

- Provide guidance on how institutions can enhance their compliance with section
 42 of the Act; and
- as a result of numerous enquiries to the FIC from accountable and reporting institutions wanting to know what they should tell their clients when the FIC,

issued an intervention order under Section 42 of the Act, which results in freezing of all or certain transactions on a client's account.

This document provides guidance on measures that can enhance effective compliance with section 42, without escalating the risk of "Tipping off" clients as contained in sections 46 of the Act.

1.3 Commencement

This guidance note shall come into effect on date of publication on the FIC website.

2. THE FINANCIAL INTELLIGENCE CENTRE (FIC)

The principal objects of the FIC are to help the Government of the Republic of Namibia combat ML,TF and PF activities in collaboration with the other law enforcement agencies and relevant stakeholders. In furtherance of this objective, the FIC, amongst others, receives STRs and SARs from accountable and reporting institutions, analyze such reports and disseminate the financial intelligence gathered on suspected money laundering, terrorist and proliferation financing activities to law enforcement agencies, both domestic and international, for further investigation and possible prosecution.

The FIC is further empowered to conduct compliance audits/inspections on accountable and reporting institutions in order to enhance compliance with the provisions of the Act. Issuing guidance such as this document is another effort to enhance the compliance behaviour of stakeholders.

3. UNDERSTANDING MONEY LAUNDERING, TERRORISM AND PROLIFERATION FINANCING ACTIVITIES

3.1 Money laundering

In simple terms, money laundering is the Act (or attempt to) of disguising the true source of proceeds of unlawful activities. The Act further defines "money laundering" or "money laundering activity" as the act of a person who -

- i. engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity;
- ii. acquires, possesses or uses or removes from or brings into Namibia proceeds of any unlawful activity; or
- iii. conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of any unlawful activity;

3.2 Terrorism financing

3.2.1 The meaning of terrorism

Whilst no acceptable international definition on terrorism exists, it is generally described as the execution of acts of violence against persons or property, or a threat to use such violence, with the intent to intimidate or coerce a Government, the public, or any section of the public to achieve or promote any tribal, ethnic, racial, political, religious or ideological objectives¹.

3.2.2 Understanding the financing of terrorism

Financing of terrorism involves the provision of funds to enable the commission of terrorism or terrorist activity. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as funds derived from criminal activity, such as drug trafficking, illegal diamond smuggling, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

¹ See full definition of "terrorist activity" as provided for in section 1 of the Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014)(PACOTAPAA)

Recent trends indicate that terrorism activities are also funded by proceeds from artefacts, social media fund raising activities, selling of oil etc.

3.2.3 Understanding how financing of terrorism is committed

Terrorists use techniques similar to those used by money launderers in order to evade the attention of the authorities and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. Financial transactions associated with terrorist financing tend to be in smaller amounts than is the case of money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds are difficult. Those involved in acts of terrorism or financing of terrorism, move their funds by using the formal banking system, money transfer services, informal valuetransfer systems like the Hawalas, the physical cross border transportation of cash, uncut diamonds, gold and other valuables such as the sale of artefacts, oil and fundraising in other means such as social media. It has been noted in some countries that, in what seem to be an effort to conceal the final destination of funds suspected of being used for terrorist financing, money is moved to countries that has major financial hubs. For example, remittances made for non-existent or fictitious imports. It has also come to the fore that large amounts of money are remitted to certain jurisdictions on the basis of highly inflated invoices.

3.2.4 Targeted financial sanctions related to terrorism and terrorist financing

Countries, Namibia included, are required to implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require Namibia and other countries who are UN member states to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either:

i. designated by, or under the authority of, the mandatory United Nations Security Council Resolutions issued under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or

ii. designated by that country pursuant to resolution $1373 (2001)^2$.

