Subject: AML/CTF Policy

Chapter 1 - INTRODUCTION

The Financial Intelligence Centre Act, promulgated in 2001 in South Africa, sets up anti-money laundering procedures to prevent criminal groups and individuals from converting illegal profits into “clean money”. FICA requires all individuals and institutions to report specified as well as unusual or suspicious transactions to the Financial Intelligence Centre.

Money laundering (ML) is a term used to describe a number of techniques, procedures or processes in which funds obtained through illegal, unlawful or criminal activities are converted into assets in such a way so as to conceal their true origin, ownership or any other factors that may indicate an irregularity.

The main objective of money laundering is to legitimize income originating from these sources. Generally, money laundering occurs in three stages:

1. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's cheques, or deposited into accounts at financial institutions.

2. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

3. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorism financing (TF) is the financial support of terrorism or of those who encourage, plan, or engage in terrorist activities.

Money laundering and terrorism financing (ML/TF) risk refers to the likelihood and impact of the firm being involved with or facilitating this unlawful activity. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

POLICY

Our Firm is committed to the highest standards of anti-money laundering (AML) compliance and requires management and employees to adhere to these standards, and the contents of our internal policies and procedures, to prevent the use of our products and services for money laundering purposes, terrorist financing or other financial crime.

OBJECTIVE

The Firm is intent on satisfying its local regulatory and international obligations in a sustainable manner and our policies, procedures and internal controls are designed to ensure compliance.

The objective is to:

1. Establish the framework to fight against money laundering and assist law enforcement agencies
2. Meet its regulatory obligations in the identification, treatment and management of ML/TF risk;
3. Protect the firm from reputational risk and breaches of regulatory requirements that may lead to severe fines and penalties; and
4. Safeguard the firm, its customers and employees from becoming a victim of, or unintentional accomplice to, ML/TF activities.
5. Lay down compliance norms for all employees

GOVERNANCE

The designated the AML/CTF Compliance Officer (MLCO) is appointed in terms of a written authorization.

The MLCO is responsible for:

- drawing up the appropriate AML/TF procedures,
- regularly reviewing and updating the policy with changes in laws, or the business
- allocating duties and responsibilities to ensure compliance and implementation of the policy,
- coordinating training and disseminating information,
- reviewing products and services offered to ensure compliance with the internal policy and procedures,
- Prompt reporting of reportable transactions to the Regulator
- Prompt reporting as and when required both to the Regulator and the Governing authority of the firm on compliance

All material documents, processes and procedures, including this policy, that form part of the framework, must be approved and adopted in terms of a written resolution by the Governing authority.

Management is responsible for ongoing oversight of the program as it affects their area of responsibility and for delivering effective compliance on a day to day basis.

Chapter 2 - REGULATION

The Financial Intelligence Centre (FIC) is South Africa's Anti-Money Laundering/Counter-Terrorism Financing Regulator. The principal pieces of applicable legislation include:

1. Financial Intelligence Centre Act 38 of 2001 ("FICA"), as amended by The Financial Intelligence Centre Amendment Act 11 of 2008;
2. The Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("POCDATARA"), which criminalizes commercial acts likely to support the commission of specified offences, i.e. terrorism and the financing of terrorist activity;
3. The Prevention of Organized Crime Act 121 of 1998 ("POCA"), which criminalizes money laundering in general and creates a number of offences; and
4. The Prevention and Combating of Corrupt Activities Act 12 of 2004 ('PRECCA"), which creates offences in connection to corrupt activities relating to, amongst others, judicial officers.

FRAUD AND CORRUPTION

The firm is committed to the eradication of fraud and corruption in the workplace and has a zero-tolerance approach. All fraud will be investigated and addressed by applying all remedies available within the full extent of the law. It is the responsibility of all employees to immediately report any allegation of fraud to their immediate manager, or to the Compliance officer. Cases of fraud and corruption can be reported by the Compliance officer to the National Anti-Corruption Hotline (corruptionwatch.co.za / 0800 023 456)

CUSTOMER ACCEPTANCE

FSP's are expected to develop clear customer acceptance and procedures, including a description of the type of customer that is likely to pose a higher than average risk to their business of "POTENTIAL MONEY LAUNDERING ACTIVITIES."

Although the financial products to which the regulation in terms of FICA applies, predominantly includes voluntary money investments and savings, or cash transactions, it is the firm's policy to remain vigilant in all areas in order to identify and report any incidents which may possibly constitute money laundering or terrorist financing activities.

The firm's policy is to accept only those customer s whose identity is established by conducting a due diligence appropriate to the risk profile of the customer.

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

- product type;
- transaction value;
- background;
- country of origin;
- public or high-profile position; (PEP's)
- business activities/ occupation

It is the policy of the FSP to accept the following customers as "low risk" customers, unless information to the contrary is obtained:

1. Local Individuals and entities whose identities and sources of wealth can be easily identified and who are not:
    a. listed on any sanctions list – whether jurisdiction or United Nations known terrorist and
    b. PEP's and
    c. Who are transacting in a financial product where the risk of money laundering is limited or negligible and/or
    d. engaging in just a single transaction but have an ongoing relationship with the FSP
2. Juristic entities where the nature of the business is such that the risk of money laundering is limited or negligible
3. Local Individuals and entities whose identities and sources of wealth can be easily identified and who
    a. transfer monies using electronic funds transfer and not cash deposits
    b. are utilizing a low risk financial product
4. Existing customer s with whom a relationship is already established, and the customer is known to the Firm

High Risk customers requiring extensive due diligence include:

1. Non-Resident Customers and Customers based in high risk countries / jurisdictions or locations
2. Politically exposed persons (PEPs) and customers who are close relatives of PEPs
3. Non-face to face customers
4. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries,
5. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their customers where the identity of the underlying customer is not disclosed to the financial institution.

We do not accept business from entities that cannot be identified, or shell banks.
We do not accept cash or third-party payments.

Chapter 3 - AML PROCEDURE MANUAL

The Financial Intelligence Centre (FIC) has established a Compliance Contact Centre to deal with queries related to compliance with the Financial Intelligence Centre Act

The FIC Compliance Contact Centre can be reached at: 0860 222 200 email: fic_feedback@fic.gov.za

For calls unrelated to compliance matters, call the FIC on: 0860 342 342

The Firm must allocate responsibility for internal controls and effective risk management to a member of senior management and must ensure that the appointed MLCO has sufficient seniority and authority to carry out his task, whether or not these two functions are held by the same person.

The firm needs systems and controls, appropriate to the size and nature of the business, sufficient to achieve the following:

- determining and recording the firm's systems for anti-money laundering training (awareness), customer acceptance, customer due diligence and on-going monitoring requirements (including whether a customer is a PEP), consultation with and internal reporting to the MLCO, and distributing and implementing policies and procedures to all relevant staff;
- development and documentation of the firm's risk assessment of its business;
- training of all relevant staff, including systems and controls to ensure training is undertaken/attended and understood;
- methods for identification of topical update material and its dissemination as appropriate to senior management and other personnel;
- systems for periodic testing that policies and procedures comply with legislative and regulatory requirements;
- monitoring the compliance of the firm with policy and procedures, including reporting to senior management on compliance and addressing any identified deficiencies.

The purpose of this Internal Procedure Manual is to ensure compliance with counter money laundering legislation and to ensure that each employee knows his role in complying with the requirements as imposed. Although there is a summary of the internal rules, the entire program, policy and procedures is adopted as the Rules of the Firm.

These procedures apply to any product where potential money laundering may occur, such as voluntary savings, investments, unit trusts, deposits and sales, as well as to any transactions which may be reportable in any way.

DEFINITIONS

THE LEGAL STUFF

"accountable institution" means all businesses or persons listed in Schedule 1 to the Act and includes (but is not restricted to), all listed companies, all estate agents, all insurance companies, all long term/ life insurance intermediaries and all unit trust management companies.

"bearer negotiable instrument" for the purposes of this Act, means any instrument that may on demand by the bearer thereof be converted to the currency of the Republic or that of another country, and includes, amongst others, cheques, promissory notes or money orders;

"business relationship" means an arrangement between a customer and an accountable institution for the purpose of concluding transactions on a regular basis;

"FIC" means the Financial Intelligence Centre, the government authority who ensures compliance with the Act

“POCDATARA” means Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004

"transaction" a once-off transaction carried out other than in the normal course of business for one of the parties (see business relationship definition).

APPLICATION OF THE ACT

An accountable institution may not establish a business relationship or conclude a single transaction with a customer unless the accountable institution has taken the prescribed steps

The requirements of the Act apply to all transactions, unless these are specifically exempted. This means every transaction, whether “cash” or not, should comply with the KYC, as well as reporting obligations, unless specifically exempted.

