

BANK OF NAMIBIA

FINANCIAL INTELLIGENCE CENTRE

REPUBLIC OF NAMIBIA

P.O.BOX 2882, Windhoek

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

Web address: www.bon.com.na

E-mail address: leonie.dunn@bon.com.na

BANK OF NAMIBIA
Financial Intelligence Centre

GUIDANCE NOTE NO.2 OF 2009 ON:
CUSTOMER IDENTIFICATION AND KEEPING OF
RECORDS

MARCH 2009

TABLE OF CONTENTS

1. **Introduction**

- 1.1 General
- 1.2 Commencement
- 1.3 Definitions
- 1.4 Application

2. **The Financial Intelligence Centre (FIC)**

- 2.1 Functions of the FIC

3. **Money laundering activities**

- 3.1 Criminalization of Money Laundering
- 3.2 Process of Money Laundering

4. **Identification when business relationship is started or a single transaction is concluded**

- 4.1 The duty to identify clients
- 4.2 Business relationships that were established before commencement of the Act
- 4.3 Single Transactions
- 4.4 Identification information
- 4.5 Non face-to-face customers in the banking industry

5. **Deployment of Customer Due Diligence**

6. **Adoption and development of international standards on customer acceptance policies by banks**

- 6.1 Substitute forms of establishing identity and keeping records for new customers under the general exemptions
- 6.2 Politically exposed persons

6.3 Correspondent banking

7. **Reliance on identification and verification already performed**

8. **Formulation and development of internal rules concerning establishment of identity**

9. **Verification of identification information**

10. **Record Keeping**

10.1 Circumstances prompting record keeping

10.2 What Records must be kept

10.3 Who must keep records

10.4 Form of keeping Records

10.5 Period for which Records must be kept

11. **Penalties for non-compliance**

12. **Comments**

13. **How to contact the FIC**

1. INTRODUCTION

1.1 General

The Financial Intelligence Act, 2007 (Act No.3 of 2007) (Act) requires accountable Institutions to identify their clients. This Guidance Note has been issued to help accountable Institutions to develop and put systems in place that will give effect to this objective. For the purposes of this Guidance Note, where emphasis is made to a specific category of accountable institutions, e.g. a bank , that reference only applies to that category.

The principal objective of the Financial Intelligence Centre (FIC) under the Act is to combat money laundering activities (see section 5(1) of the Act. This includes facilitating investigations and prosecutions of money laundering. To these ends, the Act requires certain measures to be taken, including, among other things, the following: submission of certain specified reports, record keeping, client identification and compliance programs for accountable Institutions. If you are an accountable institution, this guidance note has been prepared to help you take such measures.

This Guidance Note uses plain language to explain the obligations under the Act, as well as the related Regulations. It is provided as general information only. It is not legal advice and is intended to explain, but not replace, the language of the Act and Regulations. The Act imposes obligations on accountable institutions to identify their clients and to keep certain records .In order to attain this objective, the FIC may issue guidance notes to accountable institutions to ensure compliance with the provisions of the Act. This Guidance Note is issued and published by the FIC in terms of sections 5(2)(e) and 5(3)(e) of the Act.

1.2 Commencement

This guidance note shall come into effect on

1.3 Definitions

“Accountable Institution” means an Institution listed in schedule 1 of the FIA;

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

“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.

“CDD” means Customer Due Diligence;

“Client and Customer” have their customary meaning and are used interchangeably;

"FATF" means the Financial Action Task Force;

“FIC” means the Financial Intelligence Centre ;

“PALERMO CONVENTION” refers to the United Nations Convention against Transnational Organized Crime (2000);

“PEPs” Political Exposed Persons

“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..... of 2009 promulgated in Government Gazette No...dated2009;

“**STR**” refers to a suspicious transaction report submitted to the FIC in terms of sections 21 and 23(1) of the Act.

1.4 Application of this Guidance Note

The FIC has prepared this Guidance Note to assist accountable institutions in meeting their CDD obligations under the Act. It provides general guidance on identifying clients and deploying a due diligent approach in dealing with customers. Furthermore, it also provides general guidance on record keeping obligations.

