Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID-AFRIKA

Vol. 481 Pretoria, 18 July Julie 2005 No. 27803

AIDS HELPLINE: 0800-0123-22 Prevention is the cure

CONTENTS · INHOUD

No.		Page No.	Gazette No.
	GOVERNMENT NOTICE		
Financial Intelligence Centre			
Government Notice			
715	Financial Intelligence Centre Act (38/2001): Guidance for banks on customer identification and verification and related matters	3	27803

THE GOVERNMENT PRINTING WORKS

PUBLICATIONS DIVISION

NB: The Publications Division of the Government Printing Works will be relocating to its new premises within the:

MASADA BUILDING at 196 PROES STREET, PRETORIA
(i.e. CORNER OF PAUL KRUGER AND PROES STREETS)

with effect from **3 May 2005.**

For enquiries and information:

Mr M Z Montjane
Tel: (012) 334-4653
Cell: 083 640 6121

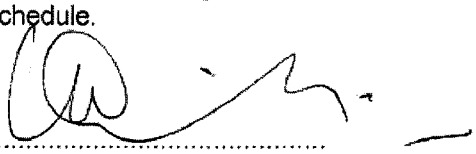
GOVERNMENT NOTICE

FINANCIAL INTELLIGENCE CENTRE

No. 715 **18 July 2005**

GUIDANCE FOR BANKS ON CUSTOMER IDENTIFICATION AND VERIFICATION AND RELATED MATTERS

The Financial Intelligence Centre has, in terms of its statutory function under section 4(c) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), issued the guidance note in the Schedule.



M Michell
DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

Date: **14/07/2005**

FINANCIAL INTELLIGENCE CENTRE
REPUBLIC OF SOUTH AFRICA
Private Bag X115, Pretoria, 0001
Tel: + 27 12 309 9200, Fax +27 12 315 5770
Web address: www.fic.gov.za
E-mail address: fic-feedback@fic.gov.za

Financial Intelligence Centre Guidance Note 3
Guidance for banks on customer identification and verification and related matters

PREFACE

Money laundering has been criminalised in section 4 of the Prevention of Organised Crime Act, 1998. 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 of enabling a person to avoid prosecution or in the diminishing of the proceeds of crime.

Apart from criminalising the activities constituting money laundering, South African law also contains a number of control measures aimed at facilitating the detection and investigation of money laundering. These control measures, as contained in the Financial Intelligence Centre Act, 2001 (the "FIC Act"), are based on three basic principles of money laundering detection and investigation, i.e. that:

- 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 Financial Intelligence Centre and the investigating authorities.

The control measures introduced by the FIC Act include requirements for institutions to establish and verify the identities of their clients, to keep certain records, to report certain information and to implement measures that will assist them in complying with the FIC Act.

The majority of obligations under the FIC Act apply to "accountable institutions". These are institutions that fall within any one of the categories of institutions listed in Schedule 1 to the FIC Act.

The FIC Act also established the Financial Intelligence Centre ("the Centre") as the agency responsible for the collection, analysis and disclosure of information to assist in the detection, prevention and deterrence of money laundering in South Africa. In addition, section 4(c) of the FIC Act empowers the Centre to provide guidance in relation to a number of matters concerning compliance with the obligations of the FIC Act.

Application of this Guidance Note

This Guidance Note applies to the accountable institutions that are referred to in the following items of Schedule 1 to the FIC Act:

- **Item 6** (a person who carries on "the business of a bank" as defined in the Banks Act, 1990).
- **Item 7** (a mutual bank as defined in the Mutual Banks Act, 1993).
- **Item 14** (The Post bank referred to in section 51 of the Postal Services Act, 1998).

- **Item 16** (The Ithala Development Finance Corporation Limited).

This Guidance Note is published by the Centre under section 4(c) of the FIC Act to assist these accountable institutions and the relevant supervisory bodies with the practical application of certain client identification and client verification requirements of the FIC Act. Some of the terminology used in this Guidance Note is explained in the glossary.

Guidance provided by the Centre is the only form of guidance formally recognised in terms of the FIC Act and the Regulations issued under the Act. Guidance emanating from industry associations or other organisations, therefore, in the Centre's view, does not have a bearing on compliance with the obligations imposed by the FIC Act or interpretation of its provisions.

The guidance provided **by the Centre** in this Guidance Note, **although authoritative,** is provided as general information only. The Guidance Note does not provide legal advice and is not intended to replace the FIC Act or the Money Laundering Control Regulations ("the Regulations") issued under the FIC Act in December 2002.

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING POLICIES AND PROCEDURES

1. Board approval of a bank's anti-money laundering and terrorist financing policies and procedures

Board of directors' approval of a bank's own internal policies and procedures to address money laundering and terrorist financing is critical if a bank wishes to be seen to be fully committed to its appreciation of, and willingness to, mitigate money laundering and terrorist financing risks in its daily banking operations.

