GUIDELINES ON

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

FOR

FINANCIAL INSTITUTIONS AND NON FINANCIAL BUSINESSES & PROFESSIONS

TABLE OF CONTENTS

PREFACE

I. Short title

This Guideline may be cited as **Guideline No. 01-2006 BUP/SML: Anti-Money Laundering.**

II. Authorisation

The Guideline is issued in terms of Bank Use Promotion and Suppression Money Laundering Act [Chapter 24:24].

III. Application

This Guideline applies to all Financial and Non Financial institutions. Wherever the term "bank(s)" or "institution(s)" is used in the Guideline, it shall also be read to include non-bank banking institutions that are designated and monitored under various pieces of legislation within Zimbabwe including Holding Companies.

IV. Reporting

All reports and any enquiries of suspicious transactions whether in relation to money laundering or terrorist financing should be made to:

The Division Chief
Reserve Bank of Zimbabwe
Financial Intelligence, Inspectorate and Evaluation Unit
80 Samora Machel Avenue
HARARE

Email: mchiremba@rbz.co.zw. This could be copied to the Head of Anti-money Laundering on e-mail; jnyamuchanja@rbz.co.zw

V. DEFINITIONS

The following terms used in this Guideline shall be taken to have the meaning assigned to them hereunder:

Financial institutions mean

a) any banking institution registered or required to be registered in terms of the Banking Act Chapter 24
b) any building Society registered or required to be registered in terms of the Building societies Act Chapter 24.02
c) The People's Own Savings Bank established in terms of the People's Own Saving Bank of Zimbabwe Act Chapter 24.22
d) The Reserve Bank

Non-financial businesses and professions means:

a. Casinos (which also includes internet casinos).
b. Real estate agents.
c. Dealers in precious metals.
d. Dealers in precious stones.
e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f. Trust Companies

Institution refers to Non-financial businesses, professions and Financial Institutions

Money laundering is an activity which has or likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.

Cash dealers refers to any institution involved in bulk dealing in cash and these include money transfers agencies, bureau de change, etc

Reserve Bank" refers to the Reserve Bank of Zimbabwe established in terms of the Reserve Bank of Zimbabwe Act [Chapter 22:15].

1.0 EXECUTIVE SUMMARY

1.1. The Anti-Money Laundering Guideline issued by the Financial Intelligence, Inspectorate and Evaluation Unit provide a framework within which most activities to combat the undesirable phenomenon of money laundering by designated institutions and individuals can be executed.

1.2. The different forms and stages of money laundering are characterized by such dynamism which calls upon the issuing authority to continuously review them in liaison with all stakeholders.

1.3. The guidelines define money laundering as an activity which has or likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.

1.4. However, it must be pointed out that, these guidelines are the minimum requirements and management is expected to keep itself abreast with the anti-money laundering developments.

2.0 INTRODUCTION

2.1. The Republic of Zimbabwe as a member of **Eastern, Southern African Anti-Money Laundering Group (ESAAMLG)** is committed to the fight against money laundering and the financing of terrorism and is currently working on its legislation and relevant structures to meet regional and international requirements.

2.2. To demonstrate its firm willingness to combat money laundering and terrorist financing, Zimbabwe has so far put in place the following pieces of legislation.

2.3. These include;

2.3.1. Serious Offences (Confiscation of Profits) Act (Chapter11:90)

2.3.2. Prevention of Corruption Act; (Chapter 9:16)

2.3.3. Criminal Matters (Mutual Assistance Act); (Chapter 9:12)

2.3.4. Public Order and Security Act; (Chapter 11:17)

2.3.5. Bank Use Promotion and Suppression of Money Laundering Act; and

2.3.6. Anti-Corruption and Anti-Monopolies.

2.4. Zimbabwe through its Central Bank, the Reserve Bank of Zimbabwe, had however been proactive as far back as the year 2002, when Anti-Money Laundering Guidelines were developed and distributed in November of the same year, to financial institutions.

2.5. The commercial banks, merchant banks, building societies have been reporting suspicious transactions (STRs) since 2001 and were formally designated following the Bank Use Promotion and Suppression of Money Laundering Act of April 2004.

2.6. Other deposit taking entities including Law Firms, Accounting Firms, Insurance companies, Asset management companies, casinos, have also been designated.

2.7. Thus each institution appoints a Money Laundering or Suspicious Transactions Reporting Officer, informs Reserve Bank of contact details of respective officer(s) through the F.I.I.E. Unit, which checks on compliance with procedures and reporting standards.

2.8. In order to give full attention to the issue of money laundering and financing of terrorism in line with the international trends, Zimbabwe promulgated the Bank Use Promotion and Suppression of Money Laundering Act (Chapter 24:24) of April 2004 which led to the establishment of F.I.I.E. Unit within the Reserve Bank of Zimbabwe, which receives reports of suspicious transactions.

2.9. Part IV of the Act which is the Suppression of Money laundering. This Unit in other jurisdictions is referred to as a Financial Intelligence Unit or centre.

2.10. The Act promotes the use by the public of Financial Institutions which will make it easier to detect laundered proceeds. The Act also gives powers to the Director to issue directives to financial institutions relating to bank use.

2.11. Furthermore, the Act encourages Banking Institutions to know their customers (KYC). Under this Act, no person is allowed to hoard hard currency. Banking institutions are mandated to report suspicious monetary transactions to the Unit.

2.12. Financial and non-financial institutions and corporates that accept cash deposits from the public are obliged to establish and maintain customer records.

2.13. The establishment of the Unit focused on dealing with the various challenges facing the Zimbabwean economy which included local cash and foreign currency shortages, parallel market activities, under invoicing of exports, over invoicing of imports and out right externalization of foreign currency.

2.14. These activities threaten to derail national efforts aimed at economic revival and constitute potential ground for money laundering activities.

2.15. With regard to terrorism, the Government is yet to ratify the following United Nations Conventions,

2.15.1. The Convention of the Suppression of Unlawful Seizure of Aircraft;

2.15.2. The Convention for the Suppression of financing of International Terrorism (1999);

2.15.3. The Convention on Offences and Certain Other Acts committed on board an aircraft; and,

2.15.4. The Protocol for the Suppression of Unlawful acts of Violence at Airports Serving International Civil Aviation is supplementary to the convention for the Suppression of Unlawful Act against the Safety of Civil Aviation of 1971.

2.16. Currently the prosecution of financing of terrorism is conducted using the Public Order and Security Act which provides for the criminalization of terrorist activities, including those who harbor, assist or fail to report the presence of terrorists in Zimbabwe.

3.0 PURPOSE AND STATUS OF THE GUIDANCE NOTES

3.1. These guidelines on Anti-Money Laundering and combating the Financing of Terrorism are ;

(a) Issued to financial institutions and non-financial institutions by the Reserve Bank of Zimbabwe by virtue of powers conferred it by sections 24 and 26 of the Bank Use Promotion and Suppression of Money Laundering Act.
(b) They should be in continuance of the existing guidelines which shall be replaced by these new guidelines.

© These new guidelines will come into force on **1st April 2006** and will be binding on financial and non-financial institutions.

3.2. The guidelines outline the requirements, appropriate to the Bank Use Promotion and Suppression of Money Laundering Act of April 2004.

3.3. For the purposes of these guidelines financial and non-financial institution have the same meaning as in the Bank Use Promotion and Suppression of Money Laundering Act.

3.4. These guidelines are a statement of the minimum standards expected of all financial and non-financial institutions.

3.5. The Reserve Bank of Zimbabwe in the exercise of its supervisory duties will monitor adherence to these guidelines and failure to measure up to the standards contained in these guidelines will be dealt with in line with the appropriate penalties.

3.6. It is a criminal offence for financial institutions and non-financial institutions to fail to take measures as contained in the guidelines to prevent their institutions or the services their institutions offer from being used to commit or to facilitate the process of money laundering.

3.7. It is recognized that for the guidelines to be effective they need to be reviewed on a regular basis to reflect changing circumstances in the environment. Revisions and updates will be communicated to all the stakeholders (financial and non-financial institutions as and when necessary).

4.0 MONEY LAUNDERING

4.1. Various definitions on anti-money laundering

4.1.1. Money Laundering is about concealing the proceeds of crime.

4.1.2. The anti-money laundering act defines ***money laundering*** as an activity which has or likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.

4.1.3. **Money laundering** is also defined as a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities.

(a) If undertaken successfully, it allows them to maintain control over those proceeds and ultimately provides them with a legitimate cover for their source of income.

(b) Money launderers exploit weaknesses in legislative and institutional frameworks both domestic and international.

(c) They take advantage of unregulated and unsupervised sectors to white wash their ill-gotten gains. They make sure that their proceeds of crime escape the scrutiny of law enforcement agencies.

(d) One way they clean dirty money is to moving it around the world's financial systems.

4.2. The Need To Combat Money Laundering

4.2.1. Money laundering has adverse effects, both in economic and social terms. If left unchecked can erode a nation's economy in the following ways;

(a) changing the demand for cash;

(b) making interest rates and exchange rates more volatile; and,

(c) could be a cause of high inflation where criminal elements are conducting business.

4.2.2. Money laundering does not only undermine savings, but also deters foreign investment and make a country vulnerable to financial crisis and macro- economic instability.

4.2.3. Money laundering and financing of terrorism are global problems that affect not only security, but also potentially cause economic distortions. A weak financial system which is vulnerable to money laundering hampers the financial intermediation process and dampens the savings rates and investments in an economy.

4.2.4. An underground economic system distorts the allocation of funds in the economy and leads to lower than potential growth. Besides tax revenues are also affected. The tax base is eroded and honest tax payers have to bear the burden.

4.2.5. It undermines the integrity of a country's financial institutions, financial markets and also international financial systems. This is so because, financial institutions work on the basis of trust, integrity and honest.

4.2.6. In the absence of elements of integrity and high standards, financial markets lose credibility in the eyes of both the investors and consumers.

4.2.7. Laundered money especially in an offshore financial centre can harm the country's *reputation* and *balance of payment*.

4.2.8. The most disturbing of all is that money laundering can have social and political consequences. Money laundering facilitates corruption in society. Growth of crime undermines national economies and the democratic system.

4.2.9. The social fabric of society is eroded. The overall corrupt and unethical environment diminishes productivity and work effort. The country can run into turmoil as public confidence in the legal systems and in the country's governance structures are eroded.

4.3. Stages Of Money Laundering

4.3.1. The money laundering process is accomplished in three stages namely placement, layering and integration.

a) **Placement**
Occurs when funds derived from illicit activities are placed into the financial system, for example deposited into a bank account

b) **Layering**
These funds once deposited are moved from, one account or company to another and through various geographical jurisdictions. In this stage criminals try to create confusion by destroying the original source of the funds.

c) **Integration**
This is the final stage where the illicit funds are brought back to use as clean and often taxable income

4.3.2. The three steps occur as separate and distinct phases. They may also occur simultaneously or more commonly they may overlap. How these basic steps are used, entirely depends on the available laundering mechanisms and the requirements of the criminals.

4.3.3. Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid and where his/her activities are more susceptible to being recognized specifically.

These are:
(a) Entry of cash into the financial system, and

(b) Transfers within and from the financial system.

4.4. Categories Of Money Laundering

4.4.1. Concealment Within Business Structures

4.4.2. Misuse of Legitimate Business

4.4.3. Use of False Identities, Documents.

4.4.4. Use of Anonymous Asset Types.

4.5. Money Laundering Exposes Financial Sector Business

4.5.1. Historically efforts to combat money laundering have to a large extent concentrated on the deposit taking procedures of financial sector business where the launderers' activities are more susceptible to recognition. Zimbabwe of late has witnessed an anomalous high-speed growth of the financial sector.

4.5.2. Exchange Controls have deterred the large-scale abuse of the financial system by international launderers.

4.5.3. However, Zimbabwean criminals have over the recent years recognized that cash payments made into the financial sector business can often give rise to additional enquiries and have now sought different ways to convert their ill-gotten gains or to mix it with legitimate cash earnings before it enters the financial system, thus making it difficult if not harder to detect at the placement stage.

