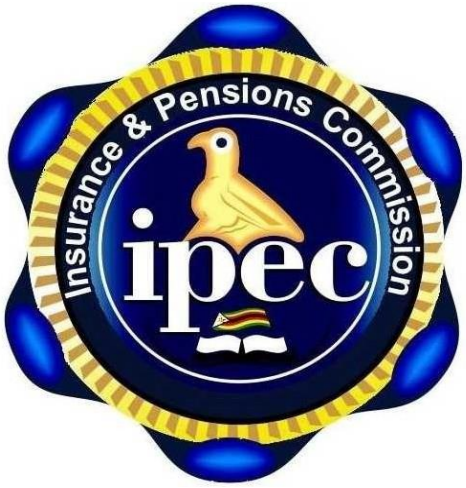
INSURANCE AND PENSIONS COMMISSION



GUIDELINE ON ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING

FOR THE

INSURANCE AND PENSIONS INDUSTRY IN ZIMBABWE

August 2023

`

Disclaimer

This Guideline is for guidance purposes only and not intended to be an exhaustive manual. For detailed and exhaustive guidance, players are required to refer to Financial Action Task Force (FATF) forty (40) Recommendations, the Money Laundering and Proceeds of Crime Act, related legislation and directives.

`

Contents

`

`

ABBREVIATIONS

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CPF	Countering Proliferation Financing
DNFBP	Designated Non-Financial Business or Profession
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
IPEC	Insurance and Pensions Commission
KYC	Know Your Customer
ML	Money Laundering
MLPC-Act	Money laundering and Proceeds of Crime Act [Chapter 9:24]
PEP	Politically Exposed Person
PF	Proliferation Financing
RBS/RBA	Risk Based Supervision/Risk Based Approach
RBZ	Reserve Bank of Zimbabwe
S.I.	Statutory Instrument
STR	Suspicious Transaction Reports
TF	Terrorism Financing
UBO	Ultimate Beneficial Owner
UNSCR	United Nations Security Council Resolutions

`

1. INTRODUCTION

1.1 This Guideline on "**Anti-money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing**" has been issued by the Insurance and Pension Commission (hereinafter referred to as IPEC or the Commission) in terms of section 3(3) of Money Laundering and Proceeds of Crime Act *[Chapter 9:24]*. IPEC is a competent supervisory authority in terms of Part 11(10) of the First Schedule of the Money Laundering and Proceeds of Crime Act *[Chapter 9:24]*.

1.2 The Guideline sets out the relevant anti-money laundering and combating the financing of terrorism and proliferation financing (AML/CFT/CFP) statutory and regulatory requirements, and the AML/CFT/CPF standards which registered insurers, reinsurers, intermediaries, and pension funds, (hereinafter referred to as "registered entities"), should meet to comply with the statutory provisions of the MLPC Act *[9:24]*.

1.3 The content of this Guideline is not intended to be an exhaustive way of meeting the statutory and regulatory requirements. Registered entities should therefore use this Guideline as a basis to develop measures most suited to their structure and business activities.

2. OBJECTIVES OF THE GUIDELINE

The objectives of the Guideline are to:

(a) provide a general background on money laundering, terrorist financing and proliferation financing (ML/TF/PF);

(b) provide the main provisions of the AML/CFT/CPF legislation relevant to registered entities in Zimbabwe;

(c) assist insurance and pension entities to establish a risk-based approach in their AML/CFT/CPF framework; and

(d) provide practical guidance to assist registered entities and their senior management in designing and implementing their own policies, procedures and controls, taking into consideration their special

`

circumstances, so as to meet the relevant AML/CFT/CPF statutory and regulatory requirements.

3. SCOPE OF APPLICATION AND EFFECTIVE DATE

3.1 This Guideline applies to all life insurance companies, reinsurance companies, brokers and agents for life and investment related products, pension funds and fund administrators, that are licensed and supervised by IPEC under the Insurance Act [Chapter 24:07] and Pensions and Provident Fund Act [Chapter 24:09].

3.2 Registered entities that fail to comply with this Guideline shall be liable to penalties and other stringent disciplinary actions under the MLPC Act [9:24] for the non-compliance.

3.3 The Guideline shall take effect immediately.

4. DEFINITION OF KEY TERMS

4.1 The following definitions of terms are set out in section 2, section 13 and section 16 of the Money Laundering and Proceeds of Crime Act.