THE LEGAL STUFF - FICA

EXTRACTS FROM THE FINANCIAL INTELLIGENCE CENTRE ACT 38 OF 2001

Section 7 - Exemption from Parts 1 and 2 of Chapter 3 of Act 38 of 2001

1) Every accountable institution which performs the functions of an accountable institution referred to in items 5, 8, 12, 17 and 18 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of Parts 1 and 2 of Chapter 3 (duty to identify customer s and duty to keep records) of the Act in respect of every business relationship or single transaction concerning –
    a. any long term insurance policy which is a fund policy or a fund member policy as defined in the Long-term Insurance Act, 1998 and the regulations thereto and in respect of which the policyholder is a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962;
    b. any unit trust or linked product investment effected by a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962, including an investment made to fund in whole or in part the liability of the fund to provide benefits to members or surviving spouses, children, dependents or nominees of members of the fund in terms of its rules;
    c. any annuity purchased as a compulsory annuity in terms of the rules of a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962;
    d. any reinsurance policy issued to another accountable institution;

e. any long-term insurance policy classified in terms of the Long term Insurance Act, 1998 as an assistance policy;
f. any long term insurance policy which provides benefits only upon the death, disability, sickness or injury of the life insured under the policy;
g. any long-term insurance policy in respect of which recurring premiums are paid which will amount to an annual total not exceeding R25 000,00, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every customer –
    i. who increases the recurring premiums so that the amount of R25 000,00 is exceeded;
    ii. who surrenders such a policy within three years after its commencement; or
    iii. to whom that accountable institution grants a loan or extends credit against the security of such a policy within three years after its commencement;
h. any long term insurance policy in respect of which a single premium not exceeding R 50 000,00 is payable, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every customer –
    i. who surrenders such a policy within three years after its commencement; or
    ii. to whom that accountable institution grants a loan or extends credit against the security of such a policy within three years after its commencement;
i. any contractual agreement to invest in unit trust or linked product investments in respect of which recurring payments are payable amounting to an annual total not exceeding R 25 000,00, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every customer who liquidates the whole or part of such an investment within one year after the making of the first payment;
j. any unit trust or linked product investment in respect of which a once-off consideration not exceeding R 50 000,00 is payable, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every customer who liquidates the whole or part of such an investment within one year after the making of the first payment;
k. any other long term insurance policy on condition that within the first three years after the commencement of the policy the surrender value of the policy does not exceed twenty per cent of the value of the premiums paid in respect of that policy.

Section 18 - Exemptions do not apply in case of suspicious and unusual transactions

No exemption referred to in paragraph 4 (1), 5 (1), 6 (1), 9 and 13 of this Schedule shall apply in any circumstances where consideration is given to the making of a report under section 29 of the Act unless the accountable institution concerned may, by carrying out the required steps to which the exemptions referred to in those paragraphs apply, directly or indirectly alert, or bring information to the attention of another person which will, or is likely to, prejudice an investigation.

PLAIN LANGUAGE - EXEMPT PRODUCTS FROM KYC

Every accountable institution must FICA every transaction, unless there is an exemption or exclusion. The following products are exempt from having to identify and keep records of this identification process, although the reporting obligations still apply.

NOTE: REGARDLESS OF WHAT PRODUCT IS SOLD, IF A CASH TRANSACTION (SUCH AS THE SALE/ SERVICING OF A VEHICLE) HAPPENS, THE CUSTOMER MUST BE IDENTIFIED AND VERIFIED

- Any Long Term insurance policy where the surrender value of the policy is less than twenty per cent of the premiums or the policy is "pure risk"(includes all pure risk policies/ credit life)
- Short term insurance policies and Medical Aids are NOT included. (warranties/ extended warranties/ gap cover etc.)
- A long term insurance policy (fund policy or a fund member policy) held by a pension fund, provident fund or retirement annuity fund
- A unit trust (collective investment scheme) or linked product investment made by a Pension Fund, Provident Fund or Retirement Annuity (including investments made to provide benefits to members or surviving spouses, children, dependents or nominees of members of the fund in terms of its rules)
- A compulsory Annuity (retirement benefits paid out as an annuity/ "pension" at retirement)
- A reinsurance policy issued to another accountable institution
- An Assistance Policy – this is a life policy with a maximum value of risk policy benefits of R30 000 or an annuity where the capital amount buying the annuity is less than R30 000
- A Long-Term insurance policy where annual premiums are not more than R25 000.
- If the premium total is increased to be more than R25 000 per year, OR a loan/ surrender/ part surrender is taken within the first 3 years full KYC is required
- A Long Term insurance policy with a single premium of less than R 50 000.If the premium total is increased to be more than R50 000, OR a loan/ surrender/ part surrender is taken within the first 3 years full KYC is required
- Unit trusts / linked product investments where recurring payments are less than R 25 000 except where a customer repurchases all or part within the first year
- Unit trusts / linked product investments with a single investment less than R 50 000 except where a customer repurchases all or part within the first year

Chapter 4 - THE RULES

FIC ACT THE RULES

Section 42. Formulation and implementation of internal rules. —

1) An accountable institution must formulate and implement internal rules concerning—
    a. the establishment and verification of the identity of persons whom the institution must identify in terms of Part 1 of this Chapter;
    b. the information of which record must be kept in terms of Part 2 of this Chapter
    c. the manner in which and place at which such records must be kept;
    d. the steps to be taken to determine when a transaction is reportable to ensure the institution complies with its duties under this Act; and such other matters as may be prescribed
2) Internal rules must comply with the prescribed requirements.
3) An accountable institution must make its internal rules available to each of its employees involved in transactions to which this Act applies.
4) An accountable institution must, on request, make a copy of its internal rules available to
    a. the Centre;
    b. a supervisory body which performs regulatory or supervisory functions in respect of that accountable institution.

FICA REGULATIONS CHAPTER 5 INTERNAL RULES

Section 25. Internal rules concerning establishment and verification of identities.

The internal rules of an accountable institution concerning the establishment and verification of identities must—

1) provide for the necessary processes and working methods which will cause the required particulars concerning the identities of the parties to a business relationship or single transaction to
2) be obtained on each occasion when a business relationship is established or a single transaction is concluded with the institution
3) provide for steps to be taken by the relevant staff members aimed at the verification of the required particulars concerning the identities of the parties to a business relationship or single transaction;
4) provide for the responsibility of the management of the institution in respect of compliance with the Act, these regulations and the internal rules;
5) allocate responsibilities and accountability to ensure that staff duties concerning the establishment and verification of identities are complied with;
6) provide for disciplinary steps against the relevant staff members for non-compliance with the Act, these regulations and the internal rules; and
7) take into account any guidance notes concerning the verification of identities which may apply to that institution.

Section 26. Internal rules concerning the keeping of records.

The internal rules of an accountable institution concerning the keeping of records in terms of section 22 of the Act must—

1) provide for the necessary processes and working methods to ensure that the relevant staff members of the institution obtain the information of which record must be kept on each occasion when a business relationship is established or a transaction is concluded with the institution;
2) provide for the responsibility of the management of the institution in respect of compliance with the Act, these regulations and the internal rules;
3) allocate responsibilities and accountability to ensure that staff duties concerning the establishment and verification of identities are complied with;
4) provide for disciplinary steps against the relevant staff members for non-compliance with the Act, these regulations and the internal rules;
5) provide for the necessary processes and working methods to ensure that the accuracy and that the integrity of those records are maintained for the entire period for which they must be kept;
6) provide for the necessary processes and working methods to ensure that access as may be required or authorised under the Act by the relevant staff members to those records can be obtained without undue hindrance; and;
7) take into account any guidance notes concerning the verification of identities which may apply to that institution.

Section 27. Internal rules concerning reporting of information.

The internal rules of an accountable institution concerning reporting of suspicious and unusual transactions must—

1) provide for the necessary processes and working methods which will cause suspicious and unusual transaction to be reported without undue delay;
2) provide for the necessary processes and working methods to enable staff to recognise potentially suspicious and unusual transactions or series of transactions;
3) provide for the responsibility of the management of the institution in respect of compliance with the Act, these regulations and the internal rules;
4) allocate responsibilities and accountability to ensure that staff duties concerning the reporting of suspicious and unusual transactions are complied with;
5) provide for disciplinary steps against the relevant staff members for non-compliance with the Act, these regulations and the internal rules; and
6) take into account any guidance notes concerning the reporting of suspicious or unusual transactions which may apply to that institution.

Failure to formulate and implement internal rules. —
An accountable institution that fails to—

a) formulate and implement internal rules in accordance with section 42 (1) and (2);
b) make the internal rules available to its employees in accordance with section 42 (3); or
c) make a copy of its internal rules available to the Centre or a supervisory body in terms of section 42 (4), is guilty of an offence

THE RULES SUMMARY

- Rule 1 – MLCO/Compliance Officer

The Governing authority of the Firm shall ensure the appointment of a suitable Money Laundering Control Officer. The Money Laundering control officer is responsible for ensuring compliance with the Act, the Firms policies and procedures, and these internal rules

- Rule 2 - Sanction

Failing to comply with the provisions of the Act, the internal policy and procedures and these internal rules will result in disciplinary action and possible criminal sanction of the offender

- Rule 3 – Registration compliance

All accountable and reporting institutions are required to register with the Financial Intelligence Centre and ensure that registration information remains current and correct. The MLCO is responsible for ensuring compliance with this at all times

- Rule 4 - Training and awareness

All applicable persons must be adequately trained annually and equipped to comply with the requirements of legislation and internal policies and procedures. Each employee is obliged to read through the AML training material and ensure that he/she fully understands the contents, duties and obligations. A training register must be kept on file recording this and updated annually.

- Rule 5 - Procedures

The correct customer identification, verification, and record keeping procedures must followed at all times and compliance with the contents of the firm's policies and procedures is an ongoing requirement.

- Rule 6 - Reporting

Every employee who becomes aware of a reportable transaction has a duty to report this to the MLCO within the required timeframes.

- Rule 7 - Confidentiality

The fact that a report has been made [or a suspicion that a report has been made], or the information contained in the report may not be disclosed to any person, except as provided for in the Act. Any request for information held by the Company relating to the Act is to be referred to the MLCO.

- Rule 8 – Records

All records shall be securely and confidentially kept for the required period Staff should consult with MLCO should they require further clarification of the internal rules or provisions of the Act.