4.5.4. These include the issue of smart cards and wire transfers which are not easily amenable to tracking.

4.5.5. Financial and non financial institutions business and professions, as providers of a wide range of money transmission mechanisms, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.

4.5.6. Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names.

4.5.7. Some banks and cash dealers will additionally be susceptible to the attention of the more sophisticated **criminal organizations** and **professional money launderers**.

4.5.8. Such organizations, possibly under the disguise of front companies and nominees, will create large scale but false international trading activities in order to move their illicit monies from one country to another.

4.5.9. They will create the illusion of international trade using falsely inflated invoices to generate apparently legitimate international wire transfers, and will use falsified bogus letters of credit to confuse the trail further.

4.5.10. Many of the front companies may even approach their bankers for credit in order to fund the business activity. Banks and cash dealers offering international trade services should be on their guard for laundering by these means.

5.0 TERRORIST FINANCING

5.1. The main pieces of legislation relating to terrorist financing are Public Order and Security Act Bill on Suppression of Financing of International Terrorism currently gazetted.

6.0 ENHANCING EXISTING DUE DILIGENCE REQUIREMENTS

6.1. Terrorist activities and the means that are used to further those activities require financing and wittingly or unwittingly the services of banks and cash dealers may be used to hide or move terrorist funds.

6.2. While financial gain is generally the objective of other types of criminal activities. The goal of terrorism may be different for example aims at finding resources then supply to the required entity.

6.3. A successful terrorist group like any criminal organization is therefore necessarily one that is able to build and maintain an effective financial infrastructure.

6.4. For this it must develop sources of funding, a means of laundering those funds and then finally a way of ensuring that the funds can be used to obtain material and other logistical items needed to commit terrorist acts.

6.5. Banks and cash dealers should therefore protect themselves from being used as a conduit for such activities and make use of their already existing due diligence requirements along with current policies and procedures on money laundering and enhance them where necessary to detect transactions that may involve terrorist funds.

6.6. Banks and cash dealers should review their practices in this area as part of their general internal and external audit processes.

7.0 SOURCES OF TERRORIST FUNDS

7.1. Terrorist financing may be derived from two primary sources, although there are other sources which are no less important.

7.2. The first major source is the financial support provided by States or organizations with large enough infrastructures to collect funds and then make them available to terrorist organizations.

7.3. Also individuals with sufficient financial means may provide such funding to the terrorist.

7.4. The second major source of funds for terrorist organizations is income derived directly from various **revenue-generating** activities.

7.5. As with criminal organizations, a terrorist group's income may be derived from crime or other unlawful activities such as large-scale smuggling, various types of fraud, thefts and robbery, and narcotics trafficking.

7.6. Funding of terrorist groups may, unlike criminal organizations, also include income derived from legitimate sources such as donations or from a combination of lawful and unlawful sources.

7.7. Indeed, this funding from legal and apparently legitimate sources is key, the difference between terrorist groups and traditional criminal organizations.

7.8. Community solicitation and fundraising appeals are very effective means of raising funds to support terrorism. Often such fundraising is carried out in the name of organizations having the status of a charitable or relief organization.

7.9. In many cases, the charities to which donations are given are in fact legitimate in that they do engage in some of the work they purport to carry out.

7.10. Most of the members of the organization, however, have no knowledge that a portion of the funds raised by the charity is being diverted in a distinct pattern to terrorist causes.

7.11. Some of the specific fund raising methods might include: collection of membership dues and/or subscriptions; sale of publications; cultural and social events; door-to-door solicitation within the community; appeals to wealthy members of the community; and donations of a portion of their personal earnings.

8.0 LAUNDERING OF TERRORIST RELATED FUNDS

8.1. The methods used by terrorists and their associates to generate funds from illegal sources differ a little from those used by traditional criminal organizations. Although funds from legitimate sources need not be laundered, there is nevertheless a need for terrorists to obscure or disguise links between it and its legitimate funding sources.

8.2. It follows then that terrorists must find ways to launder these funds in order to be able to use them without drawing the attention of authorities.

8.3. In examining terrorist related financial activity, FATF experts have concluded that terrorists and their support organizations generally use the same methods as criminal groups to launder funds.

8.4. Some of the particular methods detected with respect to various terrorist groups include:

(a) cash smuggling,
(b) deposits to or withdrawals from bank accounts,
(c) purchases of various types of monetary instruments (travellers' cheques, bank cheques, and money orders),
(d) use of credit or debit cards, and
(e) wire transfers.

8.5. The terrorist's ultimate aim is not to generate profit from his fund but to obtain resources to support his operations.

8.6. Thus, the direction taken by fund transfers would be particularly relevant to the tracking down of terrorist financing.

8.7. A view may be taken in this regard either on the basis of repetitive similar transactions either from a sole account or from a number of accounts maintained in the same institution by different parties.

8.8. When terrorists obtain their financial support from legal sources (donations, sales of publications, etc), there are certain factors that make the detection and tracing of these funds more difficult.

8.9. For example, charities or non-profit organizations and other legal entities have been cited as playing an important role in the financing of some terrorist groups.

8.10. At first sight, the apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

8.11. Other important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved.

8.12. Several FATF experts have mentioned that the funding needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex and many involve the movement of small sums through wire transfers.

8.13. Enhanced due diligence techniques are therefore required for tracking down terrorist financing.

8.14. Terrorist financing which is an offence in itself is also a predicate offence for money laundering.

9.0 THE LEGISLATIVE FRAMEWORK OF ZIMBABWE

9.1. Historical Background

9.1.1. There were a number of pieces of legislation touching on money laundering in existence in Zimbabwe before the coming into being of the Bank Use Promotion and Suppression of Money Laundering Act in 2004.

9.1.2. These inter alia were:-

(a) The Serious Offences (Confiscation of Profits) Act of 1990
(b) The Prevention of Corruption Act
(c) The Criminal Procedure and Evidence Act
(d) The Criminal matters (mutual Assistance) Act
(e) Public Order and Security Act

9.1.3. It is thus clear that provisions dealing with the suppression of money laundering were scattered in different types of instruments. This had the disadvantage that the law ceased to be easily accessible to those members of society who need to use it.

9.1.4. There is also the danger that similar policy thrusts might end up contradicting each other with different authorities being designated in different Acts to pursue similar objectives.

9.1.5. There is also the danger that different Acts would impose different penalties for the same transgressions.

9.1.6. It is in this context that the promulgation of the Bank Use Promotion and Suppression of Money Laundering Act (Chapter 24:24) was met with a lot of optimism.

9.1.7. For a long time Zimbabwe has had a weak legal regime for the regulation of commercial crime. There was no comprehensive legislation to deal explicitly with money laundering.

9.2. The Bank Use Promotion And Suppression Of Money Laundering Act (Chapter 24:24)

9.2.1. The objectives of the Act which was gazetted on 17th of February 2004 and became into operation on 1 April 2004; were as follows:-

a) The promotion of the use of the banking systems
b) To regulate possible abuse of the banking system by using it as an organ for laundering illicit money
c) To provide rules and regulations for proactive measures to contain money laundering and
d) To make provisions for the identification, tracing, seizure and confiscation of tainted property.

9.2.2. The Act provides for the establishment of a unit of the Reserve Bank which is known as the Bank Use Promotion and Suppression of Money Laundering Unit. A Director appointed by the Governor shall head the unit whose composition includes officers, inspectors or employees of the Reserve Bank.

9.2.3. The unit has an inspectorate whose officers shall be answerable to the Director of the unit.

9.2.4. Section 4 of the Act details the functions of the unit which inter alia include the promotion of the use by the public of financial institutions for mediating, facilitating or obviating cash transactions, detecting suspicious transactions and referring such to relevant law enforcement agencies, monitoring and enforcing compliance with provisions of the Act by traders, parastatals and designated institutions and other persons.

9.2.5. The unit may also exercise any other functions bestowed upon it by the Governor of the Reserve Bank.

9.2.6. The Inspectors have general investigating powers and in some cases and under certain conditions they have power to seize property as well as entering any premises in connection with the exercise of their powers under the Act.

9.2.7. The Director in consultation with the Governor can issue directives on matters relating to:

(a) Hours during which financial institutions may be open to enable persons to withdraw cash;
(b) Priority to be given as between persons or entities in allocation of cash available for withdrawal; and,
(c) Returns and reports submitted by financial institutions to the unit.

9.2.8. The unit is obliged to produce half yearly reports and submit them to the Minister of Finance and Economic Development as soon as possible after the 30th June and the 31st of December in each year. The Minister will in turn lay the report before Parliament within 14 days of receipt of the report.

9.2.9. The Act also provides for an oversight committee to oversee the functions and operations of the unit and this is in the form of the Bank Use Promotion and Suppression of Money Laundering Advisory Committee.

9.2.10. The main functions of the advisory committee are through the Director and the Central Bank Governor, to advise the Minister on the formulation of national policies to promote the use of financial institutions as the agents for cash transactions and to combat money laundering.

9.3. Bank Use Promotion

9.3.1. The Act makes it mandatory for:-

(a) Traders to be registered in terms of the Value Added Tax Act (Chapter 23:12)

(b) Parastatals, Traders and moneylenders to open and keep a Bank account with a financial institution. Traders and parastatals must keep records of all daily cash transactions.

(c) The exchange of negotiable instruments for cash at a premium by any person who is not a financial institution is made an offence.

(d) Charges by financial institutions for the withdrawal, deposit or transfer of cash and other financial services shall be reviewed regularly and minimum bank balances shall be prescribed accordingly.

(e) Unlawful hoarding of cash is not permitted and it attracts a penalty.

9.4. Suppression of Money Laundering

9.4.1. Normally money laundering involves a process by which illegally obtained money or property is given an appearance of having originated from legitimate sources, money derived from illegitimate sources such as illegal arms sales, drug trafficking, prostitution, smuggling, insider trading, corruption or fraud is put through a cycle of transactions to disguise or conceal its origin.

9.4.2. The part of the Act on Money Laundering has to be read with related provisions of the serious offences (Confiscation of profits) Act Chapter 9: 17.

Designated Institutions….

9.4.3. Under the Act the following institutions are designated i.e. financial institutions other than the Central Bank, Insurers, Legal Practitioners, Chartered Accountants, and Public Accountants, Estate Agents, Money Lenders, Cash Dealers, Pension Funds, Trusts and Persons in the business of providing money transmission services.

9.4.4. These have an obligation to verify the identity of their customers and the capacity in which their customers will be acting when they transact.

9.4.5. They have to maintain customer records. Designated institutions have a mandatory duty to report suspicious transactions to the Bank Use Promotion and Suppression of Money laundering Unit as soon as possible and not later than 3 days of the suspicious transaction.

9.4.6. The designated institutions must establish internal reporting structures to deal with suspicious acts of money laundering.

9.4.7. A duty is imposed on designated institutions to take reasonable steps to ensure that their employees are aware of the policies in place to combat money laundering. Training of staff on this has to take place.

9.5. Seizure of Cash Unlawfully held

9.5.1. Inspectors of the Financial Intelligence Inspectorate and Evaluation Unit and the Police are given powers to search and seize cash from persons where there is reasonable belief that such cash is detainable in terms of the Act or that it is subject to or connected to a serious offence. [Refer also to Section 9.3.1(e)]

9.5.2. The same applies to cash which is subject to use in contravention of the Exchange Control Act (Chapter 22:05).

9.5.3. The search or seizure may be with the consent of the person or entity concerned, with a warrant issued by a magistrate or in an emergency without a warrant.

9.5.4. An inspector who intends to enter premises, search and seize cash or property must be accompanied by a Police Officer.

9.6. General Clauses

9.6.1. One cannot be liable for breach of the duty of secrecy or confidentiality where a disclosure is made in good faith in the ordinary course of one's duties.