Term	Definition
Beneficial Owner (or Ultimate Beneficial Owner)	Refers to the natural person(s) who ultimately owns or controls the rights to or benefits from property, including a person who exercises ultimate effective control over a legal person or arrangement.
Designated Non-Financial Business or Profession (DNFBP)	Refers to a Designated Non-Financial Business or Profession as defined in section 13 of the MLPC Act and include (a) the legal practitioners (b) accountants (c) estate agents (d) casinos (e) precious stone and precious metal dealers (f) Trust and Company Service Providers and (g) car dealers.

`

Financial Institution	The FATF and MLPC Act definitions as they relate to insurance and pensions industry refers to any person who conducts as a business one or more of the following activities for or on behalf of a customer: (a) investing, administering, or managing funds or money on behalf of other persons. (*b*) underwriting and placement of life insurance and other investment-related insurance, including insurance intermediation by agents and brokers. (c) the provision— A. or transfer of ownership, of a life insurance policy or the provision of reinsurance in respect of any such policy; or B. of investment-related insurance services; or C. of services as or by means of insurance underwriters, insurance agents or insurance brokers. For full definition refer to ***Section 2 of the MLPC Act***
High risk clients	Refer to customers classified as high risk such persons previously reported by the entity/intermediary to the FIUs or who operate in a higher risk industry or profession from an AML/CFT perspective. This includes persons active in charities and non-profit organization, precious metals and stone dealers, money services businesses, cash intensive businesses such as "cash for gold" or casinos, arms dealers.
Legal arrangements	Refers to express trusts or other similar legal arrangements.
Legal persons	Any entities, other than natural persons, that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include

`

	companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities.
Money Laundering Offence	Means the conversion or transfer of proceeds of crime for the purpose of (a) disguising the illicit origin of such property; or (b) assisting any person involved in the commission of a serious offence to evade the consequences of his / her illegal act or omission. (Section 9 of the MLPC Act)
Money Laundering risk	The risk that a country, financial institution or business unit could be used for money laundering
Proliferation financing	Means the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Politically Exposed Person (PEPs)"	Refers to: (a) Domestic PEPs – i.e., individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or of government, senior politicians, senior government officials, judiciary or military officials, senior executives of state-owned corporations and senior political party officials. (b) Foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or of government, senior politicians, senior government officials, judicial or

`

	military officials, senior executives of state-owned corporations and senior political party officials. (c) Persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the board or equivalent functions. (d) Immediate family members (such as parents, children, siblings or spouses) or associates of persons referred to in (a) to (c) above.
Terrorist Financing	Providing or collecting funds, or attempts to do so, with the intention that they should be used: (a) in order to carry out a terrorist act; or (b) by a terrorist; and (c) by a terrorist organisation.
Terrorist Financing risk	The risk that a country, financial institution or business unit could be used for Terrorism Financing.
Wire transfer	Refers to a transaction carried out by an institution (the ordering institution) on behalf of another person (the originator) by electronic means with a view to making an amount of money available to that person or another person (the recipient) at an institution (the beneficiary institution).

`

5. INTERNATIONAL AML/CFT/CPF FRAMEWORK

5.1 The Financial Action Task Force (FATF) is an inter-governmental body established in 1989. The objectives of the FATF are to set international standards and promote effective implementation of legal, regulatory, and operational measures for combating of ML, TF, PF, and other related threats to the integrity of the international financial system.

5.2 The FATF has developed a series of Recommendations that are recognized as the international standards for combating of ML, TF, and PF. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field.

5.3 The FATF monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, to ensure full and effective implementation of the standards at global level. The process includes identifying high-risk and other monitored jurisdictions which could be subjected to enhanced scrutiny by the FATF, or countermeasures by the FATF members and the international community at large. Some countries are direct members of FATF whilst other counties are associate members through affiliation in any of nine (9) FATF Style Regional Bodies (FSRBs). The main task of FSRBs is to set up systems for combating money laundering, financing of terrorism and proliferation in their respective regions.