The Centre therefore expects that the internal anti-money laundering and terrorist financing policies and procedures of a bank should be adopted and approved by the board of directors of that bank.

This will also ensure that the board of a particular bank takes ownership of its obligations in terms of the FIC Act. The criminal penalties for failure to comply with the obligations under the FIC Act are severe, and directors may be held personally liable. Forbearance in prosecuting criminal matters under the FIC Act must not be expected.

2. Implementation of Guidance Note 1 in respect of a risk-based approach

Although the FIC Act and the Regulations do not expressly make reference to a risk-based approach, in respect of identification and verification of client particulars, this issue is covered in Guidance Note 1 issued by the Centre in April 2004, and distributed by the Registrar of Banks in terms of Banks Act Circular 4/2004.

Guidance Note 1 indicates that application of a risk-based approach to the verification of the relevant particulars implies that a bank can accurately assess the risk involved. It also implies that a bank can take an informed decision on the basis of its risk assessment as to the appropriate methods and levels of verification that should be applied in a given circumstance.

Guidance Note 1 further states that the assessment of these risk factors should best be done by means of a systematic approach to determine different risk classes and to identify criteria to characterise clients and products. In order to achieve this, a bank would need to document and make use of a risk framework. Such a risk framework should preferably form part of the bank's internal policies and procedures to address money laundering and terrorist financing referred to in paragraph 1, above.

Risk Indicators

3. Risk indicators to be used to differentiate between clients

The FIC Act and the Regulations require that banks identify all clients with whom they do business unless an exemption applies in a given circumstance. Banks, however, are not required to follow a "one size fits all" approach in the methods that they use and the levels of verification that they apply to all relevant clients.

It is imperative that the money laundering risk in any given circumstance be determined on a holistic basis. In other words, the ultimate risk rating accorded to a particular business relationship or transaction must be a function of all factors that may be relevant to the combination of a particular client profile, product type and transaction.

A combination of the following factors may be applied to differentiate between high risk, medium risk and low risk clients:

- product type;
- business activity;
- client attributes, for example, whether the client is on the United Nations list, duration of client relationship with bank, etc;
- source of funds;
- jurisdiction of client;
- transaction value;
- type of entity.

Please refer to Guidance Note 1 for further particulars on the implementation of a risk-based approach.

4. Client profiling procedures for high risk clients

In terms of Regulation 21 of the Regulations, a bank must obtain certain additional information whenever this information may reasonably be required to identify:

- a business relationship or single transaction that poses a particularly high risk of facilitating money laundering activities; or
- the proceeds of unlawful activity or money laundering activities.

In most instances it is a combination of factors, not any one factor that will lead to a conclusion that a transaction or relationship poses a money laundering risk. All circumstances surrounding a business relationship or transaction should be reviewed.

The risk factors referred to in paragraph 3, above, may be helpful to banks in assessing when additional information may be required in

order to enhance the institution's profile of a particular client. In addition there are a number of further factors that may indicate that a business relationship or single transaction poses a high risk of facilitating money laundering activities, or the presence of the proceeds of unlawful activity such as the following:

- a client appears to have accounts with several banks in one geographical area;
- a client makes cash deposits to a general account of a foreign correspondent bank;
- a client wishes to have credit and debit cards sent to destinations other than his or her address;
- a client has numerous accounts and makes or receives cash deposits in each of them amounting to a large aggregated amount;
- a client frequently exchanges currencies;
- a client wishes to have unusual access to safe deposit facilities;
- a client's accounts show virtually no normal business related activities, but are used to receive or disburse large sums;
- a client has accounts that have a large volume of deposits in bank cheques, postal orders or electronic funds transfers;
- a client is reluctant to provide complete information regarding the client's activities;
- a client's financial statements differ noticeably from those of similar businesses;
- a business client's representatives avoid contact with the branch;
- a client's deposits to, or withdrawals from, a corporate account are primarily in cash, rather than in the form of debit and credit normally associated with commercial operations;
- a client maintains a number of trustee accounts or client sub-accounts;

- a client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- a client makes a large volume of cash deposits from a business that is not normally cash intensive;
- a small business in one location makes deposits on the same day at different branches;
- there is a remarkable transaction volume and a significant change in a client's account balance;
- a client's accounts show substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services;
- a client's accounts show a sudden and inconsistent change in transactions or patterns.

The circumstances referred to above may be legitimate features of certain categories of businesses, or may make business sense if viewed in the context of the client's business activities. However, it is equally possible that these features would be unexpected in relation to certain categories of businesses, or would have no apparent business purpose, given a particular client's business activities. The purpose of obtaining additional information concerning certain clients in these circumstances is to assist the bank to more accurately identify truly suspicious behavior or relationships and transactions that pose a risk of money laundering, on the basis of a broader profile of the client than the mere client identification particulars.

