FINANCIAL INTELLIGENCE CENTRE

REPUBLIC OF NAMIBIA

P.O.BOX 2882, Windhoek

Tel: **+ 264 61 2835100, Fax +264 61 2835259**

Web address: www.fic.na

E-mail address: leoniedunn@fic.na

FINANCIAL INTELLIGENCE CENTRE

INDUSTRY GUIDANCE NOTE NO.2 OF 2012

ON

UNIT TRUST MANAGERS

NOVEMBER 2012

TABLE OF CONTENTS

1. INTRODUCTION

1.1 General

The Financial Intelligence Centre (FIC) performed compliance assessments during the fourth quarter of 2012 with the aim of gauging the level of compliance by Unit Trust Managers with the provisions of the Financial Intelligence Act, 2007 (Act no 3 of 2007) (FIA).

Due to generic weaknesses found in the Anti-Money Laundering programs of the various institutions that have been assessed, the FIC decided to issue a formal guidance to the industry to ensure that:

a) Identified weaknesses are addressed;

b) no competitive advantage exists in terms of compliance or non-compliance with the Act; and

c) Ensuring that the overall FIA compliance level is increased across the industry.

All Unit Trust Managers are thus hereby requested to take into account this guidance in reviewing their AML program, to ensure that their respective programs are aligned to the guidance in order to avoid any sanctions for non-compliance with the provisions of the FIA in the future.

1.2 Definitions

"FATF" means the Financial Action Task Force;

“Act” refers to the Financial Intelligence Act, 2007 (Act No 3 of 2007);

“Cash” in the context of this guidance note refer to any transaction whereby cash is deposited into the Unit Trust Managers account as part of an investment transaction;

“FIC” means the Financial Intelligence Centre;

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

"Regulations" refer to the regulations made under the provisions of section 48 of the Act and published by Government Notice No 74 of 2009 promulgated in Government Gazette No 4253 dated 5 May 2009;

"Reporter" refers to the person or entity making the suspicious transaction report;

"STR" refers to a suspicious transaction report submitted to the FIC in terms of section 21 of the Act.

1.3 Application of this Guidance Note

The FIC has prepared this Guidance Note to assist Unit Trust Managers in meeting their obligations in terms of the Act. It provides specific guidance on practical compliance with the provisions of the Act, with key interpretations and definitions provided on general misconceptions about the Act. This guidance note does not replace previous guidance notes issued in terms of the Act, but aims to compliment guidance previously given.

The guidance provided by the FIC in this Guidance Note, although authoritative, is provided as general information only aimed at assisting Unit Trust Managers to enhance the quality of their implemented Anti-Money laundering programs. It should be noted that failure to comply with the Act and its regulations constitutes an offence as defined in the Act. As this guidance explains to Unit Trust Managers on how to go about complying with the Act and its regulations, non-adherence thereto, may result in the Unit Trust Manager being non-compliant with the Act and its regulations which in turn, may lead to the Unit Trust Manager facing sanctions as provided for in the Act.

2 UNIT TRUST MANAGERS – DESIGNATED HIGH RISK SERVICES

2.1 General overview

The Financial Action Task Force (FATF), as the international standard setter for Anti-Money Laundering efforts, identifies the products or services offered by Unit Trust

Managers, as extremely vulnerable to money laundering abuse and thus require same to attract Anti-Money Laundering obligations when offered.

This guidance is thus focused on:

a) Describing this vulnerability;

b) Proposing measures to reduce the vulnerability; and

c) Ultimately, decreasing the inherent ML risk a Unit Trust Manager is exposed to.

2.2 Unit Trust Management Products, Services and Clients

2.2.1 Introduction

The Unit Trust sector is made up of mainly two types of clients or investors, namely:

a) Institutional Investor; and

b) Non-Institutional Investor

Although different types of Unit Trust products are offered to meet the individual client investment needs, the following have been identified as standard industry practice and serves as the basis for the Money Laundering risk assessment:

a) No investments are made before client acceptance or take-on forms are completed, which enables a client to be assigned with a unique investment reference or account number to use, when making investments;

b) Investors may make use of any of the available banking channels (Cash deposits, Cheque deposits, Electronic Funds transfers, etc.) when making investments, once the initial application process is completed successfully;

c) Investors must designate a bank account in their name to be used upon de-investment as no cash or cheque payouts are made;

d) Third party payments are made in exceptional cases with proper required client instruction as well as management approval obtained; and

e) No cash is received or handled at the Unit Trust Manager's office.