CHAPTER 6 REGISTRATION

Money laundering control measures

Measures to promote compliance by accountable institutions 43B. Registration by accountable institution and reporting institution

1) Every accountable institution referred to in Schedule 1 and every reporting institution referred to in Schedule 3 must, within the prescribed period and in the prescribed manner, register with the Centre.
2) The registration of an accountable institution and a reporting institution contemplated in subsection (1) must be accompanied by such particulars as the Centre may require.
3) The Centre must keep and maintain a register of every accountable institution and reporting institution registered in terms of subsection (1).
4) A registered accountable institution or reporting institution must notify the Centre, in writing, of any changes to the particulars furnished in terms of this section within 90 days after such a change. Section 61A

Any accountable institution or reporting institution that

a) fails to register with the Centre in terms of section 43B; or
b) fails to provide information in terms of section 43B is guilty of an offence. S68(2) A person convicted of an offence mentioned in section 55, 61, 62, 62A, 62B, 62C or 62D, is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R10 million.

The FIC Act requires every accountable institution, and every reportable institution to register with the Financial Intelligence Centre and to ensure that registration details remain correct;

WHERE A FIRM IS BOTH AN ACCOUNTABLE AND A REPORTING INSTITUTION, TWO SEPARATE REGISTRATIONS ARE REQUIRED. Registration numbers will begin with “AI” and “RI”

A registered accountable (AI) / reporting institution (RI) must notify the Centre, in writing, of any changes to the particulars furnished within 90 days after such change.

REGISTRATION PROCESS

- www.fic.gov.za
- click on ACQUIRE LOGIN CREDENTIALS under REPORTS & REQUESTS
- complete all details in the fields provided – note: the validator cannot also be the MLCO

NO UNAUTHORISED PERSON MAY USE LOGIN CREDENTIALS OF A MLCO. WHERE A MLCO LEAVES THE ORGANISATION, A NEW USER REGISTRATION MUST BE OBTAINED WITHIN 24 HOURS

MONEY LAUNDERING CONTROL/REPORTING OFFICER (S43 COMPLIANCE OFFICER)

Training and monitoring of compliance

An accountable institution must appoint a person with the responsibility to ensure compliance by the employees of the accountable institution with the provisions of this Act and the internal rules applicable to them; and the accountable institution with its obligations under this Act

62. Failure to provide training or appoint compliance officer
An accountable institution that fails to
b) appoint the person referred to in section 43 (b)is guilty of an offence. S68(2) A person convicted of an offence mentioned in section 55, 61, 62, 62A, 62B, 62C or 62D, is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R10 million.

- The money laundering control and reporting officer (MLCO) for the business must be a suitable and senior person nominated by the firm.
- Every MLCO must complete the MLCO Appointment Form which shall be placed on the compliance file as part of the general record-keeping.
- If an employee has any questions or any queries or is uncertain of any aspect relating to AML, the employee must report to MLCO reporting officer immediately before any transaction is finalized in order to ensure compliance with FICA.
- The reporting officer has to determine whether or not the transaction is reportable to the Financial Intelligence Centre.

Reporting periods:

- THRESHOLD TRANSACTION 2 DAYS
- TERRORIST RELATED ACTIVITITES 5 DAYS
- SUSPICIOUS OR UNUSUAL TRANSACTIONS 15 DAYS

The MLCO will:

- ensure compliance with applicable money laundering legislation by the FSP and all employees operating under the FSP;
- ensure compliance by everyone in the business with the internal rules;
- report suspicious and unusual transactions to the FIC;
- report property associated with terrorism and or related activities;
- liaise with authorities on developments in respect of applicable legislation;
- report to the FSP in regard to compliance by the FSP and persons operating under the FSP;
- monitor training of the FSP, key individuals, representatives and staff on applicable legislation
- submit online reports in terms of sec 28A of the FIC Act on the appropriate date

CHAPTER 7 TRAINING

Training and monitoring of compliance.
An accountable institution must provide training to its employees to enable them to comply with the provisions of this Act and the internal rules applicable to them;

Failure to provide training or appoint compliance officer
1)An accountable institution that fails to –

a) provide training to its employees in accordance with section 43(a);
b) appoint the person referred to in section 43(b), is guilty of an offence. S68(2) A person convicted of an offence mentioned in section 55, 61, 62, 62A, 62B, 62C or 62D, is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R10 million.

All applicable persons must be properly trained at least annually and equipped to comply with legislation and internal policies and procedures. Each employee is obliged to read through the AML training material and ensure that he/she fully understands the contents, duties and obligations. A training register must be kept on file recording this, and this must be updated annually.

It is critical to be able to demonstrate: (records to be retained of)

1) That training took place
2) Details of the specific training material which was used
3) The details of the staff in attendance
4) Qualification of understanding/assessment (such as a test)

- An annual training plan is to be constructed which takes into account the busy periods of the firm, as well as newly appointed staff.
- No shows or missed training is to be strongly discouraged as this is an indicator of a lack of commitment to AML.
- A perpetual inventory of training records and material is to be maintained.
- Audit staff and compliance officers must have the skills and knowledge to effectively assess the level of compliance within the audited areas.
- Training and independent testing of AML controllers is to annually occur to ensure quality of controls.

CHAPTER 8 CUSTOMER IDENTIFICATION PROCEDURE (SECTION 21, REGULATIONS 2 - 19)

The objective in establishing the identity of the customer is to:

1) Verify the status (legal status of legal entity) through proper and relevant documents
2) Verify that any person acting on behalf of the customer is authorized to do so and to verify the identity authorized person
3) Understand the ownership and control structure of the customer and determine who the natural persons are who ultimately have control

It is important to obtain a clear and comprehensive understanding of the customer, their line of business/occupation, financial resources and expected activities.

A customer profile is compiled based on information obtained, and this profile must be kept up to date. This information can assist in providing an understanding of the anticipated flow of funds and allows a risk rating of the customer, which in turn, facilitates the early detection and reporting of suspicious or unusual activities.

POCDATARA IDENTIFICATION

POCDATARA Act states that the President must issue a proclamation in respect of any entity that has been designated by the United Nations Security Council (the UNSC) in a resolution issued in order to combat or prevent terrorist and related activities.

The persons whose names appear on the sanction lists Security Council Resolution (UNSCR) 1267 (1999) and its successor resolutions, in particular, 1988(2011) and 1989(2011) are limited to members of, or persons associated with the Taliban and Al Qaida.

These two UNSC Resolutions are the only sanctions lists related to terrorist activities which are legally recognized within the Republic of South Africa. Identification procedures are to include screening these lists.
Section 4 of the POCDATARA Act expressly prohibits any person from dealing with property that is associated with acts of terrorism, with persons or organizations that carry out acts of
terrorism or with entities that are sanctioned pursuant to the POCDATARA Act.

Consequently, any dealings with property that is identified in a report under section 28A of the FIC Act will constitute a contravention of section 4 of the POCDATARA Act. In effect, once an institution files a report in terms of section 28A of the FIC Act, this will lead to a requirement to freeze the property and cease to conduct business with the entity in question. OFAC maintains lists of countries and persons associated with terrorism and anti-money laundering and details of customers should be checked
against these lists. The site where this information is held can be accessed at:
http://apps.finra.org/rulesregulation/ofac/1/

FICA KNOW YOUR CUSTOMER (KYC)

FICA requires customers to be identified, and a profile built, which can assist in the identification and reporting of suspicious, unusual, threshold and terrorist financing activities.

The customer identification procedure is to be carried out at the following 3 stages:

1) While establishing a relationship
2) While carrying out a financial transaction
3) Ongoing monitoring of a customer's identification – at least every 24 months

Sufficient information must be obtained in order to risk rate the customer in terms of potential money laundering or terrorist financing activities. Determining what the person does for a living, how they get their funds, and then making sure their transactions make sense are all required elements of knowing your customer.

Customer due diligence for a business is even more significant and includes determining the expected activity, primary industry and geography in which they operate, and the types of products and services used by the customer.

A business relationship: is when a customer does two or more transactions with you that require you to verify the identity of the customer (regardless of whether the transactions are related to each other). You have to assess the customer risk in both new and existing business relationships.

You have to perform a risk assessment at the beginning of a business relationship, although a comprehensive risk profile of the relationship may only become evident once you perform ongoing monitoring of those customers.

At the beginning of a new business relationships, the customer identification and information gathering measures should be robust enough to provide the information needed to feed into the risk assessment. The risk assessment requires you to consider each one of your customer s when assessing their risk for money laundering and terrorist activity financing.

RISK RATE DOCUMENT

An individual written assessment is not required for each customer, as long as you can demonstrate that you put your customer in the correct risk category, according to your policies and procedures, and risk assessment.

The risk rate document provides evidence that we have complied with our internal customer acceptance policies and have sufficient processes in place to identify our customers (KYC) to be alerted to any reportable instance.

PROCESS

All customer information required must be obtained from the customer in a diligent and accurate manner. The information is obtained to ensure that the provider knows its customer (who it is dealing with and whether the person has the necessary authority). Every document (such as ID, Proof of address) must contain the name of the verifier and the date.

Non Face to face : Any faxed/ emailed documents received, where the customer is not identified in person, requires additional due diligence such as:

- acceptance if the fax/ email was certified prior to its being sent by a suitable certifier
- making a telephone call to the telephone number provided that has been independently validated
- using electronic verification to confirm documents provided or using two or three documents from different sources to confirm the information set out in each document.

Check sanctions list. If customer is listed, do not alert, discontinue transaction and report
http://apps.finra.org/rulesregulation/ofac/1/

The matter must be reported to the MLCO where the customer does not provide the necessary information or where the customer refuses to disclose or submit the information required.

Where customer information is received in a face-to-face situation, documents will be seen as part of the verification process. If copies of those documents are not made at that stage they may be faxed, scanned or e-mailed to the accountable institution within a reasonable time.

The accountable institution must then record that the originals or certified copies of the documents, were seen and by whom and dated.

