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 3 OF 2015

GUIDANCE NOTE ON CUSTOMER IDENTIFICATION AND KEEPING OF RECORDS

First issued: July 2009

Revised and issued in: December 2015

TABLE OF CONTENTS

A. DEFINITIONS

"Accountable (AI) or Reporting institution (RI)" 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);

"Basel Committee" means the committee established by international banking regulators who provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide. It seeks to do so by exchanging information on national supervisory issues, approaches and techniques, with a view to promoting common understanding. At times, the Committee uses this common understanding to develop guidelines and supervisory standards in areas where they are considered desirable. In this regard, the Committee is best known for its international standards on capital adequacy; the Core Principles for Effective Banking Supervision; and the Concordat on cross-border banking supervision;

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

"CDD" means Customer Due Diligence;

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

"Customer due diligence" 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;

“Establish identity” means a two tier process consisting of ascertainment or collecting of certain identification information, and verification of some of the information against reliable documentation or information;

"FATF" means the Financial Action Task Force;

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

“FIC” means the Financial Intelligence Centre as created by section 7 of the FIA;

“ML” means Money Laundering

“PALERMO CONVENTION" refers to the United Nations Convention against Transnational Organized Crime (2000); Namibia ratified this Convention on 16 August 2002 and the Convention entered into force on 29 September 2003;

“PEPs” means Political Exposed Persons;

“PF” means proliferation financing

“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 activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act;

“STR” refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the Act;

“TF” means Terrorist Financing

“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 [as stated in section (2)1 of the Act]. This Guidance Note is issued and published by the FIC in terms of section 9(h) of the Act.

1.1 General

On the one hand Sections 21 and 22 of the Act require accountable and reporting institutions to identify their clients, and on the other hand, sections 26 to 29 of the Act require accountable and reporting institutions to keep records of all documents obtained during the identification process.

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 customer identification and record keeping. 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 Financial Intelligence FIC (FIC), under the Act is to help various stakeholders (including accountable or reporting institutions) combat 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. Amongst others, the major measures or obligations an accountable or reporting institution should put in place to mitigate the aforesaid risks include:

- Client identification (section 21 and 22);
- Record keeping (Section 26 to 29)

This document provides guidance on measures pertaining client identification and record keeping as per the Act. It must however be said that in order for accountable and reporting institutions to effectively mitigate the risk of ML/TF and PF, client identification and record keeping measures need to be complemented by other measures as prescribed by the Act such as developing and implementing AML programs and policies; adopting a risk based approach; on-going and enhanced due diligence of client behaviour; measures to aid detecting and reporting of suspicious transactions and activities; training of staff members on how to mitigate these risks etc. The FIC website contains other Guidance Notes and helpful documents such as the Regulations and Circulars which provides further guidance on measures to combat ML/TF and PF in terms 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 objectives[1].

3.2.2 Understanding the financing of terrorism

[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)

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. 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 value-transfer 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

(j) (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 obligations[4].

[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

3.3.2 Background on Proliferation financing

Proliferation financing facilitates the movement and development of proliferation-sensitive 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. 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 (www.fic.na) or directly on https://www.un.org/sc/suborg/ .

4. IDENTIFICATION WHEN BUSINESS RELATIONSHIPS ARE ESTABLISHED AND WHEN SINGLE TRANSACTIONS ARE CONCLUDED

4.1 The process of identifying clients

Client identification is done on a risk-based approach. This means, the extent to which identification information is obtained, ascertained and verified is dependent on the risk presented by the client. The duty to identify a client entails, firstly, the collection (called “ascertainment” in the regulations) of identification information of clients as set out in the Act and prescribed in the regulations. Secondly, it entails the verification of such identification details. Regulations 6 to 11 provide guidance on the minimum identification procedures that should be followed for the various types of clients. Furthermore, where an accountable or reporting institution seeks to ascertain the client and risk profile, such accountable or reporting institution must take reasonable steps to obtain additional identification information as contained in Regulation 12. This applies to clients where there is a need to ascertain the level of risk they could expose the accountable or reporting institution to.

If applied properly, the above mentioned procedures should eventually put any accountable or reporting institution in a position of knowing its client. This obligation places emphasis on the fact that it is the duty of the accountable or reporting institution

to know its clients. Coupled with this, section 21 (2) of the Act prohibits accountable or reporting institutions to open or maintain any anonymous accounts or accounts that are fictitious, false or incorrect.