2.2.2 Money Laundering Risk posed by Unit Trust Management services

The ML risk posed by the provision of a Unit Trust Management service is heightened by the risk of receiving potential proceeds of crime into the trust account of the Unit Trust Manager. As such, the risk each client poses should be evaluated properly, based on the nature of each transaction and in the context of the individual client profile.

In general it is FIC's assessment that the potential ML risk for Institutional Investors is considerably low due to the following reasons:

a) Source of funds are known;

b) Institutional Clients are subjected to adequate supervision and oversight as well as enhanced procedures being applied, upon investment and de-investment; and

c) Investments are primarily made from and to authorized bank accounts.

On the other hand, the potential ML risk for non-institutional clients is considerably high due to the following:

a) Funds used in investments may involve significant amounts of cash with funds being deposited by any party directly into the Unit Trust Manager's account;

b) Inadequate client profiles in relation to source of funds used in investments; and

c) Inadequate automated or manual monitoring systems to review transactional behavior against established profiles.

See **Annexure A** for a list of indicators to use in terms of identifying and assessing the risks each respective client poses.

It is of utmost importance to note that a lack of information obtained in respect of the client and specifically the source of funds for the initial investment and where possible for future investments, places the Unit Trust Manager in a very unfavorable position as

far as meeting the obligation of identifying any unusual or suspicious transactions is concerned. This is largely due to the fact that the identification of unusual or suspicious transactions relies on the availability and accuracy of relevant client information. It is also worth noting the potential ML risk when an investor deposits cash directly into the unit trust account or places funds received from a third party directly into the unit trust account, in instances where the Unit Trust Manager failed to establish an accurate client profile. No reliance may be placed on the controls of the respective commercial bank involved, as the banks are exempted in terms of Paragraph 2.6 of the General Exemption Order (as published in Government Notice 75 of Government Gazette No. 4253 of 5 May 2009) to identify (KYC) the clients who deposit funds, onto the trust accounts of Unit Trust Managers, Legal Practitioners, etc. The banks as such are not required in terms of Exemption 16, to identify the depositor or source of funds in instances such as these and as such the Unit Trust Manager are required to have performed the necessary due diligence on its clients as required by the Act.

Should the behavior of the client or the terms on which the transaction is settled, not conform to the information collected, then the Unit Trust Manager should have a procedure or mechanism in place to ensure that these deviations be evaluated and a suspicious transaction report filed, if any efforts to obtain an explanation, fail to deliver any meaningful results.

3. INDUSTRY ANTI-MONEY LAUNDERING CONTROLS

3.1 General controls mitigating potential industry money laundering risks

The FIC has identified the following controls which are in place with the majority of the Unit Trust firms in the industry, which assist in mitigating the above mentioned ML risks:

a) No investments are allowed unless client is formally accepted and a unique reference number is assigned;
b) Periodic reviews are done to ensure that up to date and complete client records are kept on file or electronically;
c) All cash deposits are flagged; and

d) All de-investments are paid *via* an electronic funds transfer into a bank account designated by the investor.

NB: All Unit Trust Managers who do not have the above controls in place, are urged to align their AML programs with the points listed under (a-d) above as far as reasonably possible, in order to further mitigate the potential ML risks.

3.1.1 Developing of adequate AML Programs

An AML Program is considered as any documented proof of how the AI intends to comply with the provisions of the FIA. As such it may consist of only one document or a bundle of documents detailing the procedures, controls, rules, etc. implemented with the aim of protecting the entity from the potential abuse by criminals aiming to use the business, its products or services for the purpose of laundering proceeds of crime. This program must be approved at the highest management level and failure to adhere to the measures must attract disciplinary steps for the respective staff members.

An AML Compliance Officer should further be designated at management level. This person will be responsible for the implementation of the AML compliance program as well as being the contact between the institution and the FIC.