2. THE FINANCIAL INTELLIGENCE CENTRE

2.1 FUNCTIONS OF THE FIC

The FIC is Namibia’s specialized institution created to collect, analyze and disclose financial information and intelligence on suspected money laundering, and to enforce compliance with the provisions of the Act. Created in 2006, the FIC is situated in the Bank of Namibia and is an integral part of Namibia’s efforts to prevent and combat money laundering.

The Centre was created to detect and deter money laundering by providing critical information to support the investigation or prosecution of money laundering offences.

More specifically, the FIC’s function is to:

- receive reports on suspicious transactions (sections 21 and 23(1) of the Act);

- receive reports on cash transactions in excess of prescribed amounts (section 20 of the Act);
- receive reports on electronic transfers of money in excess of prescribed amounts to or from Namibia (section 22 of the Act);
- receive reports on the conveyances of cash in excess of prescribed amounts to or from Namibia (section 24 of the Act);
- receive other information as appropriate (section 5 of the Act);
- analyze and assess the information it receives (section 5 of the Act);
- provide law enforcement agencies with high quality financial intelligence that would be relevant to the investigation or prosecution of money laundering offences and, if such intelligence is relevant to the national security of Namibia, to disclose such intelligence to the Namibia Central Intelligence Service (sections 5 and 34 of the Act);
- ensure compliance by Accountable Institutions and Supervisory Bodies with their obligations under the Act and regulations (section 5 of the Act);

3. MONEY LAUNDERING

3.1 Criminalisation of Money Laundering

The relevant legal statute that criminalizes money laundering is the Prevention of Organized Crime Act, 2004 (Act No. 29 of 2004) (POCA). Under the provisions of POCA, the scope of criminalization of Money laundering are wide and it entails the following:

- the disguising of unlawful origin of property;
- assisting another person to benefit from proceeds of unlawful activities;
and
- acquisition, possession or use of proceeds of unlawful activities.

Money laundering has been criminalized in sections 4, 5 and 6 of POCA. As such, a money laundering offence may be described as the performing of any act that may result in concealing the nature of the proceeds of crime or enabling a person to avoid prosecution or in the diminishing of the proceeds of crime. A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Namibia.

On the other hand, the Financial Intelligence Act defines “money laundering” or “money laundering activity” as follows:

- (a) 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;where -
 - (aa) as may be inferred from objective factual circumstances, the person knows or has reason to believe, that the property is proceeds from any unlawful activity; or
 - (bb) in respect of the conduct of a person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property is proceeds from any unlawful activity; and
- (b) any activity which constitutes an offence as defined in section 4, 5 or 6 of the POCA.

Apart from criminalizing the activities constituting money laundering, the Act also contains a number of control measures aimed at facilitating the detection and investigation of money laundering. These control measures, as contained in the Act, are based on three basic principles of money laundering detection and investigation, namely:

- intermediaries in the financial system must know with whom they are doing business;
- the paper trail of transactions through the financial system must be preserved; possible money laundering transactions must be brought to the attention of the FIC.

The control measures introduced by the Act include requirements for institutions to establish the identities of their customers, to keep certain records, to report certain information, and to implement measures that will assist them in complying with the Act. The Act has provided the FIC with the necessary powers to collect, analyze and interpret information which may lead or relate to money laundering and if necessary to disseminate such information to law enforcement agencies in Namibia.

3.2 Process of Money Laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. Profit-motivated crimes span a variety of illegal activities from drug trafficking and smuggling to fraud, extortion and corruption. Money laundering facilitates corruption and can destabilize the economies of susceptible countries. It also compromises the integrity of legitimate financial systems and institutions, and gives organized crime the funds it needs to conduct further criminal activities. It is a global phenomenon, and the techniques used are numerous and can be very sophisticated. Technological advances in e-commerce, the global diversification of financial markets and new financial product developments provide further opportunities to launder illegal profit and obscure the money trail leading back to the underlying crime.

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

- Placement: involves placing the proceeds of crime in the financial system;
- Layering: involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds (e.g., the buying and selling of stocks, commodities or property); and
- Integration: involves placing the laundered proceeds back in the economy under a veil of legitimacy.

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

4.1 The duty to identify Clients

The duty to identify a client entails, firstly, the collection 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.