It is important to note that identification of clients is required when a business relationship is established or when a single transaction that exceeds the following thresholds is entered into:

- N$ 5,000.00 for all AIs and RIs, except for casinos and gambling houses; and
- N$ 25,000.00 for all casinos and other gaming institutions.

With the above thresholds as Guidance, accountable and reporting institutions will have to follow the identification procedures stated in the regulations. For example:

- Regulation 6: Ascertainment of information concerning natural persons;
- Regulation 7: Ascertainment of information concerning companies and close corporations;
- Regulation 8: Ascertainment of information concerning associations and other entities;
- Regulation 9: Ascertainment of information concerning partnerships;
- Regulation 10: Ascertainment of information concerning trusts; and
- Regulation 11: Additional requirements when person acts on authority of another

4.1.1 Additional identification information in terms of Regulation 12:

It is essential to keep in mind that identification procedures as per Regulations 6 to 11 is for obtaining the minimum identification information while Regulation 12 provides an avenue for obtaining additional information, the extend of which is dependent on the risk the client may pose to the accountable or reporting institution. This additional identification information as required by Regulation 12 can be obtained either:

- before establishment of business relationship or single transaction or
- during the course of the business relationship or conclusion of single transaction.

Below are some examples demonstrating identification procedures in terms of the regulations:

Example.1 - if a client, identified as normal government salaried employee with no extra income wants to establish a business relationship with an accountable or reporting institution, that person will probably be a low risk client. The Accountable or reporting institution will be allowed to only obtain and verify the minimum information as per regulation 6 before entering into the business relationship. The rest of the information as per reg.12 (1) may be obtained after the business relationship was established or somewhere during the course of the business relationship, especially when the initial client profile changes.

Example. 2 – if a client, who is identified as a wealthy business man with business interests in Angola, Iran and Afghanistan wants to enter into a business relationship with an accountable institution, such a person would be a high risk client and the accountable institution should obtain and verify all information as per regulation 6 and regulation 12(1) or even more than that if need be.

4.2 Identification when transaction is concluded in the course of business relationship

Business relationships that were established before the commencement of the Act may expose the accountable or reporting institution's financial systems to money laundering, terrorism and proliferation financing risks. The Act states that accountable or reporting institutions that established a business relationship with clients before the Act came into force must, within a period determined by the FIC, take such reasonable steps in the prescribed form and manner to, amongst others, establish the identity of the client, by obtaining and verifying identification and any further information (section 22). For the banking industry, the FIC has determined and communicated a period within which accountable or reporting institutions should identify the clients in such business relationships. All other sectors need to adopt a risk based approach in terms of

identifying such clients as provided for in section 23 of the Act (see example in 4.2.1 below).

4.3 Risk clients (s23)

4.3.1 Understanding the type of clients who may present ML, TF or PF risks

There is no one formula the world over, that can be used to accurately identify ML, TF or PF risk clients. However, given the obvious objective of wanting to mitigate such risks, the starting point is normally making a subjective assessment of the probability or chances that a particular client may engage in and therefore expose the systems of an accountable or reporting institution to potential ML, TF or PF abuse. The examples below are indicative of client position or standing and behavior may be regarded as exposing our financial systems to potential ML, TF or PF abuse:

a. **Politically Exposed Persons (PEPS):** given that Politically Exposed Persons are in positions of power and influence and are comparatively highly exposed to situations or temptations to engage in unlawful activities such as accepting or paying bribes, bypassing certain controls due to their positions and thus potential to abuse systems to advance ML, TF or PF activities. Given this understanding, those involved in politics or those exposed to such political influence and power such as the family members, relatives, friends or business associates or partners of a Minister, Governor, Ambassador etc. can thus be regarded as PEPs. However, their individual transacting behaviour and activities may have a bearing on the extent of due diligence they are subjected to by an accountable or reporting institution;

b. **Persons (including business persons) whose source of income is unknown, uncommon in a given area or too complex to understand:** when a client's profile is not easy to understand and comprehend, it is usually a reason to be cautious as an unclear financial profile or background provides room to

hide illicit behaviour under a complex background which cannot be readily understood;