The AML program should at a minimum include the following:

a) Overview of the background, governance structure and management of the business;
b) Commitment and approval of senior management to comply with the Act;
c) Description of the key internal rules, procedures, policies, etc designed and implemented to ensure compliance with the Act;
d) Description of the key controls implemented to ensure that the above internal rules, procedures, policies, etc. are adhered to and that these are operating effectively;
e) Details on AML training provided or to be provided to staff;
f) Overview on the money laundering risks faced by the firm as identified by the management, considering the client base, services or products offered by the

firm and the location of the business;

g) Description of the independent review function implemented to provide management assurance that the key AML controls are working and that the entity complies with the FIA; and
h) Copies of the relevant documents supporting any of the above.

Unit Trust Managers are also referred to the Guidance Note No 4 of 2009 on the implementation of a compliance regime previously issued.

3.2 Specific controls recommended to Unit Trust Managers to mitigate the money laundering risks associated with Unit Trust Management services

3.2.1 **Establish a policy not to accept cash above a certain threshold**

As we live in a largely cash based economy and in a society whereby bank costs are considered a deciding factor when performing any banking transaction, the FIC **do not** recommend that **no** cash be allowed on investment. In general, it is recommended not to allow clients to make any cash deposits when investing above a certain threshold, especially if the client is a legal entity. There is no amount suggested as firms of different sizes would have to assess the potential money laundering risk associated with its business. This recommendation is made in light of the current industry practice whereby all funds upon de-investment are paid to a designated bank account via an electronic funds transfer, which assumes that all investors already own a bank account.

It is recommended that Unit Trust Managers **do not** refer clients to deposit cash directly into their bank accounts without performing the required customer due diligence. This does **not** in the FIC's opinion; reduce the ML risk posed by a cash transaction as the Unit Trust Manager would be regarded as the client by the bank in such a scenario. Thus no assurance is offered to the Unit Trust Manager as the bank would not subject the person depositing the money into the institution's account, to any customer due diligence procedures. The bank might however still report a suspicious transaction to the FIC should they believe that this transaction might involve proceeds of crime. This poses a risk to the Unit Trust Manager as the report might lead to a ML investigation

being launched by law enforcement, which might eventually lead to charges of ML being instituted against the Unit Trust Manager in line with the provisions of the Prevention of Organized Crime Act, 2004 (Act No.29 of 2004) as amended (POCA)[1].

3.2.2 **Third Party payments upon de-investment subject to management approval**

Should the client indicate that a payment is to be made to a third party, it is recommended that this transaction first be approved by the relevant Senior Management within the respective Unit Trust Firm, before transactions are honored.

It is further recommended that Unit Trust Managers ensure:

a) All the required identification information has been collected and verified;
b) Evaluate the information obtained in respect of the source of funds to be used in the transaction in line with the other client information obtained;
c) Subject the client to enhanced due diligence measures aimed at gaining enough information to reduce the potential ML risk (probability that the funds might be proceeds of crime); and
d) Identify Regular (Existing) clients identified in order to establish the nature of the client's business activities and their reasons for engaging in third party payments.

3.2.3 **Investments made in the name of a third party**

Any form of non-face-to-face transactions or anonymity in transactions, poses significant potential ML risks. As such, due care should be exercised when funds are invested for the benefit of a third party ie. source of funds for the investment comes from a legal entity whilst the investment is opened in an individual's name. The Unit Trust Managers are encouraged to examine these types of transactions as to avoid assisting or facilitating the transferring of funds to an unknown beneficiary.

[1] See sections 4-6 of the POCA for ML offences

3.2.4 **Upon finalization of the transaction, the Unit Trust Manager should again ensure that all the required identification and transaction data are on the file, before approving the archiving of the file**

It is important that management ensure that the required records in terms of the FIA are kept in a safe storage space. Management should thus sign off on each unit trust file before files are archived. Should records be kept by a third party, notice should be given to the FIC as required by the FIA and its regulations.

3.2.4 **Approval and scrutiny of any refunds of (incorrectly) paid deposits by management.**

No refunds should be made to clients before the circumstances relating to the reason for such refund are evaluated as part of a formal process. Related to this is the fact that the firm's banking details should be removed from all correspondence such as letterheads, corporate stationery, etc. to avoid criminals from deliberately depositing money into a firm's trust or business account with the sole aim of requesting a refund directly into another existing bank account. A cheque or transfer from a Unit Trust Manager's account would be a very plausible explanation if provided by an individual when his/her bank enquires as to source of funds.