Where the customer is company listed on the JSE or is a legal person and non-controlled customer in respect of the JSE Rules, this step need not be followed unless the transaction is a suspicious, or unusual transaction.

SANCTIONS LIST

Sanctions searching can be executed on the link included in the process, courtesy of FINRA. Complete your customers full name and a search function will identify whether this name is listed on the especially designated nationals sanction list, the Palestinian Legislative Council list, or the Foreign Sanctions Evaders Sanction list.

NATURAL PERSONS

Clarification of an official identity document.
The Regulations define a South African citizen's identification document as an official green bar-coded identity document. Old identity documents are therefore excluded.

Regulation 4 provides for exceptional cases where a person is unable to produce an official identity document. In such instances:

- the accountable institution must be satisfied that the customer has an acceptable reason for being unable to produce an official identity document. This reason should be noted in the records of the accountable institution. The note should also reflect the details of the staff member who recorded the information.

- the accountable institution may then accept an alternative document, which contains the person's photograph; full names or initials and surname; date of birth; and identity number such as a South African driver's licence; or South African passport.
- Non- South African Citizen requires a passport issued by the country of which that person is a citizen.

ACTION

All documents must be verified and contain the name of the verifier as well as the date when the document was verified.

The purpose of dating documents in this instance is an indication that the verification of the customer was done at the take on stage of the relationship.

PROOF OF IDENTIFICATION

Full names and I.D. number together with copy of identity document (where the original is seen) or copy of a valid driver's license (only where the I.D. document is not available, a reason for no I.D. document must be supplied). Certified copies are accepted. The customer must be physically identified

PROOF OF RESIDENTIAL ADDRESS

The most secure form of verification of a residential address is achieved if a staff member and/or agent of the accountable institution visits the residential address of such a natural person to confirm that the person resides at the particular residential address. Alternatively, any of the following documents which reflect the name of the customer and the address details:

- a utility bill reflecting the name and residential address of the person (less than 3 months old)
- 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;(less than 3 months old)
- a recent lease agreement (less than 3 months old)
- a rates and taxes account (less than 3 months old)
- a telephone account (less than 3 months old)
- a mortgage statement (less than 3 months old)
- recent SARS return / IRP5
- a recent insurance policy document
- a payslip or salary advice
- a valid TV license document
- the tax reference and a certified copy of a SARS document reflecting the details

RISK

Establish whether the person is a politically exposed person – if yes, additional due diligence is required

Check to see if the person is listed on the Sanctions list and if this is the case, do not continue with the transaction, and proceed to report the matter.

WHERE A PERSON ACTS ON THE AUTHORITY OF ANOTHER

Where a customer is acting on behalf of another person, the following must be verified:

PROOF OF THE AUTHORITY TO ACT ON BEHALF OF THAT OTHER NATURAL PERSON, LEGAL PERSON OR TRUST

- A Power of Attorney or A Mandate
- A Resolution duly executed by authorized signatories
- A Court Order authorizing the third person to conduct business on behalf of another person

Proof of identification and Proof of residential address of:

- The Authorised Person AND
- The Person on whose behalf they are acting

NATURAL PERSONS UNDER LEGAL INCAPACITY E.G. MINORS/ PERSONS UNDER CURATORSHIP

Customer must be at least 18 years old to open an account with ThinkMarkets.

CLOSE CORPORATIONS. REGISTERED AND TRADE NAME

Certified copies, all duly stamped of the following documents are required:

- Founding Statement, Certificate of Incorporation, Director and Shareholder registers
- Articles

PHYSICAL ADDRESS

The physical address of the business. Where the business has multiple addresses from which it operates, the head office address and the relevant branch office address are required.

NATURAL PERSONS ASSOCIATED WITH THE CLOSE CORPORATION

Proof of identification of every Member and every Person authorized to transact on behalf of the close corporation. Proof of address of every Member and every Person authorized to transact on behalf of the close corporation

RISK

- Establish whether any natural person is a politically exposed person – if yes, additional due diligence is required
- Check to see if the person is listed on the Sanctions list and if this is the case, do not continue with the transaction, and proceed to report the matter.

COMPANIES

THE LEGAL STUFF: FICA REGULATIONS

9) Exemption from regulations made under Act 38 of 2001

1)Every accountable institution which performs the functions of an accountable institution referred to in items 4 and 15 of Schedule 1 to the Act is exempted, in respect of those functions, from compliance with the provisions of regulation 7 (f), 7 (g), 7 (h), 7 (i), 7 (j), 8 (c), 9 (h), 9 (i), 9 (j), 10 (c) and 10 (e) of the Regulations, and of section 22 (1) (a), 22 (1) (b), 22 (1) (c), 22 (1) (d), 22 (1) (e), 22 (1) (h) and 22 (1) (i) of the Act concerning the particulars referred to in those regulations, in respect of a business relationship established, or single transaction concluded, with a client which is

a) a legal person, and
b) a non-controlled client as defined in the Rules of the JSE Securities Exchange South Africa, as amended.

Where the customer is a public company listed on a recognised stock exchange the firm is exempted from certain identification and recordkeeping requirements.

We only need to obtain the following information:
South African listed companies

- the registered name of the company;
- the registration number
- the address from which the company operates, or if it operates from multiple addresses –
- the address of the office wanting to establish a business relationship; and
- the address of its head office;

Foreign listed companies

- the name under which it is incorporated; and
- the number under which it is incorporated

The information referred to above does not have to be verified but we must still keep records of the details of all transactions with the listed company.

COMPANIES NOT LISTED ON THE JSE OR OTHER SECURITIES EXCHANGE

The registered name and registration number and registered address of the entity as well as the trade name of the business (if applicable) and proof of the trade name (stamped by CIPC)

- Certificate of Incorporation (company form CM1),
- Notice of Registered Office and postal address (form CM22).
- Country of incorporation must be established and verified where a company is not registered in South Africa

PHYSICAL ADDRESS

The physical address of the business. Where the business has multiple addresses from which it operates, the head office address and the relevant branch office address are required

NATURAL PERSONS ASSOCIATED WITH THE COMPANY

For a company, the following additional requirements must be met:

- the full names, date of birth and residential address and contact particulars of the manager of the company and each natural person authorised to transact on behalf of the other company; and
- the full names, I.D. number and date of birth or registered name, registration number, registered address, trade name and business address of all persons/entities holding 25% or more of the rating rights of the company concerned;
- The manager or a director must be physically met and identified.

RISK

- Establish whether any natural person is a politically exposed person – if yes, additional due diligence is required
- Check to see if the person is listed on the Sanctions list and if this is the case, do not continue with the transaction, and proceed to report the matter.

PARTNERSHIPS

A partnership is a form of business enterprise and 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. If a partner leaves or dies, the partnership dissolves.

In terms of Regulation 13(b)(i) of the Regulations, accountable institutions are required to identify all partners within a partnership.
Where two or more persons are co-signatories on an account the Centre expects those co-signatories to sign a declaration to the accountable institution that they do not act as a partnership.

NATURAL PERSONS ASSOCIATED WITH THE PARTNERSHIP

- Requirements as per natural persons must be obtained for each partner;
- (proof of identification and proof of address)
- The ID and address details for every manager and person establishing the relationship on behalf of the partnership;
- The name and business address of the partnership and proof thereof;
- A copy of the Partnership agreement, if there is one

RISK

- Establish whether any natural person is a politically exposed person – if yes, additional due diligence is required
- Check to see if the person is listed on the Sanctions list and if this is the case, do not continue with the transaction, and proceed to report the matter.

TRUSTS

Information pertaining to Trusts which have been registered in South Africa may be accessed on the following website: https://icmsweb.justice.gov.za/mastersinformation

- The following is required to identify a trust:
- The name, trust number and a certified copy of the 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;
- The address of the Master of the High Court where the trust is registered;
- The Income Tax number of the trust and a certified copy of the SARS document;
- The Trustees' resolution authorising a person/s to act;
- Particulars of how the beneficiaries of the trust are determined

NATURAL PERSONS ASSOCIATED WITH THE TRUST:

Regulation 15 and 16 requires the verification of the identity and residential address of each natural person who is a:

- trustee,
- beneficiary and
- who acts on behalf of the trust

RISK

- Establish whether any natural person is a politically exposed person – if yes, additional due diligence is required
- Check to see if the person is listed on the Sanctions list and if this is the case, do not continue with the transaction, and proceed to report the matter.

CHAPTER 9 POLITICALLY EXPOSED PERSONS (PEP'S)

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. Due to their position and influence, it is recognized 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). This has been confirmed by analysis and case studies. The potential risks associated with PEPs justify the application of additional anti-money laundering / counter-terrorist financing (AML/CFT) preventive measures with respect to business relationships with PEPs.

The following examples serve as aids in defining PEPs:

- Heads of State, Heads of Government and cabinet ministers;
- Influential functionaries in nationalized 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 organizations;
- Members of ruling or royal families;
- Senior and/or influential representatives of religious organizations (if these functions are connected to political, judicial, military or administrative responsibilities).

Families and closely associated persons of PEPs should also be given special attention and additionally KYC processes applied. 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.

An institution should conduct proper due diligence on both:

- a PEP and
- the persons acting on his or her behalf.

KYC principles must be applied without exception to PEPs, families of PEPs and closely associated persons to the PEP.

This entails obtaining, in addition to the required FICA identification and verification, information and verification of the person's business activities or occupation, with particular reference to:

- SOURCE OF INCOME AND
- SOURCE OF THE TRANSACTION FUNDS.

"PEP"s should be regarded as high-risk customer s and, as a result, enhanced due diligence should be performed on this category of customer .