c. **Persons whose transacting behaviour is uncommon (questionable nature or purpose of transacting behaviour):** When the transacting behaviour of a client is not in the norm of what is expected of such a client, this normally would make such a client a risk client. For example, a client identified as a salaried employee is having regular or unusual deposits made onto his/her account. Also, a client who has a grocery retail business keeps paying Motor vehicle dealers or other persons which may not seem in line with the nature of his/her business activities. Another example is that of a business with unconventional transacting behaviour such as no indication of general business expenditure like paying for water and electricity, salaries etc. A client can also become high risk when funds that are deposited into his or her account are immediately remitted or paid over to other parties for unknown reasons;

d. **Persons from or with links to jurisdictions known to be safe havens of ML/TF or PF:** Persons who have links to certain jurisdictions which are regarded as safe havens for ML/TF or/and PF activities present a higher risk than those who may not have links to such jurisdictions. The reasoning is that some jurisdictions may not have adequate or effective AML controls which enhances the possibility of ML/TF or/and PF abuse of their financial systems;

e. **Persons whose known profile does not match their financial or transacting behaviour:** Simply put, if a teacher transacts in amounts beyond the expected earnings of a teacher, he or she presents a higher risk then the other teachers not transacting beyond their expected means, at least until their other sources of income are understood.

4.3.2 Identifying clients with whom business relationship commenced before the FIA

The FIC noted challenges in carrying out re-identification exercises across the board in as far as all pre-FIA clients are concerned. A risk based approach is therefore advocated. Section 23 (1) of the Act states that accountable or reporting institutions must have appropriate risk management and monitoring systems in place to identify clients or beneficial owners whose activities may pose a risk of money laundering, financing of terrorism or proliferation, or all three. Where a client or beneficial owner has been identified through such systems to be a high risk for money laundering, financing of terrorism or/and proliferation activities, the employees of an accountable or reporting institution must, amongst others, obtain approval before proceeding with such a business relationship and take measures as prescribed by the FIC to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client.

In simple terms, if a business relationship was established prior to this Act and client was not accordingly identified, the expectation is that:

- Were the client hardly transacts or transacting behaviour is such that the business is of the reasonable view that client presents minimal or tolerable money laundering, terrorism and proliferation financing risk: The accountable or reporting institution ought to take reasonable steps to identify client to an extend that there is reasonable comfort that client behaviour does not expose the accountable or reporting institution to such risks;
- Were the client's behaviour reflects complex, unusual or transacting behaviour that does not seem to be in line with what is ordinarily expected of such a client, the accountable or reporting institution has to make an assessment on the level of risk exposure presented by the business relationship with such client and take reasonable steps to identify client to an extent that there is reasonable comfort that client behaviour does not expose the accountable or reporting institution to such risks. If this assessment reflects behaviour which is suspicious in terms of money laundering, terrorism and proliferation financing, the accountable or reporting institution ought to report same to the FIC.

4.3.3 On-going and enhanced due diligence (s24 of the Act and Regulation 15)

The expectation to understand and be abreast with client behaviour is provided for in the Act. The Act states that an accountable or reporting institution must exercise on-going due diligence in respect of all its business relationships which must, at a minimum, include:

- maintaining adequate, current and up-to-date information and records relating to the client and beneficial owner;
- monitoring the transactions carried out by the client in order to ensure that such transactions are consistent with the accountable or reporting institution's knowledge of the client, the client's commercial or personal activities and risk profile; and
- ensuring the obligations relating to high risk clients, as prescribed in section 23 for risk clients, and correspondent banking relationships are fulfilled.

4.4 Identification when concluding Single Transactions

Where no business relationship has been established, accountable or reporting institutions are only required to identify the client if there is a single transaction exceeding the following client identification thresholds:

- N$ 5,000.00 for all AIs and RIs, except for casinos and gambling houses; and
- N$ 25,000.00 for all casinos and other gaming institutions.

If the amount involved in the single transaction is equal to or below the above amounts, then the obligation to identify the client is not applicable. However, there is a risk of smurfing. Smurfing refers to a client submitting transactions for processing, by accountable or reporting institutions, whose amounts are just below the identification threshold. In this regard section 21(1) of the Act states that part or multiple cash transactions in the domestic or foreign currency which, in aggregate, exceed the amount determined by the Centre must be treated as a single transaction if they are

undertaken by or on behalf of any person during any day or such period as the Centre may specify.