9.6.2. The identity of a designated institution that makes a report to the Financial Intelligence Inspectorate and Evaluation (F.I.I.E.) Unit will not be disclosed unless the institution so consents.

9.6.3. Disclosure and use of information obtained by the unit in the course of its operations for personal gain by an officer or inspector of the unit shall be an offence.

9.6.4. All actions taken by the Government, the Reserve Bank, the Unit, inspector or member of the unit, any Police officer or any other person in good faith and due diligence shall be immune to criminal and civil proceedings.

9.6.5. Lawyer client relationship based information shall continue to be covered by privilege.

9.7. Terrorist Financing

9.7.1. Currently legislation dealing with anti-Terrorist financing is as inadequate as it is scattered in various pieces of legislation.

(a) The Public Order and Security Act (POSA) deals with such aspects. It is however crafted to deal with internal strife and does not address the complexities of international terrorist financing.

(b) The serious offences (Confiscation of Profits) Act, the Prevention of Corruption Act, the Criminal Procedure and Evidence Act all provide for the forfeiture and seizure of laundered assets and proceeds.

(c) The criminal matters (Mutual Assistance) Act provides for international cooperation in evidence gathering, extradition and general information exchange in various criminal matters including money laundering.

9.7.2. In order to enhance Zimbabwe's efforts at tackling money laundering and terrorist financing there is need to harmonise efforts by moving in tandem with international developments and best practices. Zimbabwe thus has to ensure that international conventions designed to combat organized crime, money laundering and terrorist financing are ratified amongst them:

- The convention for the suppression of the financing of International Terrorism (1999).

Recently Zimbabwe ratified the following conventions;

- United Nations Convention Against Transnational Organised Crime (2001)
- The United Nations Convention against Corruption
- The African Union Convention on preventing and combating corruption
- SADC Protocol against corruption.

9.7.3. Already measures are being implemented to ensure that this is done at the earliest possible time.

10.0 INTERNAL CONTROLS, POLICIES AND PROCEDURES

10.1. Responsibilities and Accountabilities

10.1.1. Banks and cash dealers are required to have in place adequate policies, procedures and internal controls that promote high ethical and professional standards and prevent their institution from being used, intentionally or unintentionally, by criminal elements.

10.1.2. Banks and cash dealers must therefore establish clear responsibilities to ensure that policies, procedures and internal controls are introduced and maintained which deter criminals from using their facilities for money laundering and terrorist financing.

10.1.3. Under section 3 (2) of the Bank Use Promotion and Suppression of Money Laundering Act, banks and cash dealers are required to take such measures as are reasonably necessary to ensure that neither they nor any service offered by them, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence. Any bank or cash dealer who fails to take such measures shall commit an offence.

10.1.4. Banks and cash dealers are also required to implement internal controls and other procedures to combat money laundering and the financing of terrorism which among other things include establishing and maintaining a manual of compliance procedures in relation to money laundering and programmes for assessing risks relating to money laundering and the financing of terrorism.

10.1.5. It is therefore of utmost importance for banks and cash dealers to have in place a sound ***Know Your Customer (KYC***) policy and procedure. KYC is most closely associated with the fight against money laundering and the financing of terrorism.

10.2. Appointment Of A Money Laundering Reporting Officer

10.2.1. It is imperative that every bank or cash dealer appoints an appropriate person, who may be among the existing employees of the institution or cash dealer, as a Money Laundering Reporting Officer (MLRO) and to whom all internal suspicious transactions reports will be made. The MLRO must be of sufficiently senior status and not below the rank of Manager.

10.2.2. Every branch in respect of banks or cash dealers should have an officer responsible for AML/CFT matters. (Refer also to Section 10.4.4)

10.2.3. It is incumbent on the MLRO, on behalf of the bank or cash dealer, to make Suspicious Transaction Reports to the BUP & SML Unit.

10.3. Recommended Procedures

10.3.1. All banks and cash dealers operating within Zimbabwe should:

a) Have procedures for the prompt validation of suspicious transaction and subsequent reporting by the internal employees to the MLRO.

b) Provide the MLRO with the necessary access to systems and records to enable him/her to investigate and validate internal suspicious reports which have been reported to him.
c) Inform all employees of the identity of the MLRO and in his absence, the alternative MLRO.

10.4. Appointment Of A Compliance Officer

10.4.1. Banks and cash dealers are also required to appoint a Compliance Officer at Management level who will bear the responsibility to verify, on a regular basis, compliance with policies, procedures and controls relating to money laundering and the financing of terrorism activities.

10.4.2. This will help to ensure that the responsibilities of banks and cash dealers under the Bank Use Promotion and Suppression of Money Laundering Act are being discharged.

10.4.3. It is important that the procedures and responsibilities for monitoring compliance with and effectiveness of, anti-money laundering and financing of terrorism policies and procedures are clearly laid down by all banks and cash dealers.

10.4.4. Due to economic size and logistical conditions it might not be necessary, however, to appoint a Compliance Officer in each and every branch of the bank or cash dealer. The appointment of a Compliance Officer at the Head Office with jurisdiction over its branches will suffice.

11.0 IDENTIFICATION PROCEDURES

11.1. Regulatory Framework

11.1.1. Part IV of the BUP & SML Act [Chap. 24:24] in respect of identity of customers provides as follows:-

Customers Identity….

(a) Every bank shall, before opening any account, issuing a passbook, entering into a passbook, entering into a fiduciary relationship, renting a safe deposit box or establishing any other business relationship, verify the true identity and address of its customer.

(b) In the case of bank accounts and security deposits which have been opened, and safe deposit boxes which have been rented out, prior to the coming into force of this Act, and where the true identity of the customer has not been satisfactorily established, the bank concerned shall, by writing to the customer in question or otherwise, take steps forthwith to establish his/her true identity.

(c) If the steps taken under subsection (2) fail to satisfy the bank concerned that they have established beyond reasonable doubt the true identity of the customer within twelve months of the coming into force of this Act, the bank shall forthwith close the account or security deposit, or terminate the lease of the safe deposit box, as the case may be, and report the matter to the central bank.

(d) Every bank which casts in breach of this section shall commit an offence and shall, on conviction, be liable to a fine which shall not be less than Z$ 1 billion.

11.1.2. It must be noted that the Bank Use Promotion and Suppression of Money Laundering Act 2004 also expressly prohibits any bank or cash dealer to open an anonymous or fictitious account.

11.1.3. The opening of reference accounts is permitted only after the identity of the applicant for business has been verified. A reference account is an account that is identifiable solely by the reference assigned to that account.

11.1.4. The manner of verification of identity and address of customers is prescribed in the Bank Use Promotion and Suppression of Money Laundering Act 2004. It involves;

(a) requesting for an identity document, where the applicant is an individual

(b) requesting for a certificate of incorporation together with the latest annual tax return to the Zimbabwe Revenue Authority, where the applicant is a body corporate.

11.2. Caveat

11.2.1. Banks and cash dealers should therefore never open, operate or carry out transactions pertaining to anonymous or fictitious accounts for customers.

11.3. Know Your Customer (KYC) Principle

11.3.1. The foundation of any effective system to combat money laundering and the financing of terrorism is the 'Know Your Customer' (KYC) principle. It is the degree of proximity between the bank or cash dealer and the customer which the KYC principle entails that will allow banks and cash dealers to gauge a situation, decide whether a transaction is suspicious and be able to avert risks inherent in money laundering and the financing of terrorism.

11.3.2. The safety and soundness of banks and cash dealers are therefore largely dependent on their KYC procedures. Sound KYC procedures, result in:

(a) Reduced likelihood of banks and cash dealers being used as vehicles for laundering of proceeds for criminal activities relating to the movement of terrorist funds.

(b) It being an essential part of sound risk management by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities.

11.3.3. The inadequacy or absence of KYC standards can subject banks and cash dealers to serious risks, especially;

(a) **Reputational Risk** – that is, the risk that adverse publicity regarding a bank's or cash dealer's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.

(b) **Operational Risk** – That is, the risk that the bank or cash dealer will suffer direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events which in the context of KYC relates to weaknesses in the implementation of programmes, ineffective control procedures and failure to practice due diligence.

(c) Legal Risk – the possibility that lawsuits, adverse judgments or contracts turn out to be unenforceable and disrupt or adversely affect the operations or condition of a bank or cash dealer.

(d) Liquidity Risk – This is the risk of insufficient liquidity for normal operating requirements that is the ability of the company to meet its liabilities when they fall due.

11.3.4. The need for banks and cash dealers to 'know your customer' (KYC) is therefore vital for the prevention of money laundering and the financing of terrorism.

11.3.5. A bank or cash dealer which has permitted the opening of an account or performed a transaction under a false identity, address or date of birth will render it difficult for Law Enforcement Agencies to trace the customer if he is needed for interview in connection with an investigation.

11.3.6. When a business relationship is being established, the nature of the business that the customer expects to conduct with the bank or cash dealer should be ascertained at the outset, to show what might be expected as normal activity.

11.3.7. In order to be able to judge whether a transaction is suspicious or not, banks and cash dealers should have a clear understanding of the legitimate business of their customers and effect an ongoing monitoring of the activities of those customers in order to detect whether those transactions conform or otherwise to the normal or expected transactions of that customer.

11.3.8. KYC should be a core feature of banks' and cash dealers' risk management and control procedures, and should be complemented by regular compliance reviews and internal audit.

11.4. Essential Elements Of KYC Standards

11.4.1. The essential elements of KYC standards should start from the banks' or cash dealers' risk management and control procedures and should include the following:

(a) Customer acceptance policy,
(b) Customer identification,
(c) On-going monitoring of high risk accounts and
(d) Overall Risk management.

11.5. Customer Acceptance Policy

11.5.1. Bank Use Promotion and Suppression of Money Laundering Act 2004, (Chapter24:24) require banks and cash dealers to implement due diligence procedures with respect to persons and business relations and transactions carrying high risk and with persons established in jurisdictions that do not have adequate systems in place against money laundering and the financing of terrorism.

11.5.2. Accordingly, banks and cash dealers should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank or cash dealer.

11.5.3. In preparing such policies, factors such as the customer's background, nature of business or social engagement, country of origin with a view to determining whether those countries have adequate systems in place against money laundering and the financing of terrorism, public or high profile position and other risk indicators should be considered.

11.5.4. Customer acceptance policies and procedures should accordingly be graduated and require more extensive due diligence for higher risk customers, such as politically exposed persons where decisions to enter into such business relationships should be taken with the concurrence of senior management.

11.5.5. The exercise should however be calibrated to ensure that the customer acceptance policy does not result in a denial of access by the general public to legitimate banking and cash services.

11.6. Customer Identification

11.6.1. For the purposes of these Guidance Notes, the following definitions will be used:-

(a) Applicant for Business means a person, who seeks to form a business relationship, or carry out a one-off transaction with a bank or cash dealer.

(b) Business Relationship means an arrangement between a person and a bank or a cash dealer where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the person and the bank or cash dealer on a frequent, habitual or regular basis.

(c) One off Transaction means any transaction carried out other than in the course of a business relationship. For example, a single foreign currency transaction carried out for a customer who does not have an account with the bank or cash dealer concerned.

(d) Significant shareholders means shareholders**,** other than shareholders which are companies listed on a recognized Stock Exchange as shown in Appendix **A**, who directly or indirectly hold 20% or more of the capital or of the voting rights of the company.

11.7. General Identification Requirements

11.7.1. Banks and cash dealers to establish and verify the identity and current permanent address of an applicant for business, the nature of the applicant's business, his financial status and the capacity in which he is entering into the business relationship with the bank or cash dealer.

11.7.2. A bank and cash dealer should establish to its satisfaction that it is dealing with a real person or organization, and verify the identity of the person or organization accordingly.

11.7.3. If funds that are to be deposited or transferred are being supplied on behalf of a third party the identity of that third party should be established and verified. In case a bank or cash dealer is not able to determine whether the applicant for business is acting for a third party, it should make a record of the grounds for suspecting that the applicant for business is so acting and make a Suspicious Transaction Report to the Bank Use Promotion and Suppression Money Laundering Unit.