5.4 Zimbabwe is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), which is an FRSB.

5.5 Periodically, ESAAMLG assesses Zimbabwe's technical compliance and effectiveness in implementing international AML/CFT standards on behalf of FATF. Zimbabwe is obliged to implement the FATF 40 Recommendations. It is important that Zimbabwe complies with the international AML/CFT/CPF standards to maintain its ability to transact on the international financial system. Details on the FATF 40 recommendations can be obtained from the following link: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

`

6. MONEY LAUNDERING AND TERRORIST FINANCING LEGISLATION IN ZIMBABWE

6.1 The main pieces of legislation in Zimbabwe that relate to ML, TF, PF, and financial sanctions are as follows:

- Money Laundering and Proceeds of Crime Act [Chapter 9:24]
- Suppression of Foreign and International Terrorism Act *[Chapter 11:21]*.
- S.I. 76 of 2014 on the implementation of the United Nations Security Council Resolutions (UNSCR): -
    - 1267 and its Successor Resolutions
    - 1373 and its Successor Resolutions
- S.I. 110 of 2021 on Suppression of Foreign and International Terrorism Implementation of UNSCR 1540 – Proliferation of weapons of mass destruction.

7. THE NATURE OF MONEY LAUNDERING AND TERRORIST FINANCING

7.1 The term "*money laundering*" (ML) is defined in section 8 of the MLPC Act *[*Chapter 9:24] and section 4 of this guideline.

7.2 There are three stages involved in the laundering of money, albeit in most cases involving numerous transactions. The stages are:

(a) *Placement* - the physical disposal of cash proceeds derived from illegal activities into the financial system including insurance and pensions.

(b) *Layering* - separating illegal proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, erasing any paper trail and providing anonymity; and

(c) *Integration* - creating false impression of legitimate funds or wealth. In situations where the layering process succeeds, integration leads to the return of the laundered proceeds back into the general financial system as if the funds were generated from legitimate business activities.

A registered entity should be alert to any such signs for potential criminal activities.

7.3 The term "terrorist financing" (TF) is defined in section 9 of the MLPC Act and section 4 of this guideline.

7.4 Unlike ML, which focusses on the handling of "dirty money" or criminal proceeds (i.e., the source of property is what matters), the focus of TF is on the destination or use of property, which may have been sourced from legitimate sources.

Vulnerabilities in the Insurance Industry

7.5 The insurance industry is vulnerable to ML, TF and PF risks. The inherent characteristics of some insurance products may give rise to ML risks unique to the insurance industry.

7.6 When a life insurance policy matures or is surrendered, funds become available to the policy holder or specified beneficiaries e.g., trustee (where policy has been placed in trust); an assignee, where the policy has been assigned).

7.7 The beneficiary to the contract may be changed for payment before maturity or surrender, in order that payments can be made by the insurer to a new beneficiary.

7.8 A policy might be used as collateral to purchase other financial instruments. These investments may contribute to a sophisticated web of complex transactions with their origins elsewhere in the financial system.

ML, TF and PF in Life Insurance Policies

7.9 The type of long-term insurance contracts that are vulnerable as a vehicle for laundering money or financing terrorism include products such as:

(a) unit-linked or with profit single premium contracts.
(b) single premium life insurance policies that store cash value.
(c) fixed and variable annuities; and
(d) endowment policies.

`

ML, TF, and PF Using Reinsurance

7.10 ML, TF, and PF using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements, and captives or by the misuse of normal reinsurance transactions. Examples include:

- the deliberate placement via the insurer of the proceeds of crime or terrorist property with reinsurers to disguise the source of funds.
- the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding.
- the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist property with legitimate reinsurers.

ML, TF, and PF Using Insurance Intermediaries

7.11 Insurance intermediaries are important for distribution, underwriting and claims settlement. They are often the direct link to the policy holder thus playing an important role in AML/CFT/CPF. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not conform to necessary procedures, or who fails to recognize or report information regarding possible cases of ML or TF. The intermediaries themselves could have been set up to channel illegitimate funds to insurers.

7.12 In addition to the above cases, an authorised entity should also give due consideration to the ML/TF/PF threats and vulnerabilities in the insurance industry identified in the 2019 National Risk Assessment.

Red Flags in the Insurance and Pensions Industry

7.13 The insurance and pensions products can be used to launder money through the following ways:

i) Acceptance of payments or receipts from third parties;

ii) Acceptance of very high value or unlimited value payments or large volumes of lower value payments;

`

iii) Acceptance of payments made in cash or money orders;
iv) Acceptance of frequent payments outside a normal premium policy or payment schedule;
v) Acceptance of funds to be used as collateral for a loan and/or written in a discretionary or other increased risk trust;
vi) Products that accept high amount lump sum payments, coupled with liquidity features;
vii) Acceptance and placement of cross-border insurance business in Zimbabwe that is inward and outward-bound reinsurance by reinsurance companies;
viii) Selling units in investment-linked products such as annuities;
ix) Using insurance proceeds from an early policy surrender to purchase other financial assets;
x) Buying of policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer e.g., second hand endowment and bearer insurance policies; and
xi) Buying of products with insurance termination features without concern for the product's investment performance, among others.