The threshold amounts as stipulated above do not apply where accountable or reporting institutions have established a business relationship with a client. This means, where the accountable or reporting institution has established a business relationship with a client, such as an account at a bank, it does not matter whether the amount involved is less than, equal to, or exceeds set thresholds, the duty to identify the client applies and is required at the time of establishing the relationship.

4.5 Identification information

If you have to identify the individual using a document, the latter must be the type of document you used to confirm the individual's identity, and must include its reference number and its place of issue. Accountable and reporting institutions should not keep or establish anonymous accounts or accounts in fictitious names.

4.6 Non face-to-face customers in the banking industry

Banks are increasingly asked to open accounts on behalf of customers who do not present themselves face-to-face to conduct business. This has been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non face-to-face customers as for those with whom they conduct business face-to-face.

A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the internet or similar technology. Electronic banking currently incorporates a wide range of products and services delivered over telecommunication networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification. As a basic policy, the FIC expects that banks should proactively assess various risks posed

by emerging technologies and design customer identification procedures with due regard to such risks. Even though the same documentation can be provided by face-to-face and non-face-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers. With telephone and electronic banking, the verification problem is made even more difficult when there is hardly any face-to-face interaction between the client and AI or RI.

Banks must ensure that there are specific and adequate measures to mitigate the risk posed by non-face-to-face customers.

Despite regulation 4 or any other provision contained in these regulations requiring compliance with the establishment of the identity of a client, beneficiary or beneficial owner, an accountable or reporting institution must, where such regulation or other provisions regarding such establishment cannot be complied with due to impossibility or reasonable impracticability -

a. as far as is reasonably possible, take such steps to ascertain or verify such identity;
b. without delay give written notice to the Centre of such impracticability or impossibility indicating any alternative measures used to identify or verify such identity;
c. not open the account, not commence the business relationship or perform the transaction or terminate the business relationship, except if otherwise directed by the Centre; and
d. consider filing a suspicious transaction or activity report, except if otherwise directed by the Centre.

5. DEPLOYMENT OF CUSTOMER DUE DILIGENCE (CDD)

Accountable or reporting institutions should deploy customer due diligence measures at all relevant times, particularly when:

- establishing business relationships;

- carrying out single transactions above the single transaction client identification thresholds stated herein;
- there is a suspicion of money laundering, terrorism and/or proliferation financing activities; or
- the accountable or reporting institution has doubts about the veracity or adequacy of customer identification information or documentation provided by prospective clients or clients with whom a business relationship was established before the Act was commenced.

6. ADOPTION AND DEVELOPMENT OF INTERNATIONAL STANDARDS ON CUSTOMER ACCEPTANCE POLICIES BY BANKS

Banks should develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to a bank. In preparing such policies, the following factors should be considered:

- customers' background;
- country of origin;
- public or high profile position;
- linked accounts, business activities or other risk indicators.

Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, such policies may prescribe only the most basic due diligence for opening an account for a working individual with a small account balance, but enhanced due diligence measures for clients with unknown, complex, unconventional financial backgrounds or unclear sources of income. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access to the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with

higher risk customers, such as politically exposed persons should be taken exclusively at senior management level.

6.1 Substitute forms of establishing identity and keeping records for new customers under the general exemptions

The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. As per regulation 5(6), all accountable and reporting institutions including banks are allowed to rely on the procedures undertaken by other banks or introducers, when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. It is therefore important to maintain the necessary level of diligence given that regulation (5)10 cautions that the ultimate responsibility for client identification and verification remains with the accountable or reporting institution that chooses to rely on the client identification and verification of another accountable or reporting institution. This means that relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own CDD procedures or that is unwilling to share copies of due diligence documentation.

The Basel Committee recommends that banks use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:

- it must comply with the minimum customer due diligence practices identified in the regulations and in this guidance note;

- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted in establishing and maintaining a business relationship with that client;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- the bank must reach an agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage and all relevant identification data and other documentation pertaining to the customer's identity will be immediately submitted by the introducer to the bank who will then carefully review the documentation provided;
- Such information must be available for review by the supervisor body and or the FIC;
- In addition, banks should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out herein above.