11.7.4. Banks and cash dealers need to obtain all information necessary to establish to their full satisfaction the identity of the applicant for business and the purpose and nature of the business relationship or transaction.

11.7.5. They should cross check information by assessing available public database such as Financial Clearing Bureau (FCB), both at the local and international levels and keep on their files the full information on the ultimate beneficial owners in case they are not the same persons as the applicant.

11.7.6. Once identification procedures have been satisfactorily completed, and the business relationship established, no further evidence of identity is needed when transactions are subsequently undertaken for that customer, as long as regular contact is maintained.

11.7.7. When an existing customer closes one account and opens another there is no need to verify again identity, although good practice requires that the details on the customer's file be reconfirmed.

11.7.8. This is particularly important if there has been no recent contact with the customer e.g. for the past twelve months. Details of the previous accounts and steps originally taken to verify identity or any introduction records should be transferred to the new account records.

11.7.9. Subsequent changes to the name of the applicant for business, address or employment details of which the bank or cash dealer becomes aware, should be recorded and be duly substantiated by the appropriate documentary evidence as part of the KYC process.

11.7.10. In the case of an applicant for business transferring an opening balance from an account which he maintains with one bank directly to another bank, banks should consider the possibility that the previous account manager may have asked for the account to be closed because of suspicious or dubious activities.

11.7.11. If a bank or cash dealer has any reason to believe that an applicant is being or has been rejected by another bank or cash dealer, it should apply enhanced diligence procedures before accepting the customer e.g. cross checking with the Financial Clearing Bureau.

11.7.12. Banks and cash dealers should, in the case of personal accounts ensure that evidence of identity is obtained during the course of an interview with the applicant for business so that the bank or cash dealer can verify that the customer is actually the person he claims to be, i.e. the applicant for business should be seen personally and photographic evidence of his identity obtained.

11.7.13. In respect of joint personal accounts, the names and addresses of all account holders should be verified.

11.7.14. The verification procedures necessary to establish the identity of the applicant for business should be the same whatever the type of account or service that is required (e.g. current, deposit, or other accounts).

11.7.15. The full name of the member of staff undertaking or responsible for the account procedure should be noted on the customer's file together with that of the senior officer who has approved the business relationship.

11.7.16. Generally, the main objective of banks and cash dealers should be to look behind the institution to identify those who have control over the business and the assets.

11.7.17. The best identification documents are those that are the most difficult to obtain illicitly and to counterfeit. No single form of identification can be fully guaranteed as genuine or representing correct identity. To verify identity beyond reasonable doubt, the identification process will generally need to be cumulative. Refer to **Appendix C.**

11.8. Account Opening For Personal Customers

11.8.1. Paragraph 4 of Regulation 4 of the Bank Use Promotion and Suppression of Money Laundering Act 2004 provides that where an applicant for business is an individual customer, he shall submit to a bank or cash dealer, the original or a certified copy of an official valid document containing details of his current permanent address, a recent photograph of him and such other documents as may be required, to enable the bank or cash dealer to establish his identity.

11.8.2. Accordingly, banks and cash dealers are required to maintain the following identification procedures in respect of individual customers.

11.9. Face To Face Applications

Residents of Zimbabwe (Personal)……..

11.9.1. An individual's true identity comprises his/her date of birth, current permanent residential address, the nature of business, normal financial transactions and any agency or beneficiary relationship.

11.9.2. The name of individuals residing in Zimbabwe should, during the course of an interview with him, be verified from an **original** official valid document bearing his/her recent photograph and any of the following may be relied upon:-

(a) National identity cards
(b) Current valid passports
(c) Current valid driver's licenses.

11.9.3. What constitutes recent, for the purposes of the photograph, will in the circumstances, be decided during the course of the interview with the individual. A material difference in the photograph will lead the inference that the photograph may not be recent.

11.9.4. Banks and cash dealers should keep a copy of that page which contains the photograph of the applicant for business and ensure that the relevant reference numbers of those documents are recorded and the signatures on the application form and the official unexpired document cross-checked.

11.9.5. Because documents providing photographic evidence of identity need to be compared with the applicant's appearance, and to guard against the dangers of fraud, it would be appropriate to ensure that applicants for business do not send those identity documents by post to a bank or cash dealer.

11.9.6. In addition to the name, it is important that the current permanent address of the applicant or business be verified as an integral part of identity. Satisfactory evidence of address can be obtained by any of the following, a copy of which should be retained, after the original has been sighted. The retained copy shall be duly annotated "original sighted":

(a) A recent paid utility bill.
(b) A recent bank or credit card statement.
(c) A recent bank reference.

11.9.7. An introduction from a respected customer personally known to the manager, or from a trusted member of staff, may assist the verification procedure but must not replace the need for address verification procedures.

11.9.8. Details of those who initiated and authorized the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm. Directors/ senior managers must not require or request other staff to branch account opening procedures as a favour to the applicant.

11.9.9. Banks and cash dealers may effect additional verification of identity by

(a) Checking a local telephone directory.
(b) Checking a current register of electors.
(c) Visiting the applicant for business at his/her permanent residential address.

Non Residents (Personal).....

11.9.10. Regarding applicants for business who are not resident in Zimbabwe but who make face to face contact with a bank or cash dealer, they should be required to complete a standard application form which should incorporate the following details:-

(a) True name
(b) Current permanent address
(c) Mailing address
(d) Telephone and fax number
(e) Date and place of birth
(f) Nationality
(g) Occupation and name of employer (if self employed, the nature of the self employment)
(h) Signature/signatures
(i) Authority to obtain an independent bank reference.

11.9.11. The form, duly filled in, must be supported by a clear legible copy of any of the following documents:-

(a) National Identity Card
(b) Current valid passports
(c) Current valid driving licences
(d) Armed forces identity card

11.9.12. Banks and cash dealers should keep a copy of that page which contains the recent photograph of the applicant for business; ensure that the relevant reference numbers of the passports or National Identity Card, driving licences or armed forces identity card are duly recorded. The signatures on the application form and the abovementioned document should be cross checked.

11.9.13. In the case of non-residents making face- to-face contact, however, banks and cash dealers should in addition verify identity and current permanent address of the applicant for business with a reputable credit or financial institution in the applicant's normal home country or country of residence.

11.10. Non Face-To-Face Verification

11.10.1. It is most important that the procedures adopted to confirm identity for non face-to-face verification is at least as robust as those for face-to-face verification.

11.10.2. As with face-to-face verification, the procedures to check identity must serve two purposes:-

(a) They must ensure that a person bearing the name of the applicant exists and lives at the address provided; and
(b) That the applicant is that person.

11.10.3. Accordingly, in accepting business from non-face-to-face customers:

(a) Banks and cash dealers should apply equally effective customer identification procedures as for those available for interview; and
(b) Other specific and adequate measures to mitigate the high risk posed by non-face-to-face verification of customers.

Non-Resident (Personal) Applying from Abroad…….

11.10.4. Non-Residents applying from abroad should be required to complete a standard application form, which should incorporate the following details:

(a) True name
(b) Current permanent address
(c) Mailing address
(d) Telephone and fax number
(e) Date and place of birth
(f) Nationality
(g) Occupation and name of employer (if self employed, the nature of the self employment)
(h) Passport details, or National Identity Card, Driving Licence or Armed Forces identity Card details (i.e. number and country of issuance), together with issue date and expiry date.
(i) Signature/Signatures
(j) Authority to obtain independent verification of any data provided.

11.10.5. The application form, duly filled in, should be accompanied by any of the following supporting documents:-**Identity** – a clearly legible photocopy of any of the following documents:-

(a) National Identity Card
(b) Current valid passports
(c) Current valid driving licences
(d) Armed forces identity card

11.10.6. Duly certified as a true copy by a lawyer, accountant or other professional persons who clearly adds to the copy (by means of a stamp or otherwise) their name, address and profession to aid tracing of the certifier if necessary and which the bank or cash dealer believes in good faith to be acceptable.

Address…….

(a) An original or certified copy of utilities bill addressed to the applicant at the address from which he, she or they are applying:
(b) An original or certified copy of a bank statement addressed to the applicant at the address from which he, she or they are applying.

11.10.7. The following additional steps may be taken:-Confirmation by the bank or cash dealer from directory enquiries or from a recognized telephone directory for the locality from which the applicant is applying, containing an entry for the applicant and showing the address from which he, she or they are applying.

11.11. Account Opening For Institutions

Locally Incorporated Companies…..

11.11.1. With regard to locally incorporated companies, banks and cash dealers should verify the identity of those who have control over the company's business and assets, more particularly:

(a) Their directors,
(b) Their significant shareholders,
(c) Their authorized signatories and;
(d) The legal existence of the company.

11.11.2. The following documents should be obtained and retained in the case of locally incorporated companies:-

(a) In respect of employees authorized to open and operate accounts on their behalf, their directors and significant shareholders the same documents as are required for the identification of a personal customer;
(b) A certified copy of the resolution of the Board of Directors or managing body and the power of attorney granted to its employees to open and to operate accounts on their behalf; and

(c) Official documents which collectively establish the legal existence of that entity, e.g. the original or certified copy of the certificate of incorporation of the company, details of its registered office and place of business etc.

11.11.3. Enquiries should be made to confirm:

(a) that the company continues to exist and has not been, or is not in the process of being dissolved, struck off, wound up or terminated.

(b) By conducting in cases of doubt a visit to the place of business of the company, to verify that the company exists for a legitimate trading or economic purpose.

11.11.4. As with personal accounts, 'know your customer' is an on-going process. If changes to the company structure or ownership occur subsequently or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

Foreign Companies….

11.11.5. Where the applicant for business is a foreign company, the same documents as those required for locally incorporated companies should be sought for and retained.

11.11.6. In addition, banks and cash dealers should check the accuracy of the information provided with a credit or financial institution of good standing in the permanent place of business of the company.

11.11.7. Banks and cash dealers should also rely on other regulated institutions to verify identity of foreign companies.

Partnerships/Unincorporated Businesses…….

11.11.8. The applicant for business is a partnership or an unincorporated business;

(a) The identity of the partners, controllers of the unincorporated business and their authorized signatories should be verified in accordance with procedures required for the identification of personal applicants for business, and

(b) The same documents as are required for personal applicants for business should be requested and retained.

11.11.9. In the case of unincorporated businesses, in addition, the necessary license given by the competent Authorities for the conduct of such business should be requested and retained and in the case of partnerships, an original or certified copy of the partnership deed obtained.

11.11.10. Banks and cash dealers should also in cases of doubt make enquiries to confirm the true nature of the business activities to ascertain whether the business activities have a legitimate purpose.

Clubs and Charities……

11.11.11. It is increasingly being recognized that terrorists and terrorist groups are having recourse to clubs and charities for the financing of terrorism.

11.11.12. Accordingly, in the case of accounts to be opened for clubs or charities, banks and cash dealers should at the very beginning satisfy themselves as to the legitimate purpose of the organization by requesting a certified copy of the constitution of the club or charity and also in case of doubt by paying a visit to its premises where practicable to satisfy themselves as to the true nature of their activities.

11.11.13. They may also satisfy themselves by independent confirmation of the purpose of the institution.

11.11.14. The identity of the persons in control of the club or charity should be ascertained, in accordance with the procedures required for personal customers.

11.11.15. Control of clubs and charities are most likely to change from time to time and the identity of those new controllers of the clubs or charities should be verified as and when banks and cash dealers are advised of any change.

Societies……

11.11.16. In the case of societies, the original or certified copy of the Act should be requested and retained.

11.11.17. For Zimbabwean societies, the bank and cash dealer should ensure, by verifying with the Registrar of Companies, that the society is a legal entity.

11.11.18. As regards foreign societies the bank or cash dealer should obtain a certificate of good standing from them.

11.11.19. Banks and cash dealers should also, in accordance with the procedures set out for personal customers, verify the identity of those in control of the society, e.g. its administrators and should retain the same relevant documents as are required for personal customers accordingly.