The information that a bank must obtain in the circumstances referred to above must be adequate to reasonably enable the bank to determine whether transactions involving a client are consistent with the bank's knowledge of that client and that client's business activities and must include particulars concerning:

- the source of that client's income; and
- the source of the funds that the particular client expects to use in concluding the single transaction or transactions in the course of the business relationship.

5. Client acceptance policies

In terms of the Core Principles, banks should develop clear customer acceptance policies and procedures, including a description of the type of customer that is likely to pose a higher than average risk to a bank. In preparing such policies, banks should take into account all risk indicators, including factors such as the customer's:

- background;
- country of origin;
- public or high profile position;
- linked accounts and;
- business activities.

Banks should develop graduated customer acceptance policies and procedures that require extensive due diligence for higher risk clients. These policies and procedures should form part of a bank's risk framework, referred to in paragraph 2 above.

ESTABLISHING AND VERIFYING IDENTITIES NATURAL PERSONS – SOUTH AFRICAN CITIZENS AND RESIDENTS

6. Clarification of an official identity document

The Regulations define "identification document" in respect of a natural person who is a citizen of, or resident in, the Republic of South Africa, as an official identity document. The Department of Home Affairs describes an official identity document as a green bar-coded identity document. Therefore, old identity documents may not be construed as official identity documents.

Regulation 4 of the Regulations, however, provides for exceptional cases in which a person is unable to produce an official identity document. In such instances, the bank must be satisfied that the client has an acceptable reason for being unable to produce an official identity document. This reason should be noted in the records of the bank. The note should also reflect the details of the staff member who recorded the information. The bank may then accept an alternative valid, meaning current and unexpired, document, which contains the person's:

- photograph;
- full names or initials and surname;
- date of birth; and
- identity number.

The following are examples of documents that may be accepted in such exceptional circumstances as an alternative form of verification:

- valid South African driver's licence; or
- valid South African passport.

Decisions concerning the reasons for being unable to produce an official identity document, which may be accepted by a bank, and the documents that may be regarded as acceptable alternatives, should be based on a bank's risk framework referred to in paragraph 2 above.

7. Clarification of whether the address slip found in identity documents issued by the Department of Home Affairs provides adequate proof of verification of residential address

Regulation 4(3) of the Regulations requires that a bank use "information which can reasonably be expected to achieve" verification of an address. It is the view of the Centre that the address slips issued by the Department of Home Affairs do not constitute information that can reasonably be expected to achieve verification of a person's current address. The Centre does not regard these address slips as independent source documents. In addition, the information contained in an address slip may be outdated and, therefore, may not reflect current information.

8. Alternate means of verification if identity document has been lost or stolen

This issue is addressed under paragraph 6 above.

9. Acceptable KYC procedures for non face-to-face verification

Regulation 4 of the Regulations concerning the verification of a person's identity is based on a view that the customer is met face-to-face when his or her particulars are obtained.

Regulation 18 of the Regulations provides for instances in which client information is obtained in a non face-to-face situation. In such cases,

banks "must take reasonable steps" to confirm the existence of the client and to verify the identity of the natural person involved.

Additional guidance may be taken from the Core Principles. These indicate that banks should apply equally effective customer identification procedures and ongoing monitoring standards for non face-to-face customers. In accepting business from non face-to-face customers:

- banks should apply customer identification procedures to non face-to-face customers that are as effective as those that were applied to customers who were available for interview; and
- there must be specific and adequate measures to mitigate the higher risk.

According to the Core Principles, examples of measures to mitigate risk include:

- certification of documents presented;
- requisition of additional documents to complement those that are required for face-to-face customers;
- independent contact with customer by the bank;
- third party introduction.

Decisions concerning the additional steps to be taken in cases of a non face-to-face situation should be based on a bank's risk framework, referred to in paragraph 2 above.

10. Status of "faxed copies"

Faxed copies of documents may be relevant in instances when client information is obtained in a non face-to-face situation. In such cases, the principles discussed in paragraph 9 above would apply. This implies that documents that are certified as true copies of originals may be accepted, but a bank would have to take additional steps to confirm that the said documents are in fact those of the client in question.

In cases when client information is received in a face-to-face situation, the relevant documents will be sighted as part of the verification process. If copies of those documents are not made at that stage for record keeping purposes, they may be faxed to the bank in question shortly thereafter. The bank should then record that the originals or certified copies of the documents, as the case may be, were sighted as part of the verification process.

11. Examples of acceptable documentation to verify residential address of natural person

Regulation 4(3) of the Regulations sets out instances in which the residential address of a natural person needs to be verified. The most secure form of verification of a residential address would be achieved if a staff member and/or agent of the bank were to visit the residential address of such a natural person to confirm that the person resides at the particular residential address.

In most instances, however, it would be sufficient to review the original document and to obtain a copy of a document that offers a reasonable confirmation of the information in question. Since the documentation must be current, a good practice would be to require documentation that is less than three months old.