The various lists of persons or entities designated by, or under the authority of the mandatory United Nations Security Council Resolutions issued under Chapter VII of the Charter of the United Nations can be accessed on the FIC website (www.fic.na) or on https://www.un.org/sc/suborg/

3.3 Proliferation financing

3.3.1 Understanding Proliferation financing

Proliferation financing is defined by Financial Action Task Force (FATF)³ as the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations⁴.

3.3.2 Background on Proliferation financing

Proliferation financing facilitates the movement and development of proliferationsensitive items and as such, can contribute to global instability and potentially catastrophic loss of life if weapons of mass destruction (WMD) are developed and deployed. Proliferators operate globally and mask their acquisitions as legitimate trade.

² The International standards on combating money laundering and the financing of terrorism & proliferation, the Financial Action Task Force (FATF) recommendations, February 2012

³ Combating proliferation financing: A status report on policy development and consultation, FATF Report, February 2010

⁴ Also see the definitions of "funding of proliferation" and "proliferation activity" as provided for in section 1 of the PACOTAPAA

They exploit global commerce, for example by operating in countries with weak export controls or utilising free-trade zones, where their illicit procurements and shipments are more likely to escape scrutiny.

Proliferators abuse both the formal and informal sectors of the international financial system or resort to cash in order to trade in proliferation relevant goods. It should be noted that organized networks, which make use of the formal international financial system, may be easier for authorities to detect than those using informal sectors. When abusing the formal international financial system, purchases must appear legitimate to elude suspicions, as proliferation-sensitive goods and services may be purchased on the open market. Proliferation networks also use ordinary financial transactions to pay intermediaries and suppliers outside the network. Proliferation support networks therefore use the international financial system to carry out transactions and business deals, often acting through illicit intermediaries, front companies and illegal trade brokers. These procurement networks have become significantly more complex over time, increasing the probability that the true end-users of proliferation sensitive goods will avoid detection. Financial institutions are usually unwitting facilitators of proliferation.

3.3.3 Targeted financial sanctions related to Proliferation

Namibia has implemented targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require Namibia (along with other countries) to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the mandatory United Nations Security Council Resolutions issued under Chapter VII of the Charter of the United Nations.

On a practical level, all Accountable and Reporting Institutions should observe the various United Nations Sanctions Lists, which contain lists of designated persons and entities. The institutions should then compare their client database to these lists and if

matches are identified, business activities with such clients should cease immediately and such matches should immediately be reported to the FIC. These lists can be accessed on the FIC website (<u>www.fic.na</u>) or directly on <u>https://www.un.org/sc/suborg/</u>.

4. UNDERSTANDING THE INTERVENTION: SECTION 42 OF THE FIA

In summary, section 42 of the Act states that if the FIC, after consulting an accountable or reporting institution, has reasonable grounds to suspect that a transaction or a proposed transaction may involve the proceeds of unlawful activities or may constitute money laundering, the financing of terrorism or proliferation activities; it may direct the accountable or reporting institution in writing not to proceed with the carrying out of that transaction or any other transaction in respect of the funds affected by that transaction or proposed transaction for a period determined by the FIC, which will not be more than 12 working days at a time, in order to allow the FIC -

- a) to make the necessary inquiries concerning the transaction; and
- b) if the FIC thinks it appropriate, to inform and advise an investigating authority or the Prosecutor-General.

Part of combatting ML/TF and PF activities entails placing proceeds from unlawful activities or funds and property meant to advance TF and PF activities beyond the reach of such suspected criminals and terrorists. In furtherance of this purpose, the section empowers the FIC with the means to direct that involved proceeds be frozen for a certain period, until such time that investigations can reasonably establish the source or purpose of such proceeds. The process that may result in placing funds or/and property beyond the reach of suspected criminals or terrorists prudently commences with the:

- freezing, seizing; and, if need be
- confiscating under the Prevention of Organised Crime Act, as amended (Act No. 29 of 2004) (POCA) or any other law applicable to the Republic of Namibia.