Trusts……

11.11.20. Banks and cash dealers should exercise caution with respect to trusts, given the common perception that trusts are often used for laundering the proceeds of crime and hiding terrorist funds.

11.11.21. In the case of trusts, a certified copy of the original trust deed, or probate copy of a will creating the trust, and the deed evidencing appointment of the current trustees, the nature and purpose of the trust,.

11.11.22. Documentary evidence as are required for personal customers on the identity of the current trustees, the settler and/or beneficial owner of the funds and of any controller or similar person having power to appoint the trustees should be requested and retained.

11.11.23. Banks and cash dealers should also obtain written confirmation from the trustees that they are themselves aware of the true identity of the underlying principals' i.e the settlers/named beneficiaries, and that there are no anonymous principals.

'Client Accounts' Opened By Professional Intermediaries…..

11.11.24. Stockbrokers, fund managers, law practitioners, accountants, estate gents and other intermediaries frequently hold funds on behalf of their clients in **client accounts** opened with banks. Such accounts may be opened on behalf of either a single client or for many clients. In each case it is the intermediary who is the bank's customer.

11.11.25. In such cases, the bank is required to verify the identity of the professional intermediary itself and also to obtain from the intermediary;

(a) An undertaking that it has verified the identity of its clients and
(b) Particulars of the identity of those clients.

11.12. Reliance On Other Regulated Institutions To Verify Identity

11.12.1. Although the ultimate responsibility for verifying the identity and address of customers always lies with the bank and cash dealer, it is recognized that to avoid duplication, banks and cash dealers may rely on other eligible or group introducers to verify the identity of applicants for business.

11.12.2. Eligible introducers are persons who introduce other persons or bodies to Zimbabwean banks and cash dealers and have legislation in their country at least equivalent to that obtainable in Zimbabwe. A list of the jurisdictions which have legislation which is at least equivalent to that obtainable in Zimbabwe should be maintained.

11.12.3. **A group introducer** is an introducer who forms part of the same group as the bank or cash dealer and is subject to the consolidated supervision by a regulator.

11.12.4. Banks and cash dealers that use introducers should carefully assess whether the introducers are "fit and proper" in accordance with the guidelines on fit and proper issued by the Bank, a copy of which should be kept at Head Office and all branches.

11.12.5. Banks and cash dealers should use the following criteria to determine whether an introducer can be relied upon:

(a) It must comply with the customer due diligence practices identified in these Guidance Notes;

(b) The customer due diligence procedures of the introducer should be as rigorous as those which the bank or cash dealer would itself have conducted for the customer; and

(c) The systems put in place by the introducer to verify the identity of the customer should be very reliable.

11.12.6. In addition, banks and cash dealers should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above.

11.12.7. Banks and cash dealers must request group of eligible introducers to provide them with a duly completed Group Introducers Certificate or Eligible Introducers Certificate as the case may be.

11.12.8. It is left to banks and cash dealers to design their own Group or Eligible Introducers Certificates, provided that the information called for in the certificate does not differ materially with the specimens. The bank or cash dealer must reach an agreement with the introducer that it will be permitted at any stage to verify the due diligence undertaken by the introducer.

11.12.9. Banks and cash dealers should ensure that all relevant identification data and other documentation as stated in these Guidance Notes duly certified pertaining to the customer's identity should be immediately submitted by the introducer to the bank or cash dealer, who must carefully review the documentation provided.

11.13. Correspondent Services

11.13.1. Correspondent services consider services by one bank or cash dealer to another bank or cash dealer. The services are used by banks and cash dealers to conduct business that the banks or cash dealers do not offer directly.

11.13.2. Particular care should be taken where correspondent services involve jurisdictions where the correspondent banks or cash dealers have no physical presence.

11.13.3. If banks and cash dealers fail to apply an appropriate level of due diligence to such services, they expose themselves to a range of risks and may find themselves holding and/or transmitting money linked to terrorism, corruption, fraud or other illegal activity.

11.13.4. Banks and cash dealers should gather sufficient information about their correspondent institutions to understand fully the nature of the correspondent's business.

11.13.5. Factors to consider include: information about the correspondent's management, major business activities, where they are located and its money laundering prevention and detection efforts; the identity of any third party entities that use the correspondent services; and the condition of bank and cash dealer regulation and supervision in the correspondent's country.

11.13.6. Banks and cash dealer should only establish correspondent relationships with foreign banks and cash dealers that are effectively supervised by the relevant authorities and have effective customer acceptance and KYC policies.

11.13.7. In particular, banks and cash dealers should refuse to enter into or continue a correspondent relationship with a bank or cash dealer incorporated in a jurisdiction in which the correspondent has no physical presence and which is unaffiliated with a regulated financial group.

11.13.8. Banks and cash dealers should pay particular attention when continuing relationships with correspondents located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against money laundering and terrorist financing.

11.13.9. Banks and cash dealers should establish that their correspondent have due diligence standards as set out in these Guidance Notes.

11.13.10. Banks and cash dealers should be particularly alert to the risk that correspondent services might be used directly by third parties to transact business on their own behalf.

11.13.11. Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out for introduced business.

11.14. Exemptions

11.14.1. The Bank or cash dealer should, however, obtain and retain a written declaration from the other bank, financial institution or cash dealer that it holds documentary evidence of the existence of the legal entity, its regulated or listed status and that appropriate due diligence has already been carried out.

11.14.2. Identification procedures shall also not be required in relation to a once-off transaction, in which the proceeds of the transaction are not paid, but are directly reinvested on behalf of the person to whom the proceeds are payable in another transaction:-

(a) Of which a record is kept; and

(b) Which results only in another reinvestment made on that person's behalf or, in payment made directly to that person.

11.15. Politically Exposed Persons

11.15.1. Business relationships with individuals holding important positions and with persons or companies clearly related to them may expose a bank or cash dealer to significant reputational and/or legal risks.

11.15.2. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

11.15.3. The possibility exists that such persons may abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

11.15.4. Accepting and managing funds from corrupt PEPs is tantamount to money-laundering

11.15.5. Such a process will severely damage the bank's or cash dealer's reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove.

11.15.6. Under certain circumstances, the bank or cash dealer and/or their officers and employees themselves can be exposed to charges of money laundering, if they know or would have known that the funds were destined for financing of terrorism or stemmed from corruption or other crimes.

11.15.7. In Zimbabwe, corruption is a serious money laundering offence and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer).

11.15.8. There is a compelling need for a bank or cash dealer considering a relationship with a person whom it considers to be a PEP to identify that person fully, as well as people and companies that are closely related to him/her.

11.15.9. Banks and cash dealers should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is PEP. Banks and cash dealers should investigate the source of funds before accepting PEP.

8.64 Banks and cash dealers can reduce risk by conducting detailed due diligence at the out-set of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a "politically exposed person".

11.15.10. All banks and cash dealers should continuously assess which countries, with persons (entities) who are most vulnerable to corruption. One source of information is the Transparency International Corruption Perceptions Index (TICPI) at w.w.w.transparency.org.

11.15.11. Banks and cash dealers which are part of an international group might also use the group network as another source of information.

11.15.12. Where banks and cash dealers do have business in countries vulnerable to corruption, they should establish who the senior political figures are and, should seek to determine whether or not their customer has any connections with such individuals (for example they may be immediate family or close associates).

11.15.13. Banks and cash dealers should note the risk that individuals may acquire in such connections after the business relationship has been established.

11.15.14. Detailed due diligence should include:

(a) Close scrutiny of any complex structures (for example, involving companies, trust and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures bearing in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner rather than the reverse.

(b) Every effort to establish the source of wealth (including the economic activity that created wealth) as well as the source of funds involved in the relationship – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

(c) The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated.

(d) A review at senior management or board level of the decision to commence the business relationship and regular review, on at least an annual basis, of the development of the relationship.

(e) Close scrutiny of any unusual features, such as very large transactions, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

11.16. Wire Transfer Transactions

11.16.1. Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems.

11.16.2. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the originator is not clearly shown in an electronic payment message instruction.

11.16.3. To ensure that wire transfer systems are not used by criminals as a means to break the audit trail, where a bank or cash dealer makes a payment on behalf of its customer, accurate and meaningful originator information (name, residential address and any account number or reference of the originator) should be included on all money transfers and related messages and should remain with the transferor through the payment chain until it reaches its final destination.

11.16.4. This information is particularly important for international transfers on behalf of individual customers to ensure that the source of funds can be identified in the event of an investigation in the receiving jurisdiction.

11.16.5. Where money transfers are processed as an intermediary, e.g. where a bank or cash dealer"B" is instructed by bank or cash dealer "A" to pay funds to an account held by a beneficiary at bank or cash dealer "C", the originator and beneficiary data provided by bank or cash dealer "A" should be preserved and, wherever possible, included in the message generated by bank or cash dealer "B".

11.16.6. Banks or cash dealers should conduct enhanced scrutiny of, and monitor for suspicious activity, incoming funds transfers which do not contain complete originator information.

11.16.7. This will involve examining the transaction in more detail in order to determine whether certain aspects related to the transaction could make it suspicious (for example origin in a country known to harbour terrorists or terrorist organizations).

11.17. On-Going Monitoring Of Accounts And Transactions

11.17.1. On-going monitoring is an essential aspect of effective KYC procedures.

11.17.2. For all accounts, banks and cash dealers should have systems in place to detect unusual or suspicious patterns of activity.

11.17.3. Certain types of transactions should alert banks and cash dealers to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer.

11.17.4. Very high account turnover, inconsistent with the size of the balance sheet, may indicate that funds are being "washed" through the account.

11.17.5. Examples of suspicious activities are given at appendices **E** and **F**. Banks and Cash Dealers are encouraged to study money laundering or terrorist financing typologies coming their way or published by the Financial Action Task Force (FATF) **at http://www.fatf-gafi.org** to keep their relevant staff duly informed of the patterns of abuse.

11.17.6. Where the originator is acting on behalf of others (e.g. as nominee, agent, or trustee), then it is the name, address and account number of the nominee, agent, trustee, etc that should be included. The bank or cash dealer making the payment should have on file the name and address of underlying principles.

11.17.7. There should be intensified monitoring for high risk accounts. Every bank and cash dealer should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. Banks and cash dealers should;

(a) ensure that they have adequate management information systems to provide managers and MLROs with timely information needed to identify, analyse and effectively monitor high risk customer accounts. The types of reports that may be needed in the AML/CFT area include transactions made through an account that are unusual.

(b) develop a clear policy and internal guidelines, procedures and controls and remain very vigilant regarding business relationship with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them.

(c) As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

12.0 RISK MANAGEMENT

12.1. The board of directors of the bank and cash dealer should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness.

12.2. Explicit responsibility should be allocated within the bank and cash dealer for ensuring that their policies and procedures are managed effectively.

12.3. Banks' and cash dealers' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures.

12.4. As a general rule, the compliance function should through the Compliance Officer provide an independent evaluation of the bank's or cash dealer's own policies and procedures, including legal and regulatory requirements.

12.5. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

12.6. Internal audit plays an important role in independently evaluating the risk management controls, and should report to the Audit Committee of the Board of Directors or a similar oversight body.

12.7. Management should ensure that internal audit functions are staffed adequately with individuals who are well-versed in such best practices policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

12.8. External auditors also have an important role to play in monitoring banks' and cash dealers' internal controls and procedures, and in confirming that they are in compliance with laws, rules, regulations and these Guidance Notes.

13.0 RECORD-KEEPING

13.1. Statutory Requirements

13.1.1. Section 17 of the Bank Use Promotion and Suppression of Money Laundering Act requires banks and cash dealers to keep records, registers and documents of their customers.

13.1.2. Regulations have been made in that respect and those regulations empower the central bank to make provision for the keeping of records for periods exceeding five years.