Heightened scrutiny has to be applied whenever “PEP”s or families of “PEP”s 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 authorization.

Heightened Customer Due Diligence measures include (but are not limited to) obtaining:

1. additional information on the customer;
2. additional information on the intended nature of the business relationship, and on the reasons for intended or performed transactions;
3. information on the source of funds and source of wealth of the customer; and
4. conducting enhanced monitoring of the business relationship, potentially by increasing the number and timing of controls applied and identifying patterns of transactions that warrant additional scrutiny.

The source of wealth refers to the origin of the PEP’s entire body of wealth (i.e., total assets).

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. Although financial institutions 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.

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 financial institution

The aim is to ensure that the reason for the business relationship is commensurate with what one could reasonably expect from the PEP, given his/her particular circumstances.

Where the level or type of activity in the business relationship diverges from what can be reasonably explained, (given the knowledge of the PEP’s source of wealth and source of funds), further assessments of the situation should be undertaken. The outcomes of that assessment should determine if the business relationship is to be established or maintained, or whether further steps would be necessary, such as termination of the business relationship

When assessing the ML/TF risk level of a relationship with a domestic/international organization PEP, financial institutions should take into account such factors as whether the PEP:

- has business interests which are related to his/her public functions (conflict of interest);
- is involved in public procurement processes; whether the PEP holds several (related or unrelated) prominent public functions which may enable influence to be exerted at several key decision-making points in a process, especially in spending departments;
- is from a country which has been identified by the FATF or others as having strategic AML/CFT regime deficiencies, or is known to have a high level of corruption;
- has a prominent public function in sectors known to be exposed to corruption levels, such as the oil and gas, mining, construction, natural resources, defense industries, sports, gaming, gambling sectors; or
- has a prominent public function that would allow him/her to exert a negative impact on the effective implementation of the FATF Recommendations in his/her country. The exact range

- of prominent public positions that this would apply to will likely differ from country to country, but could include the head of state, key ministers and other political or parliamentary leaders.

PROCESS FOR DEALING WITH PEP'S:

1. Determine whether a customer is a PEP. All customers should be asked questions to determine whether they would fall into one of the categories above, or constitute family of any such persons. The risk rate document to be completed at every transaction includes questions in respect of PEP's. This document must be completed and placed on file for every FICA transaction.
    a. The PEP could be the customer or the beneficial owner of an entity that is the customer.
    b. The PEP could be the beneficial owner or beneficiary of the life insurance policy
2. Existing customer s sometimes become PEPs after they enter a business relationship, so it is essential that non-PEP accounts be monitored for a change in the PEP status, customer profile or account activity.
3. Obtain management approval for establishing business relationships with a PEP. When the customer has already been accepted, management approval to continue the business relationship should be obtained;
4. Take reasonable measures to ESTABLISH AND VERIFY the source of wealth and the source of funds of PEPs;
5. Conduct enhanced ongoing monitoring of a relationship with a PEP.

PEP RISK ALERTS

Specific behaviour and individual characteristics of PEPs may raise red flags / risk levels or cause a suspicion:

- Use of corporate vehicles (legal entities and legal arrangements) to obscure i) ownership, ii) involved industries or iii) countries.
- The PEP seems generally uncomfortable to provide information about source of wealth or source of funds.
- The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries.
- The PEP provides inaccurate or incomplete information.
- (Consistent) use of rounded amounts, where this cannot be explained by the expected business.
- Transacting large amounts of cash, use of bank cheques or other bearer instruments to make large payments.
- Other financial institutions have terminated the business relationship with the PEP.
- Other financial institutions have been subject to regulatory actions over doing business with the PEP.
- Personal and business related money flows are difficult to distinguish from each other.
- Financial activity is inconsistent with legitimate or expected activity, funds are moved between financial institutions without a business rationale.
- Transactions between non-customer corporate vehicles and the PEP's accounts.
- A PEP is unable or reluctant to provide details or credible explanations for establishing a business relationship, or conducting transactions.

THE PEP'S POSITION OR INVOLVEMENT IN BUSINESS:

The position that a PEP holds and the manner in which the PEP presents his/her position are important factors to be taken into account. Possible red flags are:

- Additional risks occur if a foreign or domestic PEP from a higher risk country would in his/her position have control or influence over decisions that would effectively address identified shortcomings in the AML/CFT system.
- Foreign or domestic PEPs from countries identified by credible sources as having a high risk of corruption.
- Foreign or domestic PEPs from countries that are dependent on the export of illicit goods, such as drugs.
- Foreign or domestic PEPs from countries (including political subdivisions) with political systems that are based on personal rule, autocratic regimes, or countries where a major objective is to enrich those in power, and countries with high level of patronage appointments.
- Foreign or domestic PEPs from countries with poor and/or opaque governance and accountability.
- Foreign or domestic PEPs from countries identified by credible sources as having high levels of (organized) crime.
- The PEP has a substantial authority over or access to state assets and funds, policies and operations.
- The PEP has control over regulatory approvals, including awarding licenses and concessions.
- The PEP has the formal or informal ability to control mechanisms established to prevent and detected ML/TF.
- The PEP (actively) downplays importance of his/her public function, or the public function s/he is relates to associated with.
- The PEP does not reveal all positions (including those that are ex officio).
- The PEP has access to, control or influence over, government or corporate accounts.
- The PEP (partially) owns or controls financial institutions either privately, or ex officio.
- The PEP (partially) owns or controls the financial institution (either privately or ex officio) that is a counter part or a correspondent in a transaction.
- The PEP is a director or beneficial owner of a legal entity that is a customer of a financial institution.

HIGH RISK INDUSTRIES MAY RAISE THE RISK OF DOING BUSINESS WITH A PEP

- Arms trade and defense industry.
- Banking and finance.
- Businesses active in government procurement, i.e., those whose business is selling to government or state agencies.
- Construction and (large) infrastructure.
- Development and other types of assistance.
- Human health activities.
- Mining and extraction.
- Privatization.
- Provision of public goods, utilities.

CHAPTER 10 KYC DUE DILIGENCE

Where a person is identified as either being a PEP, or a higher risk, additional due diligence is required in order to build a customer profile. This can be done through:

- Obtaining additional information on the customer (occupation, volume of assets, address, information available through public databases, internet, etc);
- Reducing interval for updating and reviewing customer risk profile; (annually)
- Reducing interval for updating the identification data of customer and beneficial owner;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the reasons for intended or performed transactions;
- (Obtaining additional information on the sources of funds or sources of wealth of the customer;
- (Obtaining the written approvals of senior management to continue the business relationship;
- Documentary evidence may be sought to support transaction where possible, e.g. purchase of property etc.

SOURCE OF INCOME

Proof of the origin of income is required for purposes of building a customer profile where a person is a PEP, or poses a high risk of facilitating money laundering activities or to enable the firm to identify any possible money laundering and information. The following documentation would constitute proof:

- Salary confirmation
- A donation agreement
- Income statement
- Balance sheet
- Bank statement

SOURCE OF FUNDS (REGULATION 21)

Proof of the source of funds being used in the transaction, is required for purposes of building a customer profile where a person is a PEP, or poses a high risk of facilitating money laundering activities Substantiating documentation includes:

- a copy of a will
- investment maturity letter
- balance sheet
- income statement

CHAPTER 11 RECORD KEEPING

Chapter 3 : Money laundering control measures Part 2 : Duty to keep records

23. Period for which records must be kept

1. An accountable institution must keep the records referred to in section 22 which relate to –
    a. the establishment of a business relationship, for at least five years from the date on which the business relationship is terminated;
    b. a transaction which is concluded, for at least five years from the date on which that transaction is concluded.

47. Failure to keep records

1. An accountable institution that fails to –
    a. keep record of information in terms of section 22(1); or
    b. keep such records in accordance with section 23 or section 24(1); or
    c. comply with the provisions of section 24(3), is guilty of an offence.

Chapter 4 : Compliance and Enforcement

48. Destroying or tampering with records

Any person who wilfully tampers with a record kept in terms of section 22 or section 24(1), or wilfully destroys such a record, otherwise than in accordance with section 23, is guilty of an offence.

A recordkeeping policy is a vital component of any records management programme. A policy provides the framework within which such a programme operates.

It affirms our Firm's commitment to ensure that authentic, reliable, and usable records are created, captured, and managed to a standard of best practice and to meet the our business and legislative requirements. It is also an effective means of communicating recordkeeping responsibilities and is itself a record of our attempt to meet requirements for accountability.

Documenting the AML program, and properly organizing and storing all records, is an integral part of the AML process. The verification process is considered basic due diligence, requiring a certain minimum of documentary evidence, with higher risk customers requiring more documentation.

Sufficient records must be kept relating to the AML programme. This includes the policy, procedures, processes, training interventions, compliance audits, breaches and controls, and any other pertinent information. A checklist of these records is to be kept and monitored quarterly

Testing and evaluating whether the program is effective, and whether the process is adequately being followed, is largely reliant on the documentary audit trail. Comprehensive and complete records are critical. Not only are Regulators holding institutions accountable for compliance breaches, but internal controls require evidence, therefore it is therefore critical that a full, verifiable record of compliance be available on audit.

Records must be kept of all transaction data and data obtained for the purpose of identification, as well as of all documents related to money laundering topics (e.g. files on suspicious activity reports, documentation of AML account monitoring, etc.).

ALL RECORDS MUST CONTAIN ENOUGH INFORMATION TO MAKE SENSE AND PROVIDE VERIFICATION OF THE MATTER AT HAND.

All records must be retained in accordance with the internal Recordkeeping Policy

Records may be kept in electronic form. Records may be kept by a third party on behalf of a firm as long as the firm has free and easy access to the records. If the third party fails to properly comply with the recordkeeping requirements, the firm will be held liable.