The FIC has strict standards in place to ensure that section 42 is invoked only in those circumstances where intervention is an absolute necessity. One of such circumstances

is where a risk exists that carrying out a transaction may result in possible proceeds of crime (or funds related to TF/PF activities) leaving the country and/or proceeds of crime being placed outside the reach of law enforcement agencies.

4.1 Key notable compliance deficiencies

The FIC has sadly noted the following trend, in the implementation of section 42 intervention directives:

- a. The FIC issues a written intervention directive to an accountable or reporting institution in terms of the Act;
- b. The accountable or reporting institution acknowledges receipt of the intervention directive to the FIC; and
 - i. Implements measures such as placing a *block or hold* on the relevant account to prevent further withdrawals of funds from the concerned account;
 - ii. Unfortunately, the FIC has also noted that in some instances, the *hold or block* placed on the account is not adequate and clients are still able to withdraw funds despite the intervention directive from the FIC. In some instances, it was stated that the staff members employed to assist with over the counter withdrawals by clients will hopefully read the *hold or block* notice on such account and not assist client with such withdrawals;
- iii. In some instances, where the *hold or block* indeed restricts the actual withdrawal of funds, account managing employees of the accountable or reporting institution were found to have requested persons, with authority (in the system employed) but are not involved in managing ML/TF and PF risks to remove such a *hold or block* from the account (on the operating system), thereby enabling the client access to withdraw funds from such accounts.

4.2 Recommended best practices

With due consideration to control weaknesses relating to compliance with section 42 of the Act, the FIC emphasizes the following:

- Accountable and reporting institutions implement, as a matter of urgency, control measures that will consistently ensure that intervention directives, as per the Act are complied with;
- At a practical level, such controls (especially automated system controls) are implemented to deny complete access to funds for the required period, in terms of an intervention directive; and equally
- c. Implement additional measures necessary to guide and help staff members uphold such controls implemented in terms of section 42.

With regard to the noted trends stated above (4.1), the FIC emphasizes that there has to be an appreciation of the fact that personnel (staff members) in an accountable or reporting institution are part and parcel of the entire control environment, aimed at mitigating risks. Personnel do not function in isolation from the automated systems and neither do automated systems function in isolation of the personnel. For senior management to gain reasonable assurance on control effectiveness, the controls of automated systems ought to support personnel in discharging their duties and viceversa.

It is for this reason that failure by personnel to play their part to ensure compliance with section 42 intervention directives cannot be separated from notable control weaknesses in automated systems. A failure by either the automated system or personnel is therefore a failure by the entire control system employed by an accountable or reporting institution. It is with this appreciation that section 39 of the FIA deliberately outlines measures to enhance the effectiveness of staff members in enforcing AML/CFT/CFP controls. The following are some practical examples of best practices which demonstrate how the combination of automated systems and personnel functions are structured or positioned to enhance compliance with section 42 of the Act:

16

- Automated controls: If a *hold or a block* is placed on an account in terms of section 42, the Information and Communication Technology (ICT) system in place, on which accounts are operated and managed has to terminate access to such funds for the required period;
- ii. Authority/Supervisory approvals: Firstly, authority to place and remove a block or hold on an account (in terms of section 42) should be limited to the most suitable persons in an accountable or reporting institution, with the necessary level of seniority and understanding of the FIA. It therefore goes without saying that such authority should only be granted to persons such as the AML Compliance Officer, with/or the Head of Compliance with/or/and the Managing Director. Accountable and reporting institutions would need to determine the most suitable approach given the internal risk exposure or vulnerability of control system(s) to honour intervention directives;
- iii. Staff integrity: Without questioning the level of integrity of staff members in accountable or reporting institutions, the establishment of procedures to ensure high standards of integrity of its employees and a system to evaluate the personnel, employment and financial history of those employees, as set out in section 39 of the Act is critical in enhancing compliance with Section 42;
- iv. Staff training: On-going employee training programmes should include compliance with important sections of the FIA such as intervention directives. It should be appreciated that staff need to be trained to not only comply with intervention directives, but equally understand how to advise clients without running the risk of "tipping off", which is an offense that can prejudice on-going or future investigations;