Below are examples of documents that may, depending on the circumstances, offer confirmation of a residential address. This list is not exhaustive, and other forms of documentation may be used in the verification process. Decisions as to how residential addresses are to be verified should be based on a bank's risk framework, referred to in paragraph 2 above.

Documents that may offer confirmation of residential address include the following:

- a utility bill reflecting the name and residential address of the person;
- a bank statement from another bank reflecting the name and residential address of the person if the person previously transacted with a bank registered in terms of the Banks Act and that bank had confirmed the person's particulars;
- a recent lease or rental agreement reflecting the name and residential address of the person;
- municipal rates and taxes invoice reflecting the name and residential address of the person;
- mortgage statement from another institution reflecting the name and residential address of the person;
- telephone or cellular account reflecting the name and residential address of the person;
- valid television licence reflecting the name and residential address of the person;
- recent long-term or short-term insurance policy document issued by an insurance company and reflecting the name and residential address of the person; or
- recent motor vehicle license documentation reflecting the name and residential address of the person.

When a recent utility bill from a telephone or cellular account, Eskom or a local authority does not identify the physical street address of the property owner (that is, if the bill is sent to a postal address), the utility bill will still be acceptable provided the customer's name and the erf/stand and township details are reflected on the utility bill. The customer's physical address, erf number and township should be recorded, and the township cross-referenced to the suburb in which the customer resides.

If thereafter there is any doubt about the customer or the physical address of the customer, the erf/stand and township details should be verified by reference to the Deeds Office.

If none of the above is available banks may explore other means to verify a client's address such as an affidavit containing the following particulars from a person co-habiting with the client or an employer of the client:

- name, residential address, identity number of the client and the deponent of the affidavit;
- relationship between the client and the deponent of the affidavit; and
- confirmation of the client's residential address.

12. Acceptable documents for third party verification

In terms of section 21 of the FIC Act, if a client (A) is acting on behalf of another person (B), the bank needs to establish and verify the identity of that other person (B) and the client's (A) authority to establish the business relationship or conclude the single transaction on behalf of that other person (B).

FIC Guidance Note 3 for banks on customer identification and verification and related matters **16**

In terms of Regulation 17 of the Regulations, the bank must obtain from the person acting on behalf of another person (A) information that provides proof of that person's authority (A) to act on behalf of that other natural person, legal person or trust (B).

A bank must verify the information obtained by:

- comparing the particulars of the natural or legal person, partnership or trust with information obtained by the bank from, or in respect of, the natural or legal person, partnership or trust in accordance with Regulation 4 (Verification of information concerning South African citizens and residents), Regulation 6 (Verification of information concerning foreign nationals), Regulation 8 (Verification of information concerning close corporations and South African companies), Regulation 10 (Verification of information concerning foreign companies), Regulation 12 (Verification of information concerning other legal persons), Regulation 14 (Verification of information concerning partnerships) or Regulation 16 (Verification of information concerning trusts) of the Regulations, as may be applicable; and
- establishing whether that information, on the face of it, provides proof of the necessary authorisation.

The following are examples of documents that may be accepted to confirm the authority of a person to act on behalf of another person and to confirm the particulars of the person authorising the third party to establish the relationship:

- power of attorney;
- mandate;
- resolution duly executed by authorised signatories; or

- a court order authorising the third party to conduct business on behalf of another person.

13. Legal incapacity

Regulation 3(2) of the Regulations provides for instances in which a natural person needs to be assisted by another person owing to his/her legal incapacity. Regulation 4 of the Regulations also applies to the verification of the particulars referred to in Regulation 3(2) of the Regulations, namely, the name, date of birth, identity number and residential address of the person assisting the person without legal capacity.

14. Ongoing client detail maintenance

Regulation 19 of the Regulations states that a bank must take reasonable steps, concerning the verification of client identities that may apply to that bank in respect of an existing business relationship so as to maintain the correctness of particulars that are susceptible to change.

Decisions concerning the method by means of which such maintenance is to be achieved should be based on a bank's risk framework, referred to in paragraph 2 above. Some guidance may be taken from international best practice and FATF standards that refer to on going risk-sensitive programmes to maintain relevant client details.

The following procedure for ongoing maintenance of client information may be considered:

- banks should apply their know your client (KYC) procedures to existing clients on the basis of materiality and risk, and should

conduct due diligence reviews of such existing relationships at appropriate times;

- banks need to undertake regular reviews of their existing client records. An appropriate time to do so is when a transaction of significance takes place; or when there is a material change in the way the account is operated; and
- if a bank becomes aware at any time that it lacks sufficient information about an existing client, it should take steps to ensure that all relevant KYC information is obtained as quickly as possible.

NATURAL PERSONS – FOREIGN NATIONALS

15. Identification and verification

Regulation 6(3) of the Regulations provides for instances in which a bank deems it reasonably necessary to obtain, in addition to a person's identity document (foreign passport), further information or documentation verifying the identity of such a person.