13.1.3. By virtue of these powers, the central bank is hereunder making provision for the keeping of records.

13.2. Audit Trail

13.2.1. Record keeping is an essential component in the combat against money laundering and the financing of terrorism in the sense that an audit trail is established.

13.2.2. Otherwise, an authority investigating a case related to anti-money laundering or the financing of terrorism would not be able to follow the movement of the funds through the financial system thus rendering enquiry and confiscation of those funds difficult.

13.2.3. Often the only valid role a bank or cash dealer can play in anti-money laundering or financing of terrorism investigations is through the provision of relevant records, particularly where a complex web of transactions specifically for the purpose of confusing the audit trail has been used.

13.3. Identity Records

13.3.1. All documentation required by banks and cash dealers to verify the identity of customers must be retained for a period of not less than 10 years after the closure of the account or cessation of the business relationship with the customer concerned.

13.3.2. In cases where a third party has been relied upon to undertake verification of identity procedures or to confirm identity, copies of all records relating to verification of identification should be retained in Zimbabwe for the same period as stated in the paragraph above.

13.4. Transaction Records

13.4.1. Transaction records, in whatever form they are used, e.g. credit/debit slips cheques etc. need to be maintained for a period of not less than 10 years after the completion of the transactions concerned, to enable investigating authorities to compile a satisfactory audit trail for suspected laundered and terrorist funds and establish a financial profile of any suspicious account. This should include the following:-

(a) the volume of funds flowing through the account.
(b) the source of the funds, including full remitter details.
(c) the form in which the funds were offered for withdrawal i.e. cash, cheques, etc.
(d) the identity of the person undertaking the transaction.
(e) counter party details
(f) the destination of the funds.
(g) the form of instruction and authority.
(h) the date of the transaction.

13.5. Reports made to and by the MLRO

13.5.1. Records of all internal reports made to the Money Laundering Reporting Officer and also all reports made by the MLRO to the F.I.I.E. should be retained for a period of not less than 10 years after the date of reporting.

13.6. Records Relating To On-Going Investigations

13.6.1. Where the records relate to on-going investigations, they should be retained until it is confirmed by the authorities that the case has been closed.

13.7. Electronic Records

13.7.1. Records of electronic payments and messages must be treated in the same way as any other records and kept for the period mentioned in *13.4.1*.

13.7.2. A comprehensive set of identification documents in respect of each customer should be kept in an orderly manner and produced to the central bank on request.

13.7.3. It is lawful to electronically record any matter and a personal identification mark on the electronically recorded document is as good as a signature.

14.0 RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTION

14.1. What Is A Suspicious Transaction?

14.1.1. A Suspicious transaction has been defined in the interpretation section of the Bank Use Promotion and Suppression of Money Laundering Act. This statutory definition is reproduced at paragraph **4.2** of these Guidance Notes.

14.1.2. A suspicious transaction is a transaction which gives rise to suspicion for any reason.

14.1.3. Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer and the customer's business to recognize that a transaction, or series of transactions, are unusual.

14.1.4. Questions that a bank or cash dealer might consider when determining whether an established customer's transaction might be suspicious are:-

(a) Is the size of the transaction consistent with the normal activities of the customer?
(b) Is the transaction rational in the context of the customer's business or personal activities?
(c) Has the pattern of transactions conducted by the customer changed?
(d) Where the transaction is international in character, does the customer have any obvious reason for conducting business with the other country involved?

14.2. Examples of Suspicious Transactions

14.2.1. Examples of what may constitute suspicious transactions in relation to money laundering are given in **Appendix E**.

14.2.2. However, identification of any of the types of transactions listed in **Appendix F** along with other available information including in the case of terrorism, lists of suspected terrorists, terrorist groups and associated individuals and entities issued by the United Nations, should prompt further investigation and be a catalyst towards making further enquiries.

14.2.3. Sufficient guidance must be given to staff to enable them to recognize suspicious transactions**.** The type of situations giving rise to suspicious transactions will depend on a bank's or cash dealer's customer base and range of services and products.

14.2.4. Banks and cash dealers might also consider monitoring the types of transactions and circumstances that have given rise to suspicious reports by staff, with a view to updating internal instructions from time to time.

15.0 REPORTING OF SUSPICIOUS TRANSACTIONS

15.1. There is an obligation on all staff to report in writing to the MLRO suspicious activity of money laundering and terrorist financing.

15.2. However, if the staff considers that the preparation of the report for the MLRO or refusal to carry out the transaction may jeopardize the tracking of the beneficiaries of a suspicious transaction or where it is impossible to prepare such a report, the staff may process the transaction but he must immediately thereafter report the matter to the MLRO who will accordingly lodge a report of the transaction to the FIIE.

15.3. All banks and cash dealers have a clear obligation to ensure that:-

(a) Each relevant employee knows to which person he or she should report suspicious transactions.

(b) There is a clear reporting chain under which those suspicious transactions will be passed directly and without delay to the MLRO.

(c) Once an employee has reported his/her suspicion to the MLRO, he/she has fully satisfied and discharged his/her statutory obligation.

15.4. The Money Laundering Reporting Officer (MLRO)

15.4.1. Banks and cash dealers should ensure that appropriate replacement will be provided in case the MLRO is absent. In no case, however, should a member of the Internal Audit Department of the bank or cash dealer perform the duties of the MLRO as this will create a conflict of interest.

15.4.2. The MLRO must be endowed with a significant degree of responsibility and independence. He/she is required to determine whether the information or other matters contained in the transaction report he/she has received give rise to knowledge of reasonable suspicion that a customer is engaged in money laundering or the financing of terrorism.

15.4.3. In making this judgment, he/she should consider all other relevant information available within the bank or cash dealer concerning the person or business to which the initial report relates.

15.4.4. This may include making a review of other transaction patterns and volumes through the accounts in the same name, the length of the business relationship, and referral to identification records held.

15.4.5. If, after completing this review, it is decided that there are no facts that would prove the suspicion, then he/she must report that suspicious transaction to the F.I.I.E.

15.4.6. Nevertheless, care should be taken to guard against a report being submitted as a matter of routine without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

15.4.7. The MLRO will be expected to act honestly and reasonably and to make his/her determination in good faith.

15.4.8. Provided the MLRO or in his absence, the person authorized to replace him, does act in good faith in deciding not to pass on any suspicious transaction, there will be no liability for non-reporting if his judgment is latter found to be wrong.

15.5. Internal Reporting Procedures And Records

15.5.1. Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO.

15.5.2. All suspicious transactions reported to the MLRO should be documented.

15.5.3. The report should include full detail of the customer.

15.5.4. The MLRO should acknowledge receipt of the report. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented.

15.5.5. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, is an investigation in a case on which the MLRO has opted not to report and suspicious activities are later found to be true.

15.5.6. On-going communication between the MLRO and the internal reporting person/department is important. The person who has made the report to the MLRO should be made aware of the MLRO's decision whether a report has been made by him to the F.I.I.E. Unit or otherwise.

15.5.7. Likewise, at the end of an investigation, all members of staff concerned should be informed of the outcome. It is particularly important that the MLRO is informed of all communication between the investigating authorities and the bank or cash dealer at all stages of the investigation.

15.6. Other Crimes

15.6.1. MLROs should distinguish between the making of Suspicion Transaction Reports in respect of money laundering or the financing of terrorism and the lodging of a complaint or allegation of crime with the Police for investigation.

15.7. Reporting

15.7.1. **Anyone who fails to report on activities related to money laundering shall be guilt and liable for a fine not less than $ 5 billion.**

16.0 EDUCATION AND TRAINING

16.1. On-Going Training Programme

16.1.1. Every bank or cash dealer must, in order to combat money laundering and the financing of terrorism, implement an ongoing training programme for its officers and employees in order to discharge part of its statutory duty to take reasonable measures in that regard.

16.2. Staff Awareness

16.2.1. Banks and cash dealers must take appropriate measures to make employees aware of:

(a) Policies and procedures put in place to prevent money laundering and the financing of terrorism including those for identification, record-keeping, the recognition and handling of suspicious transactions and internal reporting.

(b) The legal requirements contained in the BUP & SML Act of 2004, the Prevention of Corruption Act 2004, in so far as it is applicable to money laundering, the Bill on Suppression of International Terrorism with regard to the financing of terrorism and the Convention for the Suppression of the Financing of International Terrorism (1999) and Regulations applicable to them.

(d) Their own personal statutory obligations and the fact that they can personally be liable for failure to report information in accordance with internal procedures.

16.3. Different Requirements For Different Categories Of Staff

Account Opening Personnel…..

16.3.1. Those members of staff responsible for account opening and acceptance of new customers must receive training in respect of the need to verify a customer's identity and on the internal opening and customer verification procedures available in the institution.

16.3.2. They should also be familiarized with the recognition and handling of suspicious transactions and internal suspicious transaction reporting procedures.

Front Line Staff….

16.3.3. All front line staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorists or their agents.

16.3.4. They have to be trained to know the true identity of the customer and the need to, at the outset, know enough of the type of business activities the client is into.

16.3.5. They should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute conduct. They should be provided with training on the recognition and handling of suspicious transactions and on the procedures to be adopted when a transaction is regarded as suspicious.

New Employees….

16.3.6. New employees must, as soon as may be reasonably practicable be given a broad appreciation of the general background to the combating of money laundering and the financing of terrorism, and the internal suspicious transactions reporting procedures.

16.3.7. They should be made aware of the importance placed on the reporting of suspicious transactions by the organization, that there is a legal requirement to report and that there is a personal statutory obligation in this respect.

16.3.8. They should also be provided with a copy of the written policies and procedures in place for the reporting of suspicious transactions.

Supervisors and Managers…….

16.3.9. A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff.

16.3.10. This will include the penalties arising under the Act for non-reporting, assisting money launderers and 'tipping off; internal reporting procedures; and the requirements for the verification of identity and retention of records.

MLROs and Compliance Officers….

16.3.11. In-depth training concerning all aspects of the Bank Use Promotion and Suppression of Money Laundering Act of 2004, the Prevention of Corruption Act of 2004 in so far as it is applicable to money laundering, the Prevention of Terrorism Act 2004 in regard to the financing of terrorism and the Convention for the Suppression of the Financing of Terrorism Act 2003 and the Regulations applicable to those legislations, the internal policies applicable in their institutions and the recognition of suspicious transactions, will be required for the MLRO and Compliance Officer.

16.3.12. In addition, the MLRO and Compliance Officer will require extensive initial and ongoing instruction on the validation and reporting of suspicious transactions, on feedback arrangements, and on new trends and patterns of criminal activity.

16.4. Refresher Training

16.4.1. It will be necessary to make arrangements for refresher training at regular intervals to ensure that staff does not forget their responsibilities.

16.5. Records

Banks and cash dealers should keep a record of all anti-money laundering and combating the financing of terrorism training delivered to its employees.