6.2 Customer identification and due diligence on non-account holders in the financial institutions (especially the banking sector)

It is common in the financial sector that a services provider (e.g. a bank) will have customers who are account holders. The expectation is that such customers are identified in terms of the FIA before customers are provided with financial services by that accountable or reporting institution. It is also common that accountable and reporting institutions also provide financial services to non-account holding clients. A practical example: a non-account holder may visit a bank and use the bank’s services to remit funds to a recipient abroad (or locally). With account holders, their accounts are often used as a platform through which the remittance is facilitated. However, when a non-account holder makes use of these services to remit funds, the transactions are facilitated through the use of suspense, miscellaneous or similar account. In some cases, the non-account holder remits funds using such financial services at an accountable or reporting institution, without being subjected to identification and

customer due diligence measures as required by the FIA on the basis that such a person is not an account holder.

6.2.1 Rationale for subjecting non-account holders to customer due diligence measures of the Act

The challenge with not identifying such non-account holding clients lies in the unmitigated risk exposure to ML/TF/PF that unknown clients may present. The risk of an accountable or reporting institution's financial services being abused for ML/TF/PF purposes by non-account holders is relatively higher than the risk presented by account holding clients. This is because the non-account holder's profile and background is unknown and without this knowledge, customer due diligence and transactional monitoring measures as required by sections 23, 24, 33 & 39(1) of the Act cannot be fulfilled by accountable or/and reporting institutions. This also means, failure to identify non-account holding clients (especially those transacting regularly in one way or the other) present the accountable and reporting institutions with unmitigated risks and possible administrative and other sanctions owing to non-compliance with the Act.

The Act defines a "business relationship" as an arrangement between a client and an accountable or reporting institution for the purpose of concluding transactions on a regular basis. Regardless of whether an account is created, when carrying out services on behalf of a person (client), the accountable or reporting institution involves itself in a business relationship with such a client. Furthermore, Section 22 of the Act says that an accountable or reporting institution may not establish a business relationship or conclude a single transaction with a prospective client, unless the accountable or reporting institution has taken such reasonable steps in the prescribed form and manner to establish, amongst others, the identity of the client. It is worth highlighting that the level of risk exposure presented by a client's transacting behavior should guide the accountable institution's level or extend of the necessary customer due diligence measures such client should be subjected to (s23 & 24 of the Act). The regulations explain this expectation by stating that an accountable or reporting institution must

monitor transactions carried out by its client throughout the existence of the business relationship to ensure that such transactions are consistent with the knowledge of the accountable or reporting institution of the client, the business of the client and risk profile and where necessary, the source of funds of the client.

6.3 Correspondent banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"), usually situated in another country or jurisdiction. Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. Correspondent accounts that merit particular care, involve the provision of services in jurisdictions where the respondent banks have no physical presence. If banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to a range of risks, and may find themselves holding and or transmitting money linked to corruption, fraud, money laundering, terrorist or proliferation financing or other illegal activity. Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include:

- information about the respondent bank's management, major business activities, where they are located and its money laundering, terrorism and proliferation financing prevention and detection efforts. The objective is to gain reasonable assurance that the respondent bank has reasonable measures to mitigate ML/TF/PF risks effectively;
- the purpose of the account;
- the identity of any third party entities that will use the correspondent banking services; and
- the condition of bank regulation and supervision in the respondent's country.

Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks

should have effective customer acceptance and CDD policies. In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor CDD standards or have been identified as being uncooperative in the fight against ML, TF and PF.

Banks should establish that their respondent banks have due diligence standards as set out in this paper and employ enhanced due diligence procedures with respect to transactions carried out through the correspondent accounts. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf. Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out herein. Importantly, correspondent banking relationships should be approved by senior management after consideration of all the above mentioned factors before commencing with any business activities with the respondent bank.

This paragraph must be read in conjunction with Section 25 of the Act.

7. IDENTIFICATION AND DUE DILIGENCE MEASURES ON RISK CLIENTS (EMPHASIS ON POLITICALLY EXPOSED PERSONS)

7.1 Risk Clients: Politically exposed persons

7.1.1 Understanding politically exposed persons and ML/TF risks

A politically exposed person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function[5]. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing (TF) or funding of proliferation (PF).

It is important to note that family members and close associates of PEPs also fall under the category of PEPs, in AML/CFT/CFP context. Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Close associates are individuals who are closely connected to a PEP either socially or professionally.