In instances when a bank requires further confirmation of the identity of a foreign national, the bank may obtain such confirmation:

- a letter of confirmation from a person in authority (for example, from the relevant embassy), which confirms authenticity of that person's identity document (passport).

Decisions concerning when further confirmation of the identity of a foreign national may be required and the nature of such information should be based on a bank's risk framework, referred to in paragraph 2 above.

LEGAL ENTITIES

16. Identification and verification of subsidiaries of listed companies

Exemption 6(1) of the Exemptions, applies to companies that are listed on a stock exchange mentioned in the Schedule to the Exemptions. This Exemption does not apply to subsidiaries, whether wholly owned or not, of listed companies.

17. Identification and verification of pension and provident funds

As a general rule, a bank has to establish and verify the identity of a pension and a provident fund. A pension and a provident fund will fall into the category of "other legal person" (Regulation 11 of the Regulations).

The bank must obtain from the natural person acting or purporting to act on behalf of the pension or provident fund:

- the name of the pension or provident fund;
- the address of the legal entity establishing the fund;
- the full names, date of birth and identity number or passport number of the trustees or any other persons appointed to act on behalf of the pension and provident fund or who purports to establish a business relationship or to enter into a transaction with the bank on behalf of the pension and provident fund; and
- the residential address of the trustees or any other persons appointed to act on behalf of the pension and provident fund or who purports to establish a business relationship or to enter into a transaction with the bank on behalf of the pension and provident fund.

18. Identification and verification of "off the shelf" companies

Banks should identify and verify the information pertaining to "off the shelf" companies in the same way they would identify and verify any other company.

PARTNERSHIPS

19. The definition of a partnership

A partnership is a form of business enterprise. A partnership exists when there is a voluntary association of two or more persons engaged together for the purpose of doing lawful business as a partnership, for profit. Partnerships are assumed to exist when the partners actually share profits and losses proportionately, even though there may not be a written partnership agreement signed between the partners.

A partnership is not a legal entity and cannot conduct transactions in its own name. When a person conducts a transaction on behalf of a partnership, the transaction is conducted on behalf of all partners in that partnership jointly. All partners in a partnership are jointly and severally liable for the partnership's liabilities.

20. Clarification of partnership agreements and whether all partners in a partnership should be identified

In terms of Regulation 13(b)(i) of the Regulations, banks are required to identify all partners within a partnership.

In most instances, the interest of a prospective client to open an account will prompt the bank to obtain the information that it needs to undertake its KYC function in terms of the FIC Act and the Regulations. In some instances, a bank would be able (and would even be

expected) to obtain information from third parties in order to establish and/or verify a prospective client's identity. The bank must have policies and procedures at the account opening stage that are designed to capture all the relevant information.

The Centre cannot prescribe to banks the form that such procedures should take, but the Centre would expect such procedures to inform a prospective client that the relationship with the bank is dependent on them providing all required information (which, in the absence of a written partnership agreement would include disclosing all partners and identifying and verifying all disclosed partners).

Where two or more persons are co-signatories on an account the Centre expects those co-signatories to sign a declaration to the bank that they do not act as a partnership.

Decisions concerning account opening policies and procedures, in respect of whether confirmation of the identities of partners should be obtained from third parties, should be based on a bank's risk framework, referred to in paragraph 2, above.

TRUSTS

21. Identification of trusts

The following documents are required to identify a trust in terms of Regulations 15 and 16 of the Regulations:

- trust deed or other founding document;
- letter of authority from the Master of the High Court in South Africa or letter of authority from a competent trust registering authority in a foreign jurisdiction;

- trustees' resolution authorising person/s to act;
- personal details of each trustee, each beneficiary referred to by name in the trust deed or other founding document, the founder and the person/s authorised to act (refer to applicable the FIC Act requirements).

22. Identification and verification of each trustee of a trust

The following Regulations provide clarity on this matter:

- Regulation 15(d)(i) of the Regulations requires that a bank must establish the identity of each trustee.

- Regulation 15(g) of the Regulations requires that the residential address and contact particulars in relation to each trustee be established.

- Regulation 16 of the Regulations further explains how the identity of a trustee, as well as the residential address, must be verified.

There is therefore an obligation on all banks to establish and verify the identity and residential address of each trustee.

ORGANS OF STATE INCLUDING GOVERNMENT DEPARTMENTS

23. Identification and verification of Government departments and organs of state

The FIC Act places an obligation on all banks to establish and verify the identity of their clients. A client of a bank may include a natural

person, a juristic person, such as a close corporation and a company, a partnership, a trust and an organ of state including government departments.

There is an obligation on all banks to establish and verify the identity of their client even if the client is an organ of state including a government department.

Certain organs of state are incorporated as companies and registered with the Registrar of Companies to conduct business and must be identified as companies. In other instances, Government institutions are constituted as legal persons by statute. Regulations 11 and 12 provide for a category of client referred to as "other legal person", which includes organs of state constituted as legal persons by statute.