APPENDIX A

RECOGNISED, DESIGNATED AND APPROVED STOCK/INVESTMENT EXCHANGES

a) Recognised UK Investment Exchanges

- London Stock Exchange (LSE)
- London International Financial Futures & Options Exchange (LIFFE)
- International Petroleum Exchange of London (IPE)
- London Commodity Exchange (LCE)
- London Metal Exchange (LME)
- London Securities and Derivatives Exchange (OMLX)
- Trade point Financial Networks PLC

b) Recognised Overseas Investment Exchanges:

- The National Association of Securities Dealers Incorporated (NASDAQ)
- Sydney Futures Exchange Ltd (SFE)
- Chicago Mercantile Exchange (GLOBEX)
- Chicago Board of Trade (GLOBEX)
- New York Mercantile Exchange (NYMEX)

c) The Channel Islands Stock Exchange

2. Designated Investment Exchanges (DIEs) American Stock Exchange

- American Stock Exchange (ASE)
- Amsterdam Pork & Potato Terminal Market Clearing House (NLKKAS)
- Amsterdam Futures
- Australian Futures
- Bolsa Mexicana de Valores
- Chicago Board Options Exchange Mercantile Exchange
- Coffee, Sugar and Cocoa Exchange, Inc
- Commodity Exchange Inc
- Copenhagen Stock Exchange (Inc. FUTPO)
- DTB Deutsche Terminborse
- European Opinions Exchange
- Financiele Termijinborse
- Finnish Options Market
- Hong Kong Stock Exchange
- International Securities Market Association
- Irish Futures and Options Exchange (IFOX)
- Johannesburg Stock Exchange
- Kansas City Board of Trade
- Korea Stock Exchange
- Marche' des Options Negociables de Paris (MONEP)

- Marche a Terme International de France
- MEFF Renta Fija
- MEFF Renta Variable
- Midway Commodity Exchange
- Midwest Stock Exchange
- Minneapolis Grain Exchange
- New York Cotton Exchange (including Citrus Associates of the New York Cotton Exchange
- New York Futures Exchange
- New York Mercantile Exchange
- New York Stock Exchange
- New Zealand Futures Exchange
- New Zealand Stock Exchange OM Stockholm AB
- Osaka Stock Exchange
- Pacific Stock Exchange
- Philadelphia Board of Trade
- Philadelphia Stock Exchange
- Singapore International Monetary Exchange (SIMEX)
- Singapore Stock Exchange
- South African Futures Exchange (SAFEX)
- Swiss Options and Financial Futures Exchange
- Sydney Futures Exchange
- Tokyo International Financial Futures Exchange (TIFFE)
- Tokyo Stock Exchange
- Tokyo Futures Exchange
- Vancouver Stock exchange

3. Approved Exchanges

- Amsterdam Stock Exchange
- (Amsterdamse Effectenbeurs)
- Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen)
- Association de Intermediaros de Activos Financieros (Spanish Bond Market)
- Athens Stock Exchange (ASE)
- Barcelona Stock Exchange (Bolsa de Valores de Barcelona)
- Basle Stock Exchange (Basler de Valores de Barcelona)
- Belgium Futures & Options Exchange (BELFOX)
- Berlin Stock Exchange (Berliner Borse)
- Bergen Stock Exchange (Bergen Bors)
- Bergen Stock Exchange (Borsa de Valores de Bilbao)
- Bologna Stock Exchange (Borsa Valori de Bologna)
- Bolsa de Mercadorios & Futures (BM & F)
- Boedeaus Stock Exchange (Bourse de Boardeaux)
- Boston Stock Exchange
- Bovespa (Sao Paulo Stock Exchange)
- Bremem Stock Exchange (Bremener Werkpapierborse)
- Brussels, Stock Exchange (Societe de la Bourse des Valeurs

- MoilieresjEffecten Beursvennootschap van Brussels)
- BVR (Rio de Janeiro Stock Exchange)
- Cincinnati Stock Exchange
- Copenhagen Stock Exchange (Kobenhavns Fondsborse)
- Fukuoka Stock Exchange
- Genoa Stock Exchange (Borse Valori di Genoa)
- Hamburg Stock Exchange (Hanseatische Vertipapier Borse Hamburg)
- Hannover SE (Niedersachsische Borse zu Hannover)
- Helsinki Stock Exchange (Helsigen Arvopaperiporssi Osuuskunta)
- Kuala Lumpur Stock Exchange
- Lille Stock Exchange
- Lisbon Stock Exchange (Borsa de Valores de Madrid)
- Marseilles Stock Exchange
- Mercato Italino Futures (MIF)
- Mid West Stock Exchange
- Milan Stock Exchange (Borsa Balores de Milano)
- Munich Stock Exchange (Bayerische Borse in Munchen)
- Nagoa Stock Exchange
- Nancy Stock Exchange (Bourse de Nancy)
- Nantes Stock Exchange (Bourse de Nantes)
- Naples Stock Exchange (Borsa Valori di Napoli)
- New Zealand Stock Exchange
- Oporto Stock Exchange (Bolsa de Valores de Porto)
- Osla Stock Exchange (Osla Bors)
- Palermo Stock Exchange (Borsa Valori de Palenno)
- Rome Stock Exchange (Borsa Valori di Roma)
- Stockholm Stock Exchange (Stockholm Fondbors)
- Stuttgart Stock Exchange (Baden – Wurtembergische Wertpapierborse zu Stuttgart)
- Taiwan Stock Exchange
- Tel Aviv Stock Exchange
- The Stock Exchange of Thailand
- Trieste Stock Exchange (Borse Valori di Trieste)
- Trondhiem Stock Exchange (Trondheims Bors)
- Valencia Stock Exchange (Borsa Valori de Venezia)
- Vienna Stock Exchange
- Zurich Stock Exchange (Zurcher Borse)

4. EFA Regulated Markets Under Article 16 of the Investment Services Directive (93/22/EEC)

(Note some listed may also be included I the lists of DIEs or Approved Exchanges)

Austria

- Vienna Stock Exchange
- (Wiener Wertpapielborse)
- Austrian Financial Futures and Options Exchange (Vienna)
- (Osterreichische Termin-und Optionenborse Aktiengeselleschaft)

Belgium

De eerste en tweede markt van de effectenbeurs van Brussel/Le

Denmark

- The Copenhagen Stock Exchange, Clearing House

France

- Le Matif
- Le Premier marche et le second marche de la bourse de Paris

Finland

- Hex Ltd Helsinki Securities and Derivatives Exchange, Clearing House

France

- Le Matif
- Le premier marche et le second marche de la bourse de Paris
- Le nouveau marche
- Le monep

Germany

- Berliner Wertpapierborse (Amtlicher Handel, Geregelter Markt) (Berlin Stock Exchange)
- Wertpapierborse in Brenme (Amtlicher Handel, Geregelter Markt) (Rhine Westphalian Stock Exchange Dusseldorf)
- Frankfurter Wertpapiernborse (Amtlicher Handel, Geregelter Markt) (Frankfurt Stock Exchange)
- Deutsche Terminborse (DTB)
- Hanseatic Wertpapierborse Hamberg (Amtlicher Handel, Geregelter Markt) (Hanseatic Stock Exchange Hamburg)
- Niedersachsische Borse (Amtlicher Handel, Geregelter Markt) (Amstock Exchange of Lower Saxony (Hanover) Bayerische Borse (Amtlicher Handel, Geregelter Markt) (Bavarian Stock Exchange (Munich)
- Baden – Wurttembergische Wertpapierborse (Amtilicher Handel, Geregelter Markt) Baden – Wurttenberg Stock Exchange (Stuttgart)

Greece

- Athens Stock Exchange
- Thessalonki Stock Exchange Centes (TSEC)

Iceland

- Iceland Stock Exchange (Verdbrefathing Islands

Ireland

- Ireland Stock Exchange

Italy

- Borsa Italian SPA (Italian Stock Exchange, Milan)

Luxemburg

- Luxembourg Stock Exchange (Societe de la Bourse de Luxembourg SA)

The Netherlands

- Amsterdam Exchanges (Amsterdamse effectenbeurs) EOE –optiebeurs

Norway

- The Oslo Stock Exchange

Portugal

- Mercado de Cotacoes Oficials de Bolsa de Valores de Usboa (Market with Official Quotations of the Bolsa de Valores de Lisboa)
- Segundo Mercado de Bolsa de Valores de Lisboa (Second Market of the Bolsa de Valoras de Lisboa)
- Bolsa de Derivados de Porto

Spain

- La Bolsa de Valores de Barcelona
- La Bolsa de Valores de Bilbao
- La Bolsa de Valores de Madrid
- Los Bolsa de Valores de Valencia
- Los mercados oficiales de futuros y opciones de Meff Sociedad rectora del Mercado de Products Financieros Derivados de Renta Fija, Sa y Meff Sociedad Rectora del Mercaod de Products Financieros Derivados de Renta Variable, SA AIAF, Mercado de Renta Fija, SA Mercado de Deusa Publica en Anotaciones

Sweden

- Stockholm Stock Exchange (Stockholm Fondbors AB)
- Penningmarknadsinformation Pml AB
- OM Stockholm AB

United Kingdom

The following four of the markets comprising the London Stock Exchange Limited:

- The Domestic Equity Market
- The European Equity Market
- The Gilt-Edged and Sterling Bond Market
- The Alternative Investment Market

The London International Financial Futures and Options Exchange (LIFFE) OMLX. The London Securities and Derivatives Exchange Limited Tradepoint Stock Exchange

APPENDIX B

FATF MEMBER COUNTRIES AND TERRITORIES WITH LEGISLATION/STATUS/ PROCEDURES EQUIVALENT TO THE ZIMBABWEAN LEGISLATURE OR PROCEDURE

1. Australia
2. Bahamas
3. Bermuda
4. Belgium
5. Canada
6. Cayman Islands
7. Denmark
8. Finland
9. France
10. Germany
11. Gibraltar
12. Greece
13. Guernsey
14. Hong Kong
15. Iceland
16. India
17. Ireland
18. Isle of Man
19. Italy
20. Japan
21. Jersey
22. Luxembourg
23. Malta
24. Netherlands (Excluding Netherlands Antilles)
25. New Zealand
26. Norway
27. Portugal
28. Singapore
29. South Africa
30. Spain
31. Sweden
32. Switzerland
33. United Kingdom
34. United States

APPENDIX C

ELIGIBLE INTRODUCERS CERTIFICATE

Name of Applicant:…….....

Address of Applicant:…….....
(including postcode)
.....

I/WE CERTIFY THAT in accordance with the provisions of the Bank Use Promotion and Suppression of Money Laundering Act 2004 on the prevention of Money Laundering and Terrorist Financing as amended from time to time, or equivalent legislation:

(i) We have verified the identity of the Applicant and confirm that documentary evidence has been obtained and identity checks have been undertaken to confirm that the applicant(s) name(s) and address (es) as shown on the applicant form(s) is/are correct.

(ii) The underlying records of identity and copies of the documentary evidence received are attached to this certificate.

AND

(iii) The Applicant (s) is/are applying on his/his own behalf and not as nominee, trustee or in a fiduciary capacity for any other person.

(iv) I/WE am/are unaware of any activities of the Applicant that cause me/us to suspect either that the applicant is engaged in money laundering or any other from of criminal conduct.

Full Name of Regulated Introducer:…….....

Name of Regulator……..Country of Regulator.....

Licence or Registration No……

Signed:…….Full Names……

Job Titles:…….Dates……

APPENDIX D

NON-COOPERATIVE COUNTRIES OR TERRITORIES

The FAFT recommends that special attention should be given to business relations and transactions with persons, including companies and financial institutions, from the 'non-cooperative countries and territories' listed below:-

The current list as of 2 July 2004 of non-cooperative countries and territories is as follows:

1. Cook Islands
2. Myanmar
3. Indonesia
4. Nauru
5. Nigeria
6. Philippines

APPENDIX E

EXAMPLES OF SUSPICIOUS TRANSACTIONS (MONEY LAUNDERING)

(j) MONEY LAUNDERING USING CASH TRANSACTIONS

(a) Unusually large cash deposits made by an individual or company whose normal business activities would normally be generated by cheques and other instruments.
(b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
(c) Customers who deposit cash by means of numerous credits slips so that the amount of each deposit is unremarkable, but the total of all the credits is significant or similar deposits at a number of branches within a short space of time, all being credited to a central account.
(d) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than forms of debit and credit normally associated with commercial operations (e.g cheques, letters of credit, Bills of Exchange, etc).
(e) Customers who constantly pay in or deposit cash to cover requests for money transfers, bankers' drafts or other negotiable and readily marketable money instruments.
(f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
(g) Frequent exchange of cash into other currencies.
(h) Branches that have a great deal more cash transactions than usual.

(ii) MONEY LAUNDERING USING BANK ACCOUNTS

(a) Customers who wish to maintain a number of trustee accounts which do not appear consistent with the type of business, including transactions which involve nominees.
(b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
(c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase and turnover on an account).
(d) Paying in large third party cheques endorsed in favour of the customer.
(e) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
(f) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
(g) Greater use of safe deposit facilities. The use of sealed packets deposited and withdrawn.
(h) Companies' representatives avoiding contact with the branch.
(i) Substantial increases in deposits of cash or negotiable instruments by a professional firm or

company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client, company and trusts accounts.