If applied, these two procedures should eventually put any accountable institution in a position of knowing its client. This obligation places emphasis on the fact that, it is the duty of the accountable institution to know its clients. Coupled with this, section 13 (4) of the Act prohibits accountable institutions to open or maintain any anonymous accounts or accounts that are fictitious, false or incorrect.

Identification of clients is required when a business relationship is established or when a single transaction that exceeds N\$5000 (N\$25000 for casinos and other gaming institutions) is entered into. Accountable institutions will have to follow the procedure proposed in regulation 4 to ascertain identification information for natural persons (meaning you must follow this procedure to collect the items listed in regulation 4(1)),

for legal persons such as companies, etc., you must follow the procedure set out in regulation 5, for associations you must follow regulation 6, for partnerships you must follow regulation 7, for trusts you must follow regulation 8, and, if a person is acting on behalf of another person, regulation 9 must be applied.

Having collected this information, accountable institutions will have to verify that information by following the procedure set out in regulation 10. By way of an example, this should work like this: X proposes to enter into a business relationship with an accountable institution; the accountable institution deploys the requirements of regulation 3-9 of the regulations by asking the client to provide it with the identification particulars listed in regulations 3-9; after this, an accountable institution then verifies the identification particulars obtained by requesting the client to provide it with documents set out in regulation 10, e.g., an identification document or a passport, etc. It then compares the information appearing on the documents collected to satisfy itself whether X is the person it is dealing with and whose particulars are reflected on the documents obtained. When collecting identification information as prescribed in the regulations, accountable institutions should insist on documents that are not easy to counterfeit and should insist on demanding identification documents that will put them in a position of knowing the client.

4.2 Business relationships that were established before the commencement of the Act

Accountable institutions that established a business relationship with clients before the Act came into force have a period of three years after the commencement of the Act to identify these clients. With regard to new clients with whom (or which) accountable institutions enter into a business relationship after the commencement of the Act, accountable institutions are required to identify such clients during the stage of establishing the business relationship.

4.3 Single Transactions

Where there is no business relationship, accountable institutions are only required to identify the client if there is an engagement of a single transaction exceeding five thousand Namibian dollars (N\$5000.00). For casinos and other gaming institutions the engagement of a single transaction is twenty five thousand Namibia dollars (N\$25000.00). 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. The threshold amounts of five thousand Namibian dollars (N\$5000.00) for accountable institutions and twenty five thousand Namibia dollars (N\$25000.00) for casinos and other gaming institutions, does not apply in business relationships. This means, where the accountable institution or casino and other gaming 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 five thousand Namibian dollars (N\$5000.00) or twenty five thousand Namibia dollars (N\$25000.00). The duty to identify the client applies and is required at the time of establishing the relationship..

4.4 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 institutions should not keep or establish anonymous accounts or accounts in fictitious names.

4.5 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 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 array of products and services delivered over telecommunications 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.

As we previously mentioned, in accepting business from non-face-to-face customers, banks should apply equally effective customer identification procedures for non-face-to-face customers as for those face-to-face. Banks must ensure that there are specific and adequate measures to mitigate the risk posed by non-face-to-face customers.

5. DEPLOYMENT OF CUSTOMER DUE DILIGENCE (CDD)

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

- establishing business relationships;
- carrying out single transactions above five thousand Namibian dollars (N\$5000.00).
For casinos and other gaming institutions the amount for carrying out single transactions is above twenty five thousand Namibian dollars (N\$25000.00);
- there is a suspicion of money laundering; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken is as follows:

- (a) Identifying the customer, including verifying that customer's identity, using reliable source documents,
- (b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the accountable institution is satisfied that it knows the beneficial owner. Specifically, when the proposed customer is a legal person, a financial institution should take reasonable measures to understand the ownership and control structure of the legal entity.
- (c) Obtaining information on the purpose and intended nature of the business relationship.
- (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, and his/her business and risk profile, including, where necessary, the source of funds.

When performing a CDD process in relation to legal persons, accountable institutions should:

- (a) Verify that any person purporting to act on behalf of the customer is so authorised to do so and must proceed in identifying that person.
- (b) Identify the customer, including the types of measures that would normally be needed to satisfactorily perform this function, namely, requiring proof of incorporation, or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the customer's name, the names

of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.