Sound business practice would indicate that organs of state that are neither incorporated as companies nor constituted as legal persons by a statute should be dealt with in a manner similar to that used in respect of "other legal persons". This would apply to national, provincial and local government departments.

This implies that, among others, the identities of the persons acting on behalf of an organ of state would have to be established and verified. In some circumstances, this may include the Chief Financial Officer ("CFO") acting on behalf of a Government department. In such instances, the full name, date of birth and identity number in respect of individuals acting on behalf of the relevant organs of state should be obtained and verified. In addition, information concerning the contact particulars of such persons should be obtained.

INTERNATIONAL STANDARDS AND BEST BANKING PRACTICE

24. Extent to which international standards (FATF Recommendations, Core Principles) and best banking practice, (the Wolfsberg Principles) apply to South African banks where ever they operate

In interpreting and applying the relevant legislation, international best practice should serve as a reference to clarify what is expected from the banking industry. The FATF Recommendations form the contextual basis for the implementation of the FIC Act. International standards such as the FATF Recommendations and the Core Principles provide the minimum requirements with which countries must comply.

The international standard for banking supervision is based on the Core Principles, which set out the standards that have been designed to be applied by all countries in the supervision of the banks in their jurisdictions. Similarly, all banks supervised by a banking supervisor that adopts the Core Principles are duty bound to adhere to the Principles as a matter of best banking practice.

The approach of the Basel Committee on Banking Supervision to KYC adopts a wider prudential method of review.

Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme which involves more extensive due diligence for higher risk clients and which includes proactive account monitoring for suspicious activities.

In terms of principle 15 of the Core Principles, banking supervisors must determine that

"Banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements".

As a result it is fundamental to the market integrity and financial stability of the South African domestic banking system that international standards, as set out in the Core Principles and best banking practice, is adopted by the banking industry as an extra prudential measure when legislation does not adequately address a specific issue. Supervisory bodies should be enforcing the implementation of best practices in the industries that they supervise.

POLITICALLY EXPOSED PERSONS (PEPs)

25. Definition of a politically exposed person (PEP) and the measures that need to be put in place when dealing with a PEP

A politically exposed person or PEP is the term used for an individual who is or has in the past been entrusted with prominent public functions in a particular country. The principles issued by the Wolfsberg Group of leading international financial institutions give an indication of best banking practice guidance on these issues. These principles are applicable to both domestic and international PEPs.

The following examples serve as aids in defining PEPs:

- Heads of State, Heads of Government and cabinet ministers;

- influential functionaries in nationalised industries and government administration;
- senior judges;
- senior political party functionaries;
- senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations;
- members of ruling or royal families;
- senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities).

According to the Wolfsberg principles, families and closely associated persons of PEPs should also be given special attention by a bank. The term "families" includes close family members such as spouses, children, parents and siblings and may also include other blood relatives and relatives by marriage. The category of "closely associated persons" includes close business colleagues and personal advisers/consultants to the PEP as well as persons, who obviously benefit significantly from being close to such a person.

A bank should conduct proper due diligence on both a PEP and the persons acting on his or her behalf. Similarly, KYC principles should be applied without exception to PEPs, families of PEPs and closely associated persons to the PEP.

26. Treatment of PEPs in relation to other high-risk clients

In terms of the FATF standards, specific action should be taken in relation to PEPs as a category of high-risk client. In addition to performing customer due diligence measures, banks should put in place appropriate risk management systems to determine whether a

customer, a potential customer or the beneficial owner is a PEP. In addition banks:

- should obtain senior management approval for establishing business relationships with a PEP. When the client has been accepted, the bank should be required to obtain senior management approval to continue the business relationship;

- should take reasonable measures to establish the source of wealth and the source of funds of customers and the beneficial owners identified as PEPs;

- should conduct enhanced ongoing monitoring of a relationship with a PEP.

27. Policies for dealing with PEPs

It is crucial that banks address the issue of PEPs in their risk framework, referred to in paragraph 2, and group money laundering control policy. PEPs should be regarded as high-risk clients and, as a result, enhanced due diligence should be performed on this category of client. Heightened scrutiny has to be applied whenever PEPs or families of PEPs or closely associated persons of the PEP are the contracting parties or the beneficial owners of the assets concerned, or have power of disposal over assets by virtue of a power of attorney or signature authorisation.

The Wolfsberg principles provide additional guidance on how to recognise and deal with a PEP. In addition to the standardised KYC procedures, the following prompts are appropriate to recognise a PEP:

- the question whether clients or other persons involved in the business relationship perform a political function should form part of the standardised account opening process, especially in cases of clients from corruption prone countries;

- client advisers should deal exclusively with clients from a specific country/region to improve their knowledge and understanding of the political situation in that country/region;

- the issue of PEPs should form part of a banks regular KYC training programs;

- banks may use databases listing names of PEPs including their families, closely associated persons and advisors.