(j) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(k) Insufficient use of normal banking facilities (e.g. avoidance of high interest rate facilities for large balances).

(l) Large number of individuals making payments into the same account without an adequate explanation.

(iii) MONEY LAUNDERING BY OFFSHORE INTERNATIONAL ACTIVITY

(a) Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(c) Customers who make regular and large payments, including wire transactions, that can be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs and /or proscribed terrorist organizations.

(d) Building up large balances, not consistent with the known turnover of the customer's business and subsequent transfer of account(s) held overseas.

(e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

(f) Frequent requests for traveler's cheques. Foreign currency drafts or other negotiable instruments to be issued.

(g) Frequent paying in of traveler's cheques of foreign currency drafts, particularly if originating from overseas.

(iv) MONEY LAUNDERING INVOLVING FINANCIAL INSTITUTION EMPLOYEES AND AGENTS.

(a) Changes in employee's characteristics (e.g. lavish lifestyles).

(b) Changes in employee or agent performance (e.g. the salesman selling products for cash has remarkable or unexpected increase in performance).

(c) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

(d) Overbilling Schemes, whereby materials ordered for a purchase are of a poorer quality and lower price than what was specified, but this is not reflected in the negotiated contract.

(e) Corporate crime against the interest of shareholders and of the public at large.

(f) Admissions or statements by directors, officers or employees to law practitioners of their or their company's involvement in criminal activities.

(v) MONEY LAUNDERING BY SECURED AND UNSECURED LENDING

(a) Customers who repay problem loans unexpectedly.
(b) Request to borrow against assets held by the institutions or a third party, where the origin of the assets is not reasonably known or the assets are inconsistent with the customer's standing.
(c) Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

Sales and dealing staff……..

(a) New Business

(i) A client with no acceptable reason for using the firm's services, e.g. clients with distant addresses who could find the same service nearer their home base; clients whose requirements are not in the normal pattern of firm's business which could be more easily serviced elsewhere.
(ii) An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.
(iii) Any transaction in which the counterparty to the transaction is unknown.

(vi) Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing capacity.

Any apparent unnecessary use of an intermediary in the transaction should give rise to further enquiry.

(vii) Potentially Suspicious Circumstances – Trust Companies

The following are examples of potentially suspicious circumstance which may give rise to a suspicion of money laundering in the context of Trust Companies.

Suspicious Circumstances Relating to the Customer/Client's behaviour:
(a) The establishment of Companies or Trusts which have no obvious commercial purpose.
(b) Clients/Customers who appear uninterested in legitimate tax avoidance schemes.
(c) Sales invoice totals exceeding the known value of goods.

(d) The client/customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, bankers drafts etc
(e) The customer/client pays either over the odds or sells at undervaluation. This includes the under-invoicing of exports and over-invoicing of imports.
(f) Customers/Clients have myriad of bank accounts and pay amounts of cash into all those accounts which, in total, amount to a large overall sum.
(g) Customers/clients transferring large sums of money to or from overseas locations with instructions for payment in cash (h). The payment into bank accounts of large third party cheques endorsed in favour of the client/customer.

Potentially Suspicious Secrecy may involve the following

a) The excessive or unnecessary use of nominees.
b) The unnecessary granting of wide ranging Powers of Attorney
c) The utilization of a client account rather than the payment of things directly.
d) An unwillingness to disclose the sources of funds
e) The use of a mailing address.
f) The unwillingness to disclose the identity of the ultimate beneficial owners or beneficiaries.

Suspicious Circumstances in Groups of Companies and/Trusts:

a) Companies which continually make substantial losses
b) Complex group structures without a cause
c) Subsidiaries which have no apparent purposes
d) A frequent turnover in shareholders, directors or trustees
e) Uneconomic group structure for tax purposes
f) The use of bank accounts in several currencies for no apparent reason
g) The existence of unexplained transfers of large sums of money through several bank accounts.
h) A medium sized corporate customer, shortly before going into voluntary liquidation, sells its prime asset at apparently less than market value. At around the same time less desirable assets are purchased by the company from interest which it is suspected are associated with the directors and at prices which according to your information are well in excess of their true value.
i) The payment of secret commissions.
j) Skimming of profits to executive directors.
k) Directors or management fraudulently acting against the interest of their company.
l) Payment of large management fees to entities associated with directors or management.

It should be noted that none of these factors on their own necessarily mean that a customer/client or any third party is involved in any money laundering. However, in most circumstances a combination of some of the above factors should arouse suspicion. In any event, what does or does not give rise to suspicion will depend on the particular circumstances.

APPENDIX F

EXAMPLES OF SUSPICIOUS TRANSACTIONS (FINANCING OF TERRORISM)

A. Accounts

(i) Accounts that receive periodic deposits after lying dormant for a long time. These accounts are then used to create a seemingly legitimate financial background through which additional fraudulent activities may be carried out.

(ii) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

(iii) When opening an account the customer refuses to provide information required by the financial institution, attempts to reduce the level of information which in the end is misleading or difficult to verify.

(iv) An account for which several persons have signing powers, yet these persons appear to have no relationship (either family ties or business relationship)

(v) An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signing powers, when there is no apparent economic or legal reason for such arrangement (for example, individuals serving as company directors for multiple companies with headquarters at the same location, etc.)

(vi) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits is made in comparison with the income of the founders of the entity.

(vii) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(viii) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization.

(ix) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organization and that shows movements of funds above the expected level of income.

B. Deposits and Withdrawals

(i) Deposits for a business entity in combinations of monetary instruments that are inconsistent with the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques).

(ii) Large cash withdrawals made from a business account not normally associated with cash transactions.

(iii) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

(iv) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

(v) Multiple transactions that do not appear to have any relation to the normal use of the account.

(vi) The structuring of deposits through multiple branches of the same financial institutions or by groups of individuals who enter a single branch at the same time.

(vii) The deposit or withdrawal of cash in amounts which fall consistently just below that which would trigger reporting or identification requirements.

(viii) The presentation of uncounted funds for a transaction such that upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

(ix) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds particularly if the instruments are sequentially numbered.

C. Wire Transfers

- ❖ Wire Transfers ordered in small amounts in an apparent effort to avoid triggering identification.
- ❖ Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transactions is conducted, is not provided with the wire transfer, when the inclusion of such information is expected.
- ❖ Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.
- ❖ Foreign exchange transactions that are performed on behalf of a customer by a third party followed by transfers of the funds to a location having no apparent business connection with the customer.

D. Characteristics of the customer or his/her business activity

(i) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

(ii) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self employed, e.t.c).

(iii) Stated occupation of the transctor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfer, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(iv) Regarding non-profit or charitable organizations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

(v) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(vi) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport and documents furnished to confirm name, address and date of birth).

E. Transactions Linked to locations of concern

(i) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example countries designated by national authorities. FATF non-cooperative countries and territories, e.t.c.)

(ii) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example countries designated by national authorities, FATF non-cooperative countries and territories, e.t.c)

(iii) A business account which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

(iv) The use of multiple accounts to collect and then channel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

(v) A customer obtains a credit instrument or engages in commercial financial transactions involving, movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

(vi) The opening of accounts of financial institutions from locations of specific concern.

(vii) Sending or receiving funds by international transfers from and/or to locations of specific concern.

SOURCES OF INFORMATION

(i) Anti-money Laundering Guidance Notes for the Finance Sector issued by the Jersey Financial Services Commission.

(ii) Guidance for Financial Institutions in detecting Terrorist Financing issued by the Financial Action Task Force. (FATF)

(iii) Customer Due Diligence for banks issued by the Basel Committee on banking Supervision.

(iv) FATF Member States.

(v) FATF Identification of Non-Cooperative Countries and Territories.

(vi) Guide to Fit and Proper issued by the Mauritius Financial Services Commission

ANNEXURE 1

EXAMPLES OF SUSPICIOUS TRANSACTIONS / ACTIVITIES

Unusual characteristics or activities and changes in bank transactions

(i) Cash deposits relating to transactions that would normally be settled by cheque. For example corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

(ii) Request to exchange large quantities of low denominations for higher denominations.

(iii) Requests for cheque clearance of large sums.

(iv) Matching payments out with credits paid in by cash on the same or previous day.

(v) Significant turnover in large denomination bills uncharacteristic for the bank's (or branch's) location.

(vi) Rapid increase in size and frequency of cash deposits without any corresponding increase in non-cash deposits.

(vii) A customer who suddenly pays up a large problem loan with no reasonable explanation of the source of funds.

(viii) A depositor who purchases money orders with large amounts of cash.

(ix) Mixing of cash deposits and monetary instruments in an account which such transactions do not appear to have any relation to the normal use of the account.

(x) Where the customer's stated purpose for a loan does not make economic sense.

(xi) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals running down the transferred amount.

(xii) An account for which several persons are signatories, yet the persons appear to have no relation among each other (either family ties or business relationship).

(xiii) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(xiv) *Non- profit or charitable organizations* - Financial transactions for which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Funds transfer activities……

(xv) The sending or receipt of frequent or large volumes of wire transfers to and from offshore institutions

(xvi) Customers transferring large sums of money to or from overseas with specific requests for payment in cash.

(xvii) International transfers for accounts with no history of such transfers or where the stated business of the customer does not warrant such activity.

(xviii) Significant changes in currency shipment patterns between correspondent banks.

(xix) Deposits that are followed within a short time by wire transfers of funds to or through a location of specific concern , such as a country with lax controls

Insufficient or suspicious information…….

(xx) A business that is reluctant to provide complete information regarding the purpose of the business or details of business activities, prior banking relationships, directors, or the location of the business.

(xxi) A business that is reluctant to provide details about its activities or to provide financial statements.

(xxii) A business that provides financial statements those are noticeably different from those of similar businesses.

(xxiii) A customer who is unwilling to provide personal background information.

(xxiv) A customer who has no record of past or present employment on a loan application.

(xxv) A customer who has no record of past or present employment but makes frequent large transactions.

Attempts to avoid reporting or record keeping requirements……

(xxvi) A customer who is reluctant to provide information required for identification, and record keeping purposes.

(xxvii) A customer who does not give details on record of past or present employment on a loan application form.

(xxviii) A customer who attempts to coerce a bank employee to not file required record keeping or reporting forms.

(xxix) A customer who requests for exemption from reporting or other requirements.

(xxx) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

Banking institution employees…..

(xxxi) An employee whose lavish lifestyle cannot be supported by his salary.

(xxxii) Reluctance by an employee to take a vacation.

(xxxiii) Mysterious disappearances or unexplained shortages of significant amounts of bank funds.

The above list is not intended to be all inclusive.

ANNEXURE 2

MINIMUM Contents of Suspicious TRANSACTION / Activity Report

(I) Reporting Banking Institution Information

(xxxiv) Name and address of institution
(xxxv) Name and address of Branch where the activity occurred

(ii) Suspect Information

(xxxvi) Full Names or Name of Entity
(xxxvii) Address
(xxxviii) Phone Number - Residence - Work
(xxxix) Occupation / Type of business
(xl) Date of birth

(xli) *Forms of identification* - National registration number
- Valid Passport Number
- Zimbabwean Driver's License
(xlii) Relationship to financial institution (Employee, Director, Officer, Shareholder, Customer etc.)

(iii) Description of the suspicious activity

(xliii) Type of transaction
(xliv) Amount involved
(xlv) Other details necessary to understand the transaction

(iv) Action already taken

(xlvi) If an insider is involved what action has been taken?
(xlvii) Has any law enforcement agency been advised? If yes, provide name of agency, name and telephone number of person(s) contacted, and by what method (telephone, written communication, etc)

(v) Contact person

(xlviii) Full names
(xlix) Title / Designation
(l) Contact telephone number

(vi) Date of suspicious transaction and date of preparation of report

NOTES