Other general controls which may be tailored to enhance compliance with section 42 include:

- v. Audit: Periodically subjecting the controls designed to enhance compliance with section 42 to an independent audit function, may help management understand the level of assurance it can place on implemented controls relating to compliance with this section of the Act. The FIC's compliance assessment reports on some accountable institutions consistently calls for scope expansion to ensure that audit tests are escalated beyond Know Your Customer (KYC) control tests. The materialization of these risks is what was anticipated in such FIC reports;
- vi. Policies and procedures: Policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value. For example, a relationship manager or ICT support staff member should not have the authority to override section 42 related controls placed on an account. There should also be in-house policies and procedures to deal with queries and client persistence related to section 42 interventions;
- vii. **AML/CFT/CFP Policy:** All controls relating to compliance with section 42 should be documented in the accountable or reporting institutions' approved AML/CFT/CFP policy.

5. TIPPING OFF

5.1 Understanding the offence of tipping off

Section 46 of the Act describes a tipping off offence as one where a person who -

(a) knows or has reason to suspect that an authorised officer is acting, or is proposing to act, in connection with an investigation which is being, or is about to be, conducted under or for the purposes of this Act and who discloses to any other person information or any other matter which is likely to prejudice that investigation or proposed investigation;

or

(b) knows or has reason to suspect that a disclosure has been made to an authorised officer under this Act and discloses to any other person information or any other matter which is likely to prejudice any investigation which might be concluded following the disclosure,

From the above, the underlying objective of preventing tipping off is to minimize the risk of unduly exposing confidential information to persons with no need to know, which may in turn prejudice ongoing investigations.

5.2 Protection of confidential information (s49): May you tell a client(s) that the FIC had frozen their account(s) and/or transaction(s)?

An accountable or reporting institution or any employee of that accountable or reporting institution may not inform any person, least of all the involved client(s), that the FIC had frozen the client's account(s) and/or transaction(s) through the issuance of an intervention directive. Disclosure of such information may amount to "tipping off" which is a criminal offence in terms of the Act. According to guidance received from the FATF and international jurisprudence, a section 42 intervention directive is considered as falling within the category of information that is regarded as confidential information obtained from a Financial Intelligence Unit, such as the FIC. Section 49 speaks about protection of confidential information. The section states that a person may not disclose confidential information held by or obtained from the FIC except –

- a. within the scope of that person's powers and duties in terms of any legislation;
- b. for the purpose of carrying out this Act;
- c. with the permission of the FIC;
- *d.* for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
- e. in terms of an order of a court.

Additionally, a person who has obtained information from the FIC under this Act may not, when he or she is no longer authorised to keep the information under this Act, make a record of the information, disclose or communicate the information in any circumstances.

It is therefore clear that our legislature wanted to ensure that a client should not be tipped-off when a STR or SAR is reported to the FIC or when disclosure of related information has the potential to prejudice investigations. The moment an accountable or reporting institution advices a client that an intervention directive has been filed by the FIC, such a client may unintentionally be tipped-off and such tipping-off may prejudice an investigation or contemplated investigation pertaining ML/TF and PF, involving such client.

5.3 The FATF position on disclosure of information and "tipping-off"

In support of the above-mentioned guidance, accountable or reporting institution and Supervisory Bodies are referred to essential criteria contained under Recommendation 14 of the FATF's Forty Recommendations on Money Laundering and the Interpretative notes to both Recommendations 5 and 14.

Recommendation 14's essential criteria (2) prescribes that Financial institutions and their directors, officers and employees (permanent and temporary) should be prohibited by law from disclosing (tipping off) the fact that a STR or related information is being reported or provided to the FIU.