See **Annexure B** for generic indicators of potential suspicious transactions which should be considered by management in designing, implementing and evaluating the internal controls within the business.

4. IMPORTANCE OF KYC AND RECORD KEEPING IN REPORTING SUSPICIOUS TRANSACTIONS

Clients deliberately engaging the services of any Unit Trust Manager in a Money Laundering scheme, do not necessarily care whether or not the Unit Trust Manager might get fined for failure to report a suspicious transaction, identify a client or keep the appropriate records as required by the FIA. They also do not care whether the firm is likely to be charged for ML offences when accepting proceeds of crime into its possession or for facilitating or assisting a person in a ML scheme. As such, the importance of identifying clients and using the information to identify and report

suspicious transactions cannot be overemphasized.

In terms of the POCA, filing a suspicious transaction is considered the only valid defense when an AI is charged with a ML offence. The FIA also offers the added comfort of protection of the confidentiality of the person or institution who filed the suspicious transaction report, thus there is no risk of losing any legitimate clients as a result of filing a report to the FIC. As such it can only be to the benefit of the firm to rather file the report then to hope that the transaction suspected of involving proceeds of crime, is not detected by the National AML system.

For more comprehensive details on how and when to file suspicious transaction reports, please refer to Guidance Note 1 of 2009 on Suspicious Transaction Reporting.

5. COMMENTS

This Guidance Note shall be reviewed from time to time. If you have any comments or suggestions to help improve this Guidance Note, please send your comments to the FIC by using the particulars provided herein below.

6. HOW TO CONTACT THE FIC

You can contact the FIC at the following telephone and fax numbers:

The Director: 061-2835283 and fax number 061-2835259

The Deputy Director: Financial Investigations and Analysis: 061-2835026 and fax number 061-2835259;

The Deputy Director: Legal and Compliance: 061-2835215 and fax number 061-2835259

ISSUED AND PUBLISHED BY THE FINANCIAL INTELLIGENCE CENTRE

AUGUST 2012

All Correspondence and enquiries must be directed to:

The Director

Financial Intelligence Centre

P.O. Box 2882

No.71 Robert Mugabe Avenue

Windhoek

Republic of Namibia

Tel: 061-2835100

Fax: 061-2835259/5369

Email: leonie.dunn@fic.na

Annexure A

FACTORS TO CONSIDER IN ASSESSING THE ML/TF RISK A CLIENT POSES

Client Risk

1. Determining the potential money laundering or terrorist financing risks posed by a client, or category of clients, is critical to the development and implementation of an overall risk-based framework and an effective AML program. Based on its own criteria, Accountable Institutions should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that identified risk. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of clients whose activities may indicate a higher risk include:

a) Non-resident clients depending on the type of service they require from the Unit Trust Manager and the origin or source of funds to be used in the transaction, due to the fact that it is very difficult to perform enhanced due diligence on non-resident clients, especially with regard to verifying details pertaining occupation or source of funds to be used in the transaction;

b) Particularly Exposed Persons[2] (PEPs). If a Unit Trust Manager is advising a client who is a PEP, or where a PEP is the beneficial owner of the client, with respect to the activities specified on page 5 of this guidance note, then the Unit Trust Manager will need to carry out appropriate enhanced CDD. Relevant factors that will influence the extent and nature of the CDD include the particular circumstances of a PEP, the PEP's home country (in the case of a foreign PEP), the type of work the PEP is instructing the Unit Trust Manager to perform or carry out, and the scrutiny to which the PEP is under in the PEP's home country (in the case of a foreign PEP);

[2] Individuals who are or have been entrusted with prominent public functions by a country, domestically or internationally, for example Heads of State of Government, senior politicians, senior government officials, judicial or military officials, senior executives of state owned corporations, important political party officials etc.