`

8. RISK-BASED APPROACH

8.1 The risk-based approach (RBA) is central to the effective implementation of an AML/CFT/CPF regime. An RBA to AML/CFT/CPF means that registered entities are expected to identify, assess, and understand the ML/TF/PF risks to which they are exposed and take AML/CFT/CPF measures commensurate with those risks to manage and mitigate them effectively.

8.2 RBA allows an entity to allocate its resources more effectively and apply preventive measures that are commensurate with the nature and level of risks to focus its AML/CFT/CPF efforts in the most effective way. Therefore, an entity should adopt an RBA in the design and implementation of its AML/CFT/CPF policies, procedures, and controls (hereafter collectively referred to as "AML/CFT/CPF Systems") with a view to managing and mitigating ML/TF/PF risks.

Institutional ML/TF/PF Risk Assessment

8.3 Section 12B of the MLPC Act requires that every financial institution assesses the money laundering and terrorist financing risks that it is exposed to and maintain records of such.

8.4 ML/TF/PF institutional risk assessment forms the basis of the RBA, enabling a registered entity to understand how and to what extent it is vulnerable to ML/TF/PF. The registered entity should conduct an institutional ML/TF/PF risk assessment to identify, assess and understand its ML/TF/PF risks in relation to:

(a) its customers;
(b) the countries or jurisdictions its customers reside;
(c) the countries the registered entity is operating in;
(d) the products and or services offered;
(e) mode of transactions; and
(f) delivery/distribution channels of the registered entity.

8.5 The institutional risk assessments should be informed by national risk assessment reports, typologies in the industry among other publications issued by the regulator.

`

8.6 When conducting institutional ML/TF/PF risk assessment the following considerations should be made:

(a) documenting the risk assessment process which includes the identification and assessment of relevant risks supported by qualitative and quantitative analysis, and information obtained from relevant internal and external sources.

(b) considering all the relevant risk factors before determining what the level of overall risk is, and the appropriate level and type of mitigation to be applied.

(c) obtaining the approval of senior management on the risk assessment results.

(d) having a process by which the risk assessment is kept up-to date; and

(e) having appropriate mechanisms to provide the risk assessment to IPEC or FIU when required to do so.

Factors to Consider in Conducting the Institutional ML/TF/PF Risk Assessment

8.7 In conducting the institutional ML/TF/PF risk assessment, an entity should cover a range of factors, including:

(a) Customer risk factors, for example:

i) its target market and customer segments.

ii) the number and proportion of customers identified as high risk.

(b) Geographic or cross border risk factors, for example:

i) the countries or jurisdictions it is exposed to, either through its own activities or the activities of customers or intermediaries especially countries or jurisdictions identified by credible sources, with relatively higher level of corruption or organized crime, and/or not having effective AML/CFT/CPF regimes. The following are some of the examples of credible sources country information: *https://bit.ly/1RA355J* *https://indexbaselgovernance.org/* *http://unodc.org/, https://www.knowyourcountry.com/*

(c) Products risk, for example:

`

i) the nature, scale, diversity and complexity of its business.

ii) the characteristics of products and services offered, and the extent to which they are vulnerable to ML/TF/PF abuse.

iii) the volume and size of its transactions.

(d) Delivery/distribution channel risk covers the delivery/distribution channels, including the extent to which the registered entity:

i) deals directly with the customer,

ii) relies on (or is allowed to rely on) third party to conduct customer due diligence (CDD),

iii) uses technology, and

iv) the extent to which these channels are vulnerable to ML/TF/PF abuse.

(e) Other risk factors, for example:

i) the nature, scale, and quality of available ML/TF/PF risk management resources, including appropriately qualified staff with access to ongoing AML/CFT/CPF training and development;

ii) compliance and regulatory findings; and

iii) results of internal or external audits.

8.8 The scale and scope of the institutional ML/TF/PF risk assessment should be commensurate with the nature, size and complexity of the business being undertaken.

8.9 The institutional ML/TF/PF risk assessment should consider any higher risks identified in other relevant risk assessments which may be issued from time to time, such as ML/TF/PF National Risk Assessment and any higher risks as notified by IPEC or the FIU.