Furthermore, Interpretative Note to Recommendation 5 in 5(2) states:

"Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation."

For the sake of absolute certainty the FIC also sought advice on this matter from the FATF Secretariat who advised that, whilst it may be possible for Accountable or reporting institutions to know when investigations are being conducted, it is extremely difficult to gauge whether a future investigation may be done as a result of an intervention directive or STR or SAR being filed. They further confirmed that by telling a client that a STR or SAR has been filed or that an intervention directive from the FIC prevents transactions on an account, an accountable or reporting institution directly runs the risk of committing a tipping-off offence. The FATF Secretariat further noted that alerting a client that a report has been made or that investigations may be done, directly negates efforts to preserve proceeds of suspected crimes (or those advancing TF and PF activities) until such time that freezing orders can be obtained in a court of law. If the proceeds of suspected crimes are not preserved, the client may embark on hiding assets from law enforcement agencies, which may be the subject of freezing, seizing and confiscation orders.

5.4 What may an accountable or reporting institution tell an irate client if his/her transaction(s) and/or account(s) had been frozen by the FIC?

The FIC confirms that we do not foresee any problem with an accountable or reporting institution advising its clients as follows, when queries are received on section 42 Intervention directives:

"We regret to inform you that, due to regulatory instructions from the relevant authorities, we cannot proceed with your instruction on your accounts. Said instructions are valid for a period of twelve (12) working days." We advise that a cautious approach should at all times be deployed when advising client's as to the reason why instructions on transactions cannot be executed. Any reference to the FIC, may amount to a contravention of either section 46 or 49 of the Act. Once a breach of either of these two sections has occurred, the FIC will not be in a position to condone non-compliance.

6. PENALTIES FOR NON COMPLIANCE

6.1 Penalties for non-compliance with intervention directives by the Centre as per section 42 of the Act

An accountable or reporting institution which fails to comply with a direction made under section 42(1) commits an offence and is liable to a fine not exceeding N\$100 million or, where the commission of the offence is attributable to a representative of the accountable or reporting institution, to such fine or imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

Failure to comply with an intervention directive may also subject the Accountable or Reporting institution to administrative sanctions as provided for in section 56 of the Act. As per FIC Directive 1 of 2015 issued on 04 December 2015, failure to observe instructions contained in an Intervention Order issued by the FIC amounts to gross negligence and is regarded as inexcusable. Such failure may result in proceeds of crime being placed beyond the reach of law enforcement and jeopardize criminal investigations. As such, non-compliance will inevitably be met with administrative sanctions in terms of section 56 of the FIA.

In summary, failure to comply with an Intervention directive may subject an Accountable or Reporting institution to both administrative sanction as well as criminal charges.

6.2 Penalties for offences of Tipping off or providing confidential information (s46 and s49)

A person(s) found to have committed an offence of tipping off is liable to a fine not exceeding N\$100 million or to imprisonment for a term not exceeding 30 years, or to both such fine and such imprisonment.

6.3 Non-compliance with the provisions of this Guidance Note

The Guidance provided herein is enforceable. Any non-compliance with the directions and guidance contained in this Guidance Note is an offence in terms of section 63 of the FIA.

In terms of Section 56 of the FIA non-compliance with this Guidance Note may also attract administrative sanctions and penalties.

7. COMMENTS

The contents of this Guidance Note shall be reviewed from time to time. Accountable and reporting institutions will be notified of any aspect that may necessitate revoking or amending any guidance set out in this Guidance Note. If you have any comments or suggestions to help improve this Guidance Note, please send your comments to the mailing address provided below.

8. HOW TO CONTACT THE FIC

All Correspondence and enquiries must be directed to:

The Director Financial Intelligence FIC P.O. Box 2882 No.71 Robert Mugabe Avenue Windhoek Republic of Namibia Tel: +264 61 2835100 Fax: +264 61 2835259 Email: <u>helpdesk@fic.na</u>