CORRESPONDENT BANKS

28. Measures that need to be put in place in respect of correspondent banking relationships

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Correspondent bank accounts enable banks to conduct business and provide services that the banks do not offer directly.

According to the Core Principles, 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 KYC policies.

In particular, the Core Principles provide that 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 KYC standards or have been identified by FATF as being "non co-operative" in the fight against anti-money laundering.

The Wolfsberg principles sets out the following risk indicators that a Bank shall consider, to ascertain what reasonable due diligence or enhanced due diligence it will undertake:

- **the correspondent banking client's domicile** - the jurisdiction where the correspondent banking client is based and/or where its ultimate parent is headquartered may present greater risk. Certain jurisdictions are internationally recognised as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Institutions will review pronouncements from regulatory agencies and international bodies, such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the correspondent banking client is based and/or in which its ultimate parent is headquartered.

- **the correspondent banking client's ownership and management structures** - the location of owners, their corporate legal form and the transparency of ownership structure may present greater risks. The involvement of a PEP in the management or ownership of certain correspondent banking clients may also increase the risk.

- **the correspondent banking client's business and customer base** - the type of businesses the correspondent banking client engages in, as well as the type of the markets the correspondent banking client serves, may present greater risks. Consequently, a correspondent banking client that derives a substantial part of its business income from higher risk clients may present greater risk. Higher risk clients are those clients of a correspondent banking client that may be involved in activities or are connected to jurisdictions that are identified by credible sources as activities or countries being especially susceptible to money laundering. Each institution may give the appropriate weight to each risk factor, as it deems necessary.

FATF Recommendation 7 states that financial institutions such as banks should, in addition to performing normal due diligence measures, do the following in relation to cross-border correspondent banking and other similar relationships:

- gather sufficient information about a respondent bank to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the bank and the quality of supervision, including whether the institution has been subject to a money laundering or terrorist financing investigation or regulatory action;
- assess the respondent bank's anti-money laundering and terrorist financing controls;
- obtain approval from senior management before establishing new correspondent relationships;
- document the respective responsibilities of each bank;
- with respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to

accounts of the correspondent and that the respondent bank is able to provide relevant customer identification data upon request to the correspondent bank.

EXEMPTIONS

29. Clarification of Exemption 5 – foreign clients

Exemption 5 of the Exemptions deals with countries situated in a foreign jurisdiction. According to Exemption 5 accountable institutions, including banks, are exempted from compliance with the provisions of section 21 of the FIC Act that require the verification of the identity of a client of that institution, if:

- the client is situated in a country, where, to the satisfaction of the relevant supervisory body, anti-money laundering regulation and supervision of compliance with such anti-money laundering regulation, which is equivalent to that applicable to the bank, are in force;

- a person or institution in that country, which is subject to anti-money laundering regulation confirms in writing, to the satisfaction of the bank that the person or institution, has verified the particulars concerning that client that the bank had obtained in accordance with section 21 of the FIC Act; and

- the person or institution undertakes to forward all documents obtained in the course of verifying such particulars to the bank.

The country in which the client is situated has to have anti-money laundering regulation and supervision of compliance with such anti-money laundering regulation in force. All FATF member countries are

deemed to have adequate anti-money laundering legislation and supervision of compliance with such legislation in place.

If a country is not a FATF member country, more careful scrutiny of the anti-money laundering/combating of terrorist financing systems in that country should be undertaken to establish whether the requirements applicable to a specific institution are equivalent to the requirements of the South African legislation. If this is not the case, this exemption does not apply, and the entity has to be identified and verified as stipulated in the FIC Act and the Regulations.

30. Clarification of the difference between Exemptions 5 and 16 - identifying a bank or a client of a foreign country or institution

In terms of Exemption 16 of the Exemptions, a bank in South Africa is exempted from having to identify a bank in another country when the anti money laundering regulation and supervision that applies to that foreign bank is to the satisfaction of the supervisory body. This exemption applies in the case of transactions between the two banks and not to transactions of the underlying clients of the foreign bank.

Exemption 5 of the Exemptions relates to the underlying clients of a foreign institution, such as a bank. This exemption exempts a bank in South Africa from the verification of a foreign client's identity in cases when a regulated institution in the relevant country can verify that client's identity. The South African bank still has to establish the client's identity, but can rely on the verification undertaken by the foreign institution. The conditions to exemption 5 are that the institution providing the verification of the client's identity must be subject to anti-money laundering regulation and supervision to a standard that meets the satisfaction of the relevant supervisory body. The foreign institution should forward all documents relative to the verification of the client's identity to the South African bank, in due course.

Both of these exemptions require an indication from the appropriate supervisory body as to which countries it considers to be applying satisfactory anti money laundering regulation and supervision to the relevant institutions. In the absence of such an indication, the best practice is to use the FATF issued list of non-cooperative countries and territories ("the NCCT") as an indication of jurisdictions that lack the intent to apply AML and CFT procedures. Extreme caution should be applied in transactions with these black listed jurisdictions. It would also be acceptable for supervisors and accountable institutions to regard those countries, which are actual FATF member countries, as being jurisdictions applying adequate AML and CFT procedures.