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank's to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals, whether domestic or foreign, who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

There is always a possibility, especially with PEPs associated with sectors where corruption is widespread, that such persons may abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. Accepting and managing funds from corrupt PEPs may amount to facilitating ML/TF/PF or being in possession of proceeds from illicit activities. This may expose the bank to:

- a severely damaged image and reputation;
- undermine public confidence in the ethical standards of an entire financial institution; (since such cases usually receive extensive media attention and

[5] FATF Guidance: Politically Exposed Persons. Recommendations 12 and 22. June 2013. http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

strong political reaction even if the illegal origin of the assets is often difficult to prove);

- In addition, the bank may be subjected to punitive measures from the FIC or/and the courts.

Under certain circumstances, the bank and or its officers and employees themselves can be exposed to charges of money laundering or terrorist- or proliferation financing if they know or should have known that the funds stemmed from corruption or other serious crimes. Banks should gather sufficient information from a new customer and check publicly available information in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level. Again, PEPs can be persons from the domestic community or prominent figures from foreign countries.

7.2 Mitigating risks presented by politically exposed persons

To address the ML/TF and/or PF risks presented by PEPs, the Act requires accountable and reporting institutions implement measures to prevent the misuse of the financial system and non-financial businesses and professions by PEPs, and to detect such potential abuse if and when it occurs.

With due consideration to factors such as the client profile, behaviour and background of a PEP, Accountable or reporting institutions make an assessment on the level of risk to assign to a PEP. As a general rule, foreign PEPs are always considered a higher risk than domestic PEPs and this therefore warrants taking enhanced due diligence measures where Foreign PEPs are concerned. For higher risk PEP relationships, it is a misconception to assume that detailed knowledge of a PEP may allow the relationship to be treated as - other than high risk. For example, a foreign head of government remains a high risk PEP, no matter what the staff of the accountable or reporting

institution (i.e. account or client managers, senior executive staff) may know about this particular person, or the product provided.

All PEPs and their family members and close associates should be subjected to the same AML/CFT/CFP controls. The level of such measures may be determined by the level of risk exposure. The following enhanced due diligence measures apply are recommended:

- **senior management approval:** financial institutions and Designated non-financial business and professions DNFBPs should be required to obtain senior management approval for establishing (or continuing, for existing customers) business relationships with foreign PEPs;
- **reasonable measures to establish the source of wealth and the source of funds:** The source of wealth refers to the origin of the PEP's entire body of wealth (i.e., total assets). Although banks may not have specific information about assets not deposited or processed by them, it may be possible to gather general information from commercial databases or other open sources. This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the PEP acquired such wealth; and
- **enhanced ongoing monitoring of the business relationship:** The source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between the PEP and the accountable institution (e.g., the amounts being invested, deposited, or wired as part of the business relationship).

8. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

CDD measures do not imply that accountable and reporting institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. Regulation 5(6) states that in terms of section 67(1)(h) of the Act, the steps to be taken for establishing the identity of a client as contemplated in

sections 21 and 22 of the Act, may be completed by an employee of an accountable or reporting institution or by a third party accountable or reporting institution.

An accountable and reporting institution is therefore entitled to rely on the identification steps that it (or a third party accountable or reporting institution) has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an accountable and reporting institution to have such doubts could be where there is a suspicion of money laundering, terrorism and proliferation financing activities in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile. Accountable and reporting institutions should also update information that is more likely subject to change e.g. a client may use a maiden name before marriage and thereafter begin to use the husband's surname.

Regulation (5)10 importantly cautions that despite any allowances that may have been granted in respect of this section (10) or in the general process of establishing the identity of a client, the ultimate responsibility for client identification and verification remains with the accountable or reporting institution that chooses to rely on the client identification and verification of another accountable or reporting institution or a third party accountable or reporting institution.

9. FORMULATION AND DEVELOPMENT OF INTERNAL RULES CONCERNING ESTABLISHMENT OF IDENTITY

Accountable and reporting institutions should formulate and develop its own rules and procedures of establishing the identity of clients. This should set out the necessary processes to be followed and the steps to be taken throughout the entire identification process.

10. VERIFICATION OF IDENTIFICATION INFORMATION

Regulations 13 and 14 deal with the verification of ascertained or obtained information.