c) Clients that are cash (and cash equivalent) intensive businesses including:
    i) Money services businesses (*e.g.* remittance houses, currency exchange houses, casas de cambio, bureaux de change, money transfer agents and other businesses offering money transfer facilities);
    ii) Casinos, betting and other gambling related businesses;
    iii) Businesses that while not normally cash intensive generate substantial amounts of cash;
    iv) Charities and other "not for profit" organisations (NPOs) that are not subject to monitoring or supervision (especially those operating on a "cross-border" basis);

d) Clients using financial intermediaries, financial institutions or legal professionals that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities or Self-Regulatory Organizations;

e) Existing clients whose behavior or profile conforms to the following:
    i) Clients having convictions for proceeds generating crimes who instruct the legal professional (who has actual knowledge of such convictions) to undertake specified activities on their behalf.
    ii) Clients who have no address, or multiple addresses with multiple contact numbers without legitimate reasons.
    iii) Clients who change their settlement or execution instructions without appropriate explanation.
    iv) The use of legal persons and arrangements without any apparent legal or legitimate tax, business, economic or other reason.

Annexure B

SPECIFIC EXAMPLES OF INDICATORS OF SUSPICIOUS TRANSACTIONS

The following are examples of common indicators that may point to a suspicious transaction.

General

- Client admits or makes statements about involvement in criminal activities;
- Client does not want correspondence sent to home address;
- Client appears to have accounts with several financial institutions in one area for no apparent reason;
- Client conducts transactions at different physical locations in an apparent attempt to avoid detection;
- Client repeatedly uses an address but frequently changes the names involved;
- Client is accompanied and watched;
- Client shows uncommon curiosity about internal systems, controls and policies;
- Client has only vague knowledge of the amount of a deposit or indicates that the deposit originates from a third party;
- Client presents confusing details about the transaction or knows few details about its purpose;
- Client over justifies or explains the transaction;
- Client is secretive and reluctant to meet in person;
- Client is nervous, not in keeping with the transaction;
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities;
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after opening account;
- Normal attempts to verify the background of a new or prospective client are difficult;
- Client appears to be acting on behalf of a third party, but does not tell you;

- Client is involved in activity out-of-keeping for that individual or business;
- Client insists that a transaction be done quickly;
- Inconsistencies appear in the client's presentation of the transaction;
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client;
- Client appears to have recently established a series of new relationships with different financial entities;
- Client attempts to develop close rapport with staff;
- Client uses aliases and a variety of similar but different addresses;
- Client spells his or her name differently from one transaction to another;
- Client offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious;
- You are aware or you become aware, from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity;
- A new or prospective client is known to you as having a questionable legal reputation or criminal background;
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

Knowledge of Record Keeping Requirements

- Client attempts to convince an employee not to complete any documentation required for the transaction;
- Client makes inquiries that would indicate a desire to avoid reporting;
- Client has unusual knowledge of the law in relation to suspicious transaction reporting;
- Client seems very conversant with money laundering or terrorist activity financing issues;
- Client is quick to volunteer that funds are "clean" or "not being laundered";
- Client appears to be structuring amounts to avoid record keeping, client

identification or reporting thresholds; and

- Client appears to be collaborating with others to avoid record keeping, client identification or reporting thresholds.

Identity Documents

- Client provides doubtful or vague information;
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate or more than one customer tries to use the same identification;
- Client refuses to produce personal identification documents;
- Client only submits copies of personal identification documents;
- Client wants to establish identity using something other than his or her personal identification documents;
- Client's supporting documentation lacks important details such as a phone number;
- Client inordinately delays presenting corporate documents;
- All identification presented is foreign or cannot be checked for some reason;
- Client presents different identification documents at different times;
- Client alters or refuses to proceed with the transaction after being asked for identity documents;
- Client presents different identification documents each time a transaction is conducted.

Cash Transactions

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past;
- Client conducts a transaction for an amount that is unusual compared to amounts of past transactions;
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.);
- Stated occupation of the client is not in keeping with the level or type of activity

(for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area);

- Large transactions using a variety of denominations;
- Client uses unit trust account as a business cheque account with frequent requests to make payments to third parties;
- Direct cash deposits into the unit trust account, especially if this is not in line with established profile. Eg; Salaried individual or Business funds;
- Business funds invested on a unit trust account in the name of an individual.

Economic Purpose

- Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities;
- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the client;
- Transaction is unnecessarily complex for its stated purpose;
- Activity is inconsistent with what would be expected from declared business;
- A business client refuses to provide information to qualify for a business discount;
- No business explanation for size of transactions or cash volumes;
- Transactions of financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter);
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.