Where documents are obtained as part of the verification process, the name of the verifier as well as the date of verification must be evident on the documentation

CUSTOMER RECORDS

All records must be kept relating the customer or business partner. This means that all copies of documentation, including: identification verification, correspondence, application forms, quotes, receipts, e-mails as well as the further details required are to be kept in a secure and confidential environment.

CUSTOMER RECORD REQUIREMENTS

The following records MUST be accessible and on file, but confidential. Only authorized staff to have access.

1) The identity of the customer;
    a. if the customer is acting on behalf of another person –
        i. identity of the person on whose behalf he is acting; and
        ii. authority to act
    b. another person is acting on behalf of the customer –
        i. identity of that other person; and
        ii. authority to act
2) How the identity was established;
3) The nature of that business relationship or transaction;
    a. in the case of a transaction –
        i. amount involved; and
        ii. parties to the transaction;
4) All accounts that are involved in –
    a. transactions concluded in the course of the business relationship; and
    b. a single transaction;
5) The name of the person who obtained the information above, as well as the date; and
6) Any document or copy of a document obtained to verify a person's identity

RE-VERIFICATION OF INFORMATION

ALL EXISTING/ REPEAT CUSTOMERS ARE TO BE RE-VERIFIED AT LEAST ONCE EVERY 24 MONTHS FULL RECORDS OF THIS ARE TO BE KEPT.

It is our Firms policy to obtain updated verification on at least an annual basis to ensure that the records we have on file are correct and are a true reflection

DATA PROTECTION LEGISLATION

In addition to meeting our recordkeeping requirements, we have an obligation to protect our customer data. Confidential information may not be released and must be secured in terms of our data protection policy.

PROTECTING CUSTOMER DATA

Data integrity is an enterprise-wide activity that applies to all.
Every staff member shall protect electronically stored, accessed, or transmitted data. Processes are required that:

- Implement security protection mechanisms to protect data from unauthorized alteration or destruction.
- Monitor access to data to ensure that it has not been altered or destroyed due to unauthorized activity.
- Issue alerts if the data has been altered or destroyed in an unauthorized manner. Upon such alerts, implement corrective action procedures to ensure data is restored and implement controls to ensure data is protected and cannot be altered in an unauthorized manner in the future.

The processes and technologies must achieve a level of protection sufficient to ensure data integrity. These include:

- No person may leave customer information lying around where it can be accessed by unauthorized persons
- Ensure that data is properly filed in the correct place
- Deleting /shredding forms or notes with customer and/or transaction information properly when the retention period ends
- Locking customer records in a secure location with access control in respect of who can view
- Not disclosing any customer confidential information to any unauthorized person

PROCESS

Step 1:
Obtain all required records, verify, and ensure that the name of the employee dealing with the party as well as the name of the person obtaining and verifying the information and the date of verification is noted on the document

Step 2:
All documents and records relating to each customer (“customer information”), with whom a transaction was concluded must be maintained and kept in safe custody (protected against destruction)

Step 3:
All parties to a business relationship must confirm, in writing, all their details once every two years. Records must be updated within 3 days of receiving a change of details. All changes of detail must be accompanied by proof/ verification of the change The money laundering control officer is responsible for ensuring that records are kept in accordance with the firm’s data retention policy. Access to

customer information by employees must be monitored to ensure the correct authorizations. Hard copies of documentation may be held in a customer file or it may be held electronically

Step 4:
Each employee who removes customer information from safekeeping, must record the date, the data removed, and the reason for the removal on the central register. On return of the information, the same person must sign and date that all customer information was returned.

Step 5:
Records must be retained for a period of 5 years from the later of the date of conclusion of the transaction or date the relationship with the customer was terminated,

CHAPTER 12 REPORTING

For the purposes of this Act a person has knowledge of a fact if-
(a) the person has actual knowledge of that fact; or
(b) the court is satisfied that-
(i) the person believes that there is a reasonable possibility of the existence of that fact; and
(ii) the person fails to obtain information to confirm or refute the existence of that fact.

For the purposes of this Act a person ought reasonably to have known or suspected a fact if the conclusions that he or she ought to have reached, are those which would have been reached by a reasonably diligent and vigilant person having both-
(a) the general knowledge, skill, training and experience that may reasonably be expected of a person in his or her position; and
(b) the general knowledge, skill, training and experience that he or she in fact has Regulations Chapter

Reporting of suspicious and unusual transactions
Manner of reporting
1)Subject to subreg. (2), a report made under Part 3 of Chapter 3 of the Act must be made in accordance with format specified by the Centre, and sent to the Centre electronically by means of -
a) the internet-based reporting portal provided by the Centre for this purpose at the following internet address: http://www.fic.gov.za. or
b) a method developed by the Centre for this purpose and made available to a person wishing to make such reports
2)If a person wishing to make a report under Part 3 of Chapter 3 of the Act –
a) does not have the technical capability to make a report in accordance with the subreg. (1), or
b) is for another reason definitely unable to make a report in accordance with subregulation (1), that person shall make the report on a form specified by the Centre from time to time for this purpose and provide it to the Centre at the contact particulars specified by the Centre from time to time for this purpose.

FICA Chapter 4 : Compliance and Enforcement

51. Failure to report cash transactions
An accountable institution or reporting institution that fails, within the prescribed period, to report to the Centre the prescribed information in respect of a cash transaction in accordance with section 28, is guilty of an offence

51A. Failure to report property associated with terrorist and related activities
1)An accountable institution that has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of an entity contemplated in section 28A(1), and that fails, within the prescribed period, to report that fact and the prescribed information in respect of such property to the Centre in accordance with that section, is guilty of an offence.

52. Failure to report suspicious or unusual transactions
1)Any person who fails, within the prescribed period, to report to the Centre the prescribed

information in respect of a suspicious or unusual transaction or series of transactions or enquiry in accordance with section 29(1) or (2), is guilty of an offence.
2)Any person referred to in section 29(1) or (2) who reasonably ought to have known or suspected that any of the facts referred to in section 29(1)(a), (b) or (c) or section 29(2) exists, and who negligently fails to report the prescribed information in respect of a suspicious or unusual transaction or series of transactions or enquiry, is guilty of an offence.

53. Unauthorised disclosure
1)Any person referred to in section 29(3) who discloses a fact or information contemplated in that section, otherwise than in the circumstances or for the purposes authorised in that section, is guilty of an offence.
2)Any person referred to in section 29(4) who discloses a knowledge or suspicion or any information contemplated in that section, otherwise than in the circumstances and for the purposes authorised in that section, is guilty of an offence.

54. Failure to report conveyance of cash or bearer negotiable instrument into or out of Republic Any person, who wilfully fails to report the conveyance of cash or a bearer negotiable instrument into or out of the Republic in accordance with section 30(1), is guilty of an offence.
2)An accountable institution that fails to comply with a direction by the Director in accordance with section 28A(2), is guilty of an offence.

55. Failure to send report to Centre
A person referred to in section 30(2) who fails to send a report regarding the conveyance of cash or a bearer negotiable instrument to the Centre in accordance with that section, is guilty of an offence.

56. Failure to report electronic transfers
An accountable institution that fails to report to the Centre the prescribed information in respect of an electronic transfer of money in accordance with section 31, is guilty of an offence.

68. Penalties
1)A person convicted of an offence mentioned in this Chapter, other than an offence mentioned in subsection (2), is liable to imprisonment for a period not exceeding 15 years or to a fine not exceeding R100 million.
2)A person convicted of an offence mentioned in section 55, 61 62, 62A, 62B, 62C or 62D, is liable to imprisonment for a period not exceeding five years or to a fine not exceeding R10 million

IT IS EVERY INDIVIDUAL EMPLOYEE'S DUTY TO REPORT
Each employee must immediately report a transaction to the reporting officer – Money Laundering Control officer (MLCO) where the following is identified:

- any cash transaction over the published threshold R24 999. (even if the transaction was split into two or more, and the total exceeds this amount)
- any unusual or suspicious transaction; or
- when it was impossible for the employee to comply with the requirements in terms of FICA for whatever reason; or
- whenever in doubt as to whether to report to the reporting officer or not.

- Where any funds are suspected of being used for the financing of terrorist or related activities

EMPLOYEE REPORTING PROCESS

Where a suspicious or unusual or other transaction has been reported, you must continue with the transaction unless the MLCO or the FIC direct you otherwise, OR unless your customer is on a sanctions list.

DO NOT ALERT YOUR CUSTOMER TO THE FACT THAT THEY ARE BEING REPORTED OR DISCUSS THE REPORTING WITH ANYONE OTHER THAN THE MLCO!!!!

Employee Reporting Process

IMPORTANT - Confidentiality must be maintained!!

MLCO REPORTING PROCESS

The responsibility to report a transaction in terms of FICA to the Financial Intelligence Centre will transfer from the employee to the reporting officer (MLCO) after a transaction was reported to the reporting officer. The reporting officer will determine and decide as to whether a transaction must be reported.

STEP 1:

On receipt of the report, an acknowledgment must be provided to the member of staff who made the report, to confirm receipt of the report and to confirm that their obligations have now been fulfilled.

STEP 2:

The report will be added to the Money Laundering Disclosure Register. The customer's file will be copied so that it can be analysed and evaluated for evidence to support the reported suspicions

STEP 3:

A detailed report will be written and will state whether there is evidence to support the suspicions/ reporting obligation. This will include whether the report will be disclosed to the Financial Intelligence Centre (FIC) and give the rationale for the decision, or if there is insufficient reason to suspect money laundering, the record will state the reason for not reporting.