Accountable and reporting institutions should verify the particulars of their clients as listed in:

- Regulation 6;
- Regulation 7
- Regulation 8
- Regulation 9;
- Regulation 10;
- Regulation 11;
- Regulation 12 – additional CDD information that may be obtained either before or during the course of the business relationship or conclusion of the single transaction;

Nothing prevents and accountable or reporting institution to obtain more information than is prescribed by the Act and Regulations and to verify as much as possible, or even all the information so obtained, depending on the risk that the client poses or may pose to the institution or in situations where there are indications of a suspicious transaction or activity. Verification can be done by relying on any reliable document, data or information that reasonably serves to verify the information obtained from the client or prospective client.

11. RECORD KEEPING

11.1 Circumstances prompting record keeping

Record keeping is required when an accountable or reporting institution has:

- established a business relationship with a client;
- concluded a single transaction with a client exceeding the following thresholds:
  - ✓ N$ 5,000.00 for all AIs and RIs, except for casinos and gambling houses; and
  - ✓ N$ 25,000.00 for all casinos and other gaming institutions.

- submitted a cash transaction report exceeding a prescribed amount;
- submitted an electronic transfer of money to or from Namibia which exceeds an amount specified by the FIC;
- submitted a suspicious transaction or activity report;

11.2 What Records must be kept

- the identity and address of the beneficiary or the person on whose behalf the transaction is concluded, where applicable;
- the identity and address of the person in whose name the transaction is conducted,
- the identity of the accounts affected by the transaction, if any;
- the type of transaction involved, such as deposit, withdrawal, exchange of currency, cheque cashing, purchase of cashier cheques, money orders or other payment or transfer by, through or to that accountable or reporting institution;
- the identity of the accountable or reporting institution where the transaction occurred;
- the date, time and amount of the transaction;
- all money laundering, financing of terrorist or proliferation activities risk assessments performed in terms of section 39(1) of the Act;
- any other information which the FIC may specify in writing.

11.3 Who must keep records?

Accountable and reporting institutions and, where applicable, supervisory bodies and other persons who are obliged to keep records. A third party may keep records on behalf of an accountable or reporting institution. Furthermore, the records of two or more accountable or reporting institutions that are supervised by the same supervisory body can be centralised.

In terms of section 29 of the Act, if an accountable or reporting institution appoints a third party to perform record keeping duties imposed on it by section 26 of the Act, the accountable or reporting institution must within 30 days provide the FIC with the identification and contact particulars of the third party as per section 19 of the Act.

11.4 Form of keeping records (Section 26; Regulation 17 to 19)

Section 26 and Regulations 17 – 19 spells out which records, at a minimum, must be kept. It is important to note that neither the Act nor the Regulations limits the records that may keep and an AI or RI may go beyond what the law prescribes, depending on the risk ML/TF/PF risk exposure the institution faces or may face.

The records must be kept:

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

Furthermore, records can be kept in hard copy or electronic format as long as a paper copy can be readily produced. Accountable and reporting institutions should maintain effective record-keeping systems to enable the FIC to have access to such records in a timely fashion. An accountable or reporting institution's record keeping system can store the information required for any one record separately, as long as there is an ability to readily retrieve and put the information together for the record whenever necessary. If an accountable or reporting institution keeps records electronically, including records that require a signature on them, such as a signature card or an account operating agreement, an electronic image of the signature of the individual who signed the record has to be retained. This would not include a personal identification number (PIN).

11.5 Period for which records must be kept

Records that relate to the establishment of a business relationship must be kept as long as the business relationship exists and for at least five years from the date on which the business relationship is terminated. Records that relate to single transactions must be kept for five years from the date on which the transaction was concluded. Records that relate to copies of reports submitted to the FIC must be kept for a period of not less than five years from date of filing such report.

However, records must be kept for longer than the 5 year period if the AI or RI is requested to do so by the FIC, the Office of the Prosecutor-General or by any law enforcement agency.

12. PENALTIES FOR NON COMPLIANCE

This Guidance Note uses plain language to explain the obligations under the Act, as well as the related Regulations. It is intended to explain, but not replace, the language of the Act and Regulations.

An accountable or reporting institution which contravenes or fails to comply with client identification and record keeping measures as prescribed by the Act 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 to imprisonment for a period not exceeding 30 years, or to both such fine and such imprisonment.

Any non-compliance with the directions and guidance contained in this Guidance Note is an offence in terms of section 63 of the FIA, and may also attract administrative sanctions and penalties.

13. 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.

14. 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: helpdesk@fic.na