8.10 Locally incorporated entities with branches or subsidiaries, including those located outside Zimbabwe, should perform a group-wide ML/TF/PF risk assessment.

8.11 If an entity is a part of a financial group and a group-wide or regional ML/TF/PF risk assessment has been conducted, it may refer to or rely on

`

those assessments provided that the assessments adequately reflect ML/TF/PF risks posed to the entity in the local context.

8.12 To keep the institutional ML/TF/PF risk assessment up to date, a registered entity should conduct its assessment annually and/or upon trigger events which are material to its business and risk exposure such as new products, business practices and use of technologies.

New Products, New Business Practices and Use of New Technologies

8.13 A registered entity should identify and assess the ML/TF/PF risks that may arise in relation to:

(a) the development of new products and new business practices, including new delivery/distribution mechanisms; and

(b) the use of new or developing technologies for both new and pre-existing products.

8.14 Risk assessment should be undertaken prior to the launch of new products, new business practices, or the use of new or developing technologies, and entities should take appropriate measures to manage and mitigate the risks identified.

8.15 The risk assessment report must be submitted to the Commission during the application for approval for a new product, business practice and technologies for review.

Customer Risk Assessment

8.16 A registered entity shall assess the ML/TF/PF risks associated with a proposed business relationship, which is usually referred to as a customer risk assessment. Customer risk is the likelihood that a particular customer or type of customer will make use of the products or services of the business to commit money laundering or to finance terrorism or proliferation. The assessment conducted at the initial stage of the CDD process would determine the extent of CDD measures to be applied.

8.17 Some customers present higher risks than others. The following types of customers would, in most cases, pose a high inherent risk:

`

(a) Politically exposed persons (PEPs);
(b) High net worth individuals;
(c) Legal persons and legal arrangements with unnecessarily complex structures or opaque ownership; and
(d) Shelf companies.

8.18 The amount and type of information obtained, and the extent to which this information is verified, should be increased where the ML/TF/PF risks associated with the business relationship are higher whilst it may also be simplified where the ML/TF/PF risks associated with the business relationship is lower. The risk assessment conducted will also assist the entity to distinguish between the risks of individual customers and business relationships including the application of appropriate CDD and risk mitigating measures.

8.19 A registered entity should classify its customers by risk levels, i.e., Low Risk, Medium Risk and High Risk (or any similar risk scoring method). Results of the risk assessment will then determine the level and type of ongoing monitoring (including ongoing CDD and transaction monitoring). As the customer risk profile changes over time, an entity should review and update the risk assessment of a customer from time to time, particularly during ongoing monitoring.

8.20 A registered entity should adopt an RBA in the design and implementation of its customer risk assessment framework, and the complexity of the framework should be commensurate with the nature and size of its business informed by the results of institutional ML/TF/PF risk assessment.

8.21 Records and relevant documents of customer risk assessments should be maintained so that an entity can be able to demonstrate to IPEC or FIU:

(a) how it assesses the customer's ML/TF/PF risks;
(b) the extent of CDD measures; and
(c) the appropriateness any ongoing monitoring activities based on the particular customer's ML/TF/PF risks.

`

9. AML/CFT/CPF CONTROLS, GOVERNANCE AND MONITORING

9.1 A registered entity should take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF/PF and to prevent any contravention of the MLPC Act requirements.

9.2 To ensure compliance, an entity should implement appropriate AML/CFT/CPF systems in accordance with the RBA.

9.3 An entity should implement AML/CFT/CPF systems having regard to the nature, size and complexity of its businesses and the ML/TF/PF risks arising from those businesses.

9.4 A registered entity should:

i) have internal AML/CFT/CPF systems, which are approved by the board and senior management, to enable it to effectively manage and mitigate the risks that are relevant to the institution;

ii) monitor the implementation of those AML/CFT/CPF systems and to improve them if necessary; and

iii) take appropriate measures to manage and mitigate the risks where higher risks are identified.

9.5 The nature, scale, and complexity of AML/CFT/CPF systems may be simplified provided that:

i) the basis for such simplification should be a result of a risk assessment whose findings proved low ML/TF/PF risks (i.e., institutional ML/TF/PF risk assessment); and

ii) simplified AML/CFT/CPF systems, which are approved by senior management, must be subject to review from time to time.