STEP 4:

If reportable activities are found, then FIC will be notified by following the process below. (www.FIC.gov.za) Accountable Institutions and Reporting Institutions are required to use the new Suspicious Transaction Report (STR) and Terrorist Property Report (TPR) forms, available on the FIC website, when filing these reports to the Centre If reportable activities are not found then the customer AML file will be closed and filed in a lockable cabinet.

The Money Laundering Disclosure Register will then be updated to reflect the action taken.

- Reporting deadlines: threshold transactions: within 2 days
- property associated with terrorism: within 5 days
- suspicious or unusual transactions: within 15 days

ONLINE REPORTING PROCESS

Step 1:

Go to the FIC website www.fic.gov.za and provide your log-on details

Step 2:

Report the transaction. The report must contain the following information:

- Full particulars in respect of the natural or legal person making the report or other entity on whose behalf the report is made. This will include:
    - Identifying particulars of the person or entity. Example ID or registration number of entity;
    - address of the person or entity;
    - the type of business or economic sector of the accountable institution and reporting institution;
    - In the case of a natural person, the person's contact particulars, and in the case of a legal person or entity, the surname, initials and contact particulars of a contact person

Step 3:

In respect of the transaction for which a report under section 28 is made, the report must contain as much of the following information as is available:

- the date and time of the transaction, or in the case of a series of transactions, the time of the transactions in the 24 hour period;
- the description of the transaction or series of transactions;
- the amount of the funds per transaction or series of transactions;
- the currency in which the funds were disposed of; and
- the purpose of the transaction or series of transactions;

Step 4:

In respect of each person conducting the transaction the report must contain as much of the following information available-

- in the case of a natural person, full particulars of the person's name and surname, or initials and surname if the name is not available;
- the date of birth of the person or identification number;
- the type of identifying document from which the particulars referred to subparagraphs above were obtained;
- in the case of a legal person, full particulars of the person's or entity's name including their registration number

A report in terms of section 28 must contain a full description of the amount of cash in excess of the prescribed limit which is received or paid out by the accountable institution and reporting institution

THRESHOLD AND CASH REPORTING (SECTION 28)

Chapter 3 : Money laundering control measures Part 3 : Reporting duties and access to information 28.

Cash transactions above prescribed limit

1) An accountable institution and a reporting institution must, within the prescribed period, report to the Centre the prescribed particulars concerning a transaction concluded with a customer if in terms of the transaction an amount of cash in excess of the prescribed amount –
    a. is paid by the accountable institution or reporting institution to the customer, or to a person acting on behalf of the customer , or to a person on whose behalf the customer is acting; or
    b. is received by the accountable institution or reporting institution from the customer, or from a person acting on behalf of the customer , or from a person on whose behalf the customer is acting.

These transactions must be reported, in the prescribed format, to the Financial Intelligence Centre, within 2 days of being made aware of the transaction

SUSPICIOUS OR UNUSUAL TRANSACTIONS (SECTION 29)

Chapter 3 : Money laundering control measures Part 3 : Reporting duties and access to information

29. Suspicious and unusual transactions

1) A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that –
    i. the business has received or is about to receive the proceeds of unlawful activities;
    ii. a transaction or series of transactions to which the business is a party –
        1. facilitated or is likely to facilitate the transfer of the proceeds of unlawful activities;
        2. has no apparent business or lawful purpose;
        3. is conducted for the purpose of avoiding giving rise to a reporting duty under this Act; or
        4. may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Service; or
    iii. the business has been used or is about to be used in any way for money laundering purposes, must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.
2) A person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or suspects that a transaction or a series of transactions about which enquiries are made, may, if that transaction or those transactions had been concluded, have caused any of the consequences referred to in subsection (1)(a), (b) or (c), must, within the prescribed period after the knowledge was acquired or the suspicion arose, report to the Centre the grounds for the knowledge or suspicion and the prescribed particulars concerning the transaction or series of transactions.

3) No person who made or must make a report in terms of this section may disclose that fact or any information regarding the contents of any such report to any other person, including the person in respect of whom the report is or must be made, otherwise than –
    i. within the scope of the powers and duties of that person in terms of any legislation;
    ii. for the purpose of carrying out the provisions of this Act;
    iii. for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
    iv. in terms of an order of court.
4) No person who knows or suspects that a report has been or is to be made in terms of this section may disclose that knowledge or suspicion or any information regarding the contents or suspected contents of any such report to any other person, including the person in respect of whom the report is or is to be made, otherwise than –
    i. within the scope of that person's powers and duties in terms of any legislation;
    ii. for the purpose of carrying out the provisions of this Act;
    iii. for the purpose of legal proceedings, including any proceedings before a judge in chambers; or
    iv. in terms of an order of court.

All suspicious and/or unusual transactions are to be reported irrespective of the size of the transaction or whether it is a cash transaction or not;

The following are examples of suspicious or unusual activities:

- a deposit is made into the business account, and the firm is contacted for a refund due to “a mistaken deposit”
- a customer asks an employee how to avoid a reporting requirement.
- A customer threatens or bribes an employee to avoid providing information or having a report filed.
- a customer uses an apparently fake identification, or more than one customer tries to
- use the same identification.
- a customer refuses to proceed with a transaction when asked for identification.
- a customer refuses to provide all of the information required or seems excessively
- nervous or anxious.
- a customer (or group of customers working together) transacts in amounts just below the recordkeeping thresholds or to avoid reporting.
- a customer conducts transaction that are unusually large based on their past history,
- employment or level of income.
- a customer wishes to have correspondence/ documents sent to destinations other than his or her address;
- a customer is reluctant to provide complete information regarding his activities;
- financial statements differ noticeably from those of similar businesses;
- a business customer’s representatives avoid contact with the firm;
- a customer’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 customer maintains a number of trustee accounts or customer subaccounts;
- a customer makes a large volume of cash transactions from a business that is not normally cash intensive;
- a customer's accounts show a sudden and inconsistent change in transactions or patterns.
- where the person knows or suspects that the firm is about to or has received the proceeds of any unlawful activity.
- where the money is received for no apparent business or lawful purpose.
- where the business is conducted in a manner so as to avoid a reporting duty in terms of these rules.
- where the funds received may be as a result of any tax evasion or attempted evasion
- transactions outside the customer's normal pattern of business
- an unusual delay in the provision of information to enable verification to be completed.
- any transaction that is unnecessarily complex
- any transaction involving an undisclosed party
- early termination of a product, especially at a loss or where cash was tendered or the refund cheque is to a third party.
- a transfer of a benefit of a product to a third party
- an applicant for business shows no concern for the performance of a product but much concern for the cancellation / refund of the product.
- a customer attempts to use cash in a transaction where the customer has typically used cheques or other methods of payment.
- A person asks to make payment with foreign currency or by wire transfer from another country
- the customer provides fictitious information.
- the customer purchases products beyond his apparent means.
- the customer purchases a large policy / product and within a short time cancels / repurchases and requests the cash value returned in cash or payable to a third party.
- the customer uses a mailing address in another jurisdiction and the telephone has been disconnected when phoned for verification.
- any employees, agents or brokers who suddenly show a lavish lifestyle; an unexpected and dramatic increase sales; exceed a high level of single premium business or use their own business address as the delivery address for a customer's documentation.

The examples referred to above may be legitimate features of certain categories of businesses or may make business sense if viewed in the context of the customer'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 customer's business activities.

PROPERTY ASSOCIATED WITH TERRORISM (SECTION 28A OF THE FIC ACT)

Section 28A requires an accountable institution, listed in Schedule 1 to the FIC Act, to file a report with the Centre if the accountable institution knows that it possesses, or controls property linked to

terrorism or to entities that are sanctioned pursuant to the provisions of the Protection of Constitutional Democracy against Terrorism and Related Activities Act, 2004 (Act 33 of 2004) (the POCDATARA Act). The knowledge about the origin and ownership of the property in question is based on fact and should be acquired with reference to an objective set of circumstances or facts (as opposed to a suspicion that is formed subjectively).

The FIC Act and its Regulations do not require an accountable institution to determine whether it controls relevant property. It furthermore does not compel an accountable institution to investigate or search for links with terrorist property or names of suspected terrorists in its customer database however an accountable institution that does not have such measures in place could be found guilty of an offence associated or connected with the financing of specified offences in terms of section 4 of the POCDATARA Act.

Section 28A(1)(a) of the FIC Act states the following:
(1) An accountable institution which has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of –
(a) any entity which has committed, or attempted to commit, or facilitated the commission of a specified offence as defined in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; or
(b) … must within the prescribed period report that fact and the prescribed particulars to the Centre.

An accountable institution that files a report in terms of section 28A(1)(a) of the FIC Act knows that it is in possession of, or controls property linked to a specified offence as defined in the POCDATARA Act.
Section 28A(1)(b) of the FIC Act states the following:
(1) An accountable institution which has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of –
(a)…
(b) a specific entity identified in a notice issued by the President, under section 25 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004, must within the prescribed period report that fact and the prescribed particulars to the Centre.

DEFINITION OF TERRORISM:
In the international community, terrorism has no legally binding, criminal law definition. Common definitions of terrorism refer only to those violent acts that are intended to create fear (terror); are perpetrated for a religious, political, or ideological goal; and deliberately target or disregard the safety of non-combatants (e.g., neutral military personnel or civilians). Some definitions now include acts of unlawful violence and war.

The use of similar tactics by criminal organizations for protection rackets or to enforce a code of silence is usually not labelled terrorism, though these same actions may be labelled terrorism when done by a politically motivated group.

1. Where an employee becomes aware of the property of a customer which can be associated with terrorism and any related activities, the employee must report to the MLCO within 1 day.