GLOSSARY

The term **"bank"** in this guidance note refers to institutions that conduct banking business, in other words accountable institutions referred to in:

- **Item 6** (A person who carries on the "business of a bank" as defined in the Banks Act, 94 of 1990), or
- **Item 7** (A Mutual Bank as defined in the Mutual Banks Act, 124 of 1993),

which may be expected to be licensed as banks or mutual banks, respectively, and accountable institutions, which conduct similar activities, namely those referred to in:

- **Item 14** (A Postbank referred to in section 51 of the Postal Services Act 124 of 1998), or
- **Item 16** (The Ithala Development Finance Corporation Limited).

of Schedule 1 to the FIC Act.

"**The Centre**" means the Financial Intelligence Centre established by section 2 of the FIC Act.

"**Financial Intelligence Centre Act**" (herein referred to as the FIC Act) refers to the Financial Intelligence Centre Act, 2001 (Act No 38 of 2001).

Money Laundering Control Regulations (herein referred to as "the Regulations") refers to the regulations made in terms of section 77 of FIC Act and promulgated in Government Notice 1595 published in Government Gazette No. 24176 of 20 December 2002.

Money Laundering Control Exemptions (herein referred to as "the Exemptions") refers to exemptions made under section 74 of FIC Act and

promulgated in Government Notice 1596 published in Government Gazette No. 24176 of 20 December 2002.

The **Financial Action Task Force ("FATF")** is an inter-governmental body that engages in the development and promotion of national and international policies and standards to combat money laundering and terrorist financing. The FATF is both a policy-making and standard setting body. It was created in 1989 and works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. Further information concerning the FATF is available at **www.fatf-gafi.org**.

The **FATF Recommendations** refers to the 40 Recommendations on combating money laundering plus 9 Special Recommendations on combating terror financing of the FATF that set out the basic framework to combat money laundering and terrorist financing. The FATF Recommendations are intended to be of universal application and have come to be accepted by organisations such as the World Bank and the International Monetary Fund to be the international standard to benchmark efforts to combat money laundering and terrorist financing. Since its creation the FATF has spearheaded the effort to adopt and implement measures designed to counter the use of the financial system by criminals. The FATF Recommendations can be accessed from **www.fatf-gafi.org**.

The **Core Principles** refer to the **Basel Core Principles for Effective Banking Supervision** which is the comprehensive set of twenty-five Core Principles that have been developed by the Basel Committee on Banking Supervision, a Committee of banking supervisory authorities which was established by the central bank Governors of the Group of Ten countries in 1975, as a basic reference for effective banking supervision. The Core Principles were designed to be applied by all countries in the supervision of the banks in their jurisdictions. The Core Principles can be accessed from **www.bis.org**.

The **Wolfsberg Principles** refer to **Global Anti Money Laundering Guidelines for Private Banks**, which sets out global guidance for sound business conduct in international private banking, **Correspondent Banks and Politically Exposed Persons**. The principles can be accessed from **www.wolfsberg-principles.com**.

The **United Nations List** means the list of individuals and entities as issued by the United Nations 1267 Sanctions Committee. The updated UN list can be accessed from **www.un.org/Docs/sc/committees/1267/1267ListEng**. This list is published in a Government Gazette of the Republic of SA from time to time by proclamation under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004). The current proclamation can be accessed from **http://www.saps.gov.za/docs_publs/legislation/terrorism/gazette27598pg1_32.pdf** and **http://www.saps.gov.za/docs_publs/legislation/terrorism/gazette27598pg33_64.pdf**.

Organs of State as defined under section 239 of the **Constitution of the Republic of South Africa 1996 (Act 108 of 1999)** means

a) any department of state or administration in the national, provincial or local sphere of government; or
b) any other functionary or institution
   i) exercising a power or performing a function in terms of the Constitution or a provincial Constitution; or
   ii) exercising a public power or performing a public function in terms of any legislation,

   but does not include a court or judicial officer.

Shell Banks refers to a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

Payable through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Issued by the Director
Financial Intelligence Centre
14 July 2005

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Publications: Tel: (012) 334-4508, 334-4509, 334-4510
Advertisements: Tel: (012) 334-4673, 334-4674, 334-4504
Subscriptions: Tel: (012) 334-4735, 334-4736, 334-4737
Cape Town Branch: Tel: (021) 465-7531
Gedruk deur en verkrygbaar by die Staatsdrukker, Bosmanstraat, Privaatsak X85, Pretoria, 0001
Publikasies: Tel: (012) 334-4508, 334-4509, 334-4510
Advertensies: Tel: (012) 334-4673, 334-4674, 334-4504
Subskripsies: Tel: (012) 334-4735, 334-4736, 334-4737
Kaapstad-tak: Tel: (021) 465-7531