- (c) Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. The types of measures that would be normally needed to satisfactorily perform this function would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person.

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 customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as the customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by 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. Under the framework set out in the General Exemptions (Para 2.2.-3.2), 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.

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 that 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.

Finally we note that the exemption set forth in Para. 3.2 relieves an accountable institution from the obligation to keep for six years the records pertaining to “the reconstruction of any transaction in excess of such amount as the Bank may specify” (see section 16 (2) of the Act). This relates to the reports required under section 20 of the Act that are exempted for one year from the commencement of the Act. However, the exemption in Para 3.2 does not relieve accountable institutions from the obligation set forth in section 16(1) of the Act that still requires that records of all transactions, including those described above, be kept for five years. Thus, in essence, the exemption set forth in Para. 3.2 was devised to make the length of the period for keeping records uniform under the Act and Regulations, namely, five years, and to remove the confusion that might arise if the sub-category of records described under section 16(2) of the Act were required to be kept for six years.

6.2 Politically exposed persons

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and or legal risks. Such politically exposed persons (“PEPs”) are individuals 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 in countries 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 will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and or its officers and employees themselves can be exposed to charges of money laundering 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.

6.3 Correspondent banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). 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 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 prevention and detection efforts;
- 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 anti-money laundering. 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.

7. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

CDD measures do not imply that accountable institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a

transaction. An accountable institution is entitled to rely on the identification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an accountable institution to have such doubts could be where there is a suspicion of money laundering 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 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.

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

Accountable 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.

9. VERIFICATION OF IDENTIFICATION INFORMATION

For the purposes of verifying identity information, accountable institutions should only verify the particulars listed in regulation 4(1)(a-d), 4(2), 5(1), 6(a), (b), (c) and (e), 7, 8(1)(a), (b), (c), (d) and (g) or 9. These are the particulars concerning the identity of the client. Accountable institutions are not compelled at all times to verify the particulars listed in regulation 4(1)(e)-(i). In situations where there are indications of suspicious transactions and depending on the circumstances of each particular transaction, accountable institutions may discretionally verify the particulars concerning the source of funds involved in that transaction.

10. RECORD KEEPING

10.1 Circumstances Prompting Record Keeping

Record keeping is required when an accountable institution has:

- established a business relationship with a client;
- concluded a transaction with a client exceeding five thousand Namibian dollars (N\$5,000.00) and twenty five thousand Namibian dollars (N\$25,000.00) for 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 report;

10.2 What Records must be kept

- A record of the identity of the client;
- A record of the identity of the person acting on behalf of the client;
- The authority of the client to establish a business relationship or to conclude a transaction;
- The manner in which the identity was established;
- Account records;
- The name of the person who obtained identification and transaction information on behalf of the Accountable Institution;
- Copies of reports sent to the FIC;

10.3 Who must keep records

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

10.4 Form of Keeping Records

The records can be kept in hard copy or electronic format as long as a paper copy can be readily produced. Accountable institution should maintain an effective record-keeping system to enable the FIC to have access to the records in a timely fashion. The record keeping requirements explained in this guidance note are about each record to be kept. Your record keeping system can store the information required for any one record separately, as long as you are able to readily retrieve and put the information together for the record whenever necessary.

If you keep records electronically that require a signature on them, such as a signature card or an account operating agreement, an electronic signature of the individual who signed the record has to be retained. An electronic signature means an electronic image of the signature and does not include a personal identification number (PIN).

10.5 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 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.

11. PENALTIES FOR NON COMPLIANCE

Failure to comply with the duty to identify clients and or the duty to keep records amounts to an offence and is punishable with a fine not exceeding N\$500 000.00, or with imprisonment for a period not exceeding thirty years, or with both such fine and imprisonment .

12. COMMENTS

The guidelines embodied in this Guidance Note shall be reviewed from time to time. Accountable 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.

13. 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: 061-2835037 and fax number 061-2835259

Issued and Published by the Financial Intelligence Centre

March 2009

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

Email: leonie.dunn@bon.com.na