2. The reporting officer must report to the FIC WITHIN 5 DAYS of the business becoming aware of this
3. A report filed in terms of section 28A of the FIC Act is based on the knowledge a firm has that it has property related to the financing of terrorism in its possession or under its control.

Once the firm files a report in terms of section 28A of the FIC Act, this will lead to a requirement to freeze the property and cease to conduct business with the entity in question.

When filing a report with the Centre in terms of section 28A of the FIC Act it is an offence (by virtue of section 4 of the POCDATARA Act) to continue dealing with that property in any way, whereas if a person files a report with the Centre in terms of section 29 of the FIC Act (suspicious or unusual transaction) they may elect to continue with the transaction as provided for in section 33 of the FIC Act. The defence contained in section 17(6)(b) of the POCDATARA Act can be applied

Example: In the event of an Al Qaida member attempting to withdraw money to purchase a motor vehicle from a dealership, the transaction may not be suspicious for purposes of section 29 of the FIC Act, but the institution would need to report that they are in control of the assets of a person on the UNSC 1267 list (in terms of section 28A of the FIC Act)

REPORTING CONFIDENTIALITY

Any person who is required to make a report in terms of these rules may not disclose the fact that a report is being made or the contents of that report to any person other than the employee who is responsible for making the report to the FIC.

The customer may not, under any circumstance be informed that a report is going to be made or that money laundering is suspected.

No person who is aware that a report is to be made may disclose that fact or any information contained in the report to any other person.

Any person who suspects that a report is to be made or has been made in not to disclose that fact.

If you make a report in good faith, no criminal or civil action may be taken against you for reporting.

CHAPTER 13 DISCIPLINARY PROCEDURES

Each person will be liable to disciplinary action in the event of non-compliance with any anti-money laundering legislation (including FICA), these Internal Policy and Procedures and all other policies issued by the firm in respect of AML.

Any contravention of the rules contained in this AML programme will be dealt with in accordance with the disciplinary procedures of the Firm.

A person convicted of any offence under any AML Act will be summarily dismissed.

CHAPTER 14 CONTROLS

Business managers, as the first line of defense, are responsible for understanding and assessing key risks and effective implementation and the ongoing operation of internal controls.

Compliance, is the second line of defense, provides independent verification of the adherence to AML laws and requirements. The objective of an independent compliance framework is to ensure a consistent approach to periodically assessing the AML control environment and ensure it is sufficient.

The controls require the Firm to assess and document their AML/CFT and fraud prevention programme against each core requirement and rate its level of compliance, in order to address any shortcomings.

ANNUAL CONTROLS

- Review the appointment of the anti-money laundering control officer
- Confirm registration at FIC
- Ensure internal anti money laundering policies and processes are correct and up to date
- Ensure the governing authority has adopted the AML programme in writing annually
- Review customer acceptance procedures
- Review risk rate process and complete MLCO report
- Review products in order to identify to what AML applies
- Have all FICA processes been followed – review monitoring
- Review training records
- Review recordkeeping

MONTHLY CONTROLS

- Check that FICA processes are being followed and records monitored

FICA – RISK RATE DOCUMENT (DEALERSHIPS)
ANNEXURE A

Customer :…….. Date: ……

Verifier:……

Politically Exposed persons (PEP's) Yes No

Is the customer one of the following, or a close family member or closely associated with one of the following?

1) Heads of state, heads of Government and cabinet ministers
2) Influential functionaries in nationalised industries and Government
3) Senior judges
4) Senior political party functionaries
5) Senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organisations
6) Members of ruling or royal families
7) Senior and/or influential representatives of religious organisations (if these functions are connected to political, judicial, military or administrative responsibilities)

If any questions were answered "Yes", the source of funds and more information about the transaction and the customer should be obtained.

This includes verifying:
Source of funds:.....
verified doc:……

Source of income:.....
verified doc: ……

Risk rating: The following factors should be taken into account when risk rating a customer and should be implemented at each instance where FICA applies

Aspect: low Med high
Cash or EFT/ Bank cheque/ Financing (cash is high risk)
Natural Person (low) or business (medium)

Is the customer on the United Nations list (a known terrorist) check list!!

Does the customer easily produce identification documents

Local person (low risk) and foreign national (high risk)

Value less than R24 000 (low risk)

Fixed employment and address (low risk) or not (high risk)

_____ _____
Manager's Signature Date

INTERNAL MONEY LAUNDERING REPORT FORM
ANNEXURE B

Customer Name: ……
Customer Ref No……..
Customer Address:……
……
……

Reasons Why You Are Suspicious:
(Please give full details)
……
……
……

Transaction:
……

Reported by: ……
Date: ……

Once this form is complete please take it (sealed) to the Money Laundering Control Officer (MLCO) and ensure you receive a signed receipt.

NB. REMEMBER DO NOT DISCUSS THE CONTENT OF THIS REPORT WITH ANYONE OTHER THAN THE MLCO
……

RECEIPT:
MONEY LAUNDERING REPORT RECEIVED BY:……
ON…./……/……. REF:……..
FROM:……
SIGNED: ……..

APPOINTMENT OF COUNTER-MONEY LAUNDERING OFFICER
ANNEXURE C

I ……, hereby accept my appointment as Counter-money Laundering Officer of …….
I confirm that I have the seniority, independence and knowledge to properly perform my function

I agree that I will:

1. Ensure compliance with money laundering control obligations as set out in applicable Counter Money Laundering legislation, any amendments made from time to time and the Regulations and Guidance Notes
2. Register with the FIC and ensure all details are at all times kept current and correct with the FIC
3. Ensure I remain trained and competent in terms of AML requirements
4. Accept and acknowledge reports regarding reportable transactions made by employees within two working days.
5. Examine the report in order to establish that:
    a. there are sufficient grounds to classify the transactions as threshold, suspicious or unusual in terms of FICA
    b. there are sufficient grounds to believe that the property is associated with terrorism or related actions
    c. accompanied by the relevant documentation
6. Make the report to the FIC centre once verified and found reportable
7. Deal with the report in confidence.
8. Report all transaction above the prescribed limit to the FIC Centre
9. Attach a certified copy of my Identity Document

_____ _____
SIGNATURE DATE

MLCO ANNUAL REPORT
PRODUCTS, SERVICES, DELIVERY CHANNELS AND GEOGRAPHIC LOCATIONS
ANNEXURE D

If the Firm answers “yes” to any of the questions below, we should consider it as higher-risk for money laundering or terrorist financing.

Where appropriate, risk mitigation steps should be taken.
Identify whether the Firm provides any of the following products, services or delivery channels

- Do we offer services that make it difficult to fully ascertain the identity of customer s?
- Do we offer electronic funds payment services?
- Do we offer electronic cash (for example stored value and payroll cards)?
- Do we offer Funds transfers (domestic and international)?
- Do we offer any of the following:
    - Services involving banknote and precious metal trading and delivery?
    - Cash transactions of high value?
    - Foreign correspondent accounts?
    - Non face-to-face transactions, such as Internet services, by mail or by telephone?
- Does our firm deal with customer s or provide products or services in the following geographic location
    - Any country subject to sanctions, embargoes or similar measures issued by, for example, the UnitedNations (UN)? In some circumstances, this will include sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized.
    - Any country identified as a financial secrecy haven or jurisdiction?
    - Any country identified by the Financial Action Task Force (FATF) as a high-risk jurisdiction or subject to a FATF statement? Consult the current high-risk jurisdictions listed on the FATF website at http://www.fatf-gafi.org (select the tabs labelled "Jurisdictions for which an FATF call for action applies" and "Other monitored jurisdictions").
    - Any country identified by credible sources:
        - as lacking appropriate money laundering or terrorist financing laws and regulation
        - as providing funding or support for terrorist activities
        - as having significant levels of corruption, or other criminal activity?

Credible sources means information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly available. Such sources may include,

but are not limited to, international bodies such as the World Bank, the International Monetary Fund, the Organisation for Economic Co-operation and Development, and Transparency International as well as relevant national government bodies and non-governmental organizations.

CUSTOMER S WITHIN AND CUSTOMER S OUTSIDE OF BUSINESS RELATIONSHIPS

If the Firm answers yes to any of the questions below, it should considered as higher-risk for money laundering or terrorist financing. Where appropriate, risk mitigation steps should be taken.

Identify whether any of the following apply to customers (whether within or outside of business relationships):

- Is the customer a cash intensive business?
- ı Does the customer's business generate large amounts of cash for certain transactions that are not normally cash intensive?
- Is the customer an intermediary or "gatekeeper" such as a professional that holds accounts for customer s where the identity of the underlying customer is not disclosed to you?
- Does the customer use unsupervised intermediaries within the relationship who are not subject to adequate anti-money laundering or anti-terrorist financing obligations?
- Does customer identification take place other than face-to-face?
- Does the customer reside outside South Africa?
- Does the customer deal offshore?
- Is the customer an unregistered charity or other unregulated "not for profit" organization (especially one operating on a "cross-border" basis)?
- Does the comparison between our customers with similar profiles and high levels of assets or large transactions seem unreasonable?
- Does the knowledge of local laws, regulations and rules seem excessive for our customer?
- Is the customer a new customer?
- Do our customers use intermediate vehicles (such as corporations, trusts, foundations, partnerships) or other structures that seem unusual for their business or seem very complex and unnecessary
- Does the customer offer online gaming?
- Does the customer 's structure or nature of its business or relationship make it difficult to ascertain the identity of the true owners or controllers?
- Are we unable to obtain beneficial ownership information for our customer (if our customer is a corporation, trust or other entity)?
- Is there a significant and unexplained geographic distance between us and the customer?
- Is the customer a politically exposed foreign person?

To be completed at least annually in order to risk rate the business in terms of money laundering risk