9.6 However, AML/CFT/CPF systems are not permitted to be simplified whenever there is a suspicion of ML/TF/PF.

COMPLIANCE MANAGEMENT PROGRAMMES

9.7 A registered entity should have appropriate compliance management arrangements that enables it to implement AML/CFT/CPF systems to comply with relevant legal and regulatory obligations, as well as, to manage ML/TF/PF risks effectively.

`

9.8 Section 25 of the Act prescribes a set of requirements that are recognized as the pillars of an AML/CFT/CPF Compliance Program. It requires financial institutions and DNFBPs to have the following in place:

(a) Internal procedures, policies and controls to fulfil the requirements of the Act;

(b) Appointment of a compliance officer, at senior management level, who is responsible for day-to-day AML/CFT/CPF compliance;

(c) Employee screening;

(d) Ongoing AML/CFT/CPF training program for staff;

(e) Independent audit to review and verify effectiveness of the measures in place to comply with the requirements of the Act;

Role of the Board and Senior Management

9.9 Effective ML/TF/PF risk management requires adequate governance arrangements. The board and senior management of a registered entity should have a clear understanding of its ML/TF/PF risks and ensure that the risks are adequately managed. Information regarding ML/TF/PF risks and the AML/CFT/CPF Systems should be communicated to them in a timely, complete, understandable and accurate manner in order to make informed decisions.

9.10 The Board and senior management must be compliant with the Risk Management and Corporate Governance Guidelines issued by IPEC.

9.11 An appropriate board committee either on Audit and or Compliance must have oversight of the AMC/CFT/CPF matters.

9.12 The board and senior management of an entity is responsible for implementing effective AML/CFT/CPF Systems to manage the ML/TF/PF risks identified and ensure that sufficient compliance resources are in place to meet the requirements of its' AML/CFT/CPF compliance programme.

9.13 The senior management should appoint an AML/CFT/CPF Compliance Officer at management level to have the overall responsibility for the

establishment and maintenance of the entity's AML/CFT/CPF Systems and the central reference point for suspicious transaction reporting.

9.14 While responsibility for the consistency and effectiveness of AML/CFT/PF controls rests with the AML/CFT compliance officer, the execution of these controls is conducted by first line operational staff and is the responsibility of senior and operational management.

9.15 Senior management is responsible for approving measures needed to mitigate ML/TF/PF risks, determining the level of residual risk the life insurer or intermediary is prepared to accept; and adequately resource the life insurer's or intermediary's AML/CFT function.

A. AML/CFT/CPF Policies and Procedures

9.16 An AML/CFT/CPF policy sets out the entity's high-level commitment to implementing measures to combat money laundering and terrorism financing in line with the requirements of the MLPC Act.

9.17 The AML/CFT/CPF procedures, on the other hand, detail the processes to guide staff on the implementation of the various key AML/CFT/CPF obligations set out in the Act, including the following –

(i) Risk assessment;

(ii) Customer due diligence, including enhanced customer due diligence and transaction monitoring for high-risk customers, including Politically Exposed Persons; and

(iii) Detection and reporting of suspicious transactions.

9.18 As best practice, policies and procedures should:

A. Consider national or sectoral risk assessments to ensure control processes address the level and types of ML/TF/PF risk in their geographic region;

B. Place priority on the products, services, distribution, customers, and geographic locations that are more vulnerable to abuse, e.g., high premium, cash value products, non-resident policies or products that offer tax advantages to proposers or investors;

C. Provide for regular review of the risk assessment and risk management processes;

D. Ensure that adequate risk assessment and controls are in place before new products are offered;

E. Inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and relevant regulatory reporting (e.g., suspicious transaction reports (STRs);

F. Focus on meeting all appropriate regulatory record keeping and reporting requirements;

G. Be updated regularly to take into account regulatory and operational developments;

H. Enable the timely identification and filing of STRs; and

I. Provide for adequate supervision of employees who handle customer onboarding, transactions (including non-financial transactions such as assignments), management reporting, grant exemptions, monitoring of suspicious activity, or engage in any other activity that forms part of the business's AML/CFT/CPF programme.

B. AML/CFT Compliance Officer

9.19 The principal function of the AML/CFT Compliance Officer is to act as the focal point within an institution for the oversight of all activities relating to the prevention and detection of ML/TF/PF as well as providing support and guidance to the board and senior management on ML/TF/PF risk management measures and obligations.

9.20 In order that the AML/CFT/CPF Compliance Officer discharges his or her responsibilities effectively, an entity should, ensure that the AML/CFT/CPF Compliance Officer is:

i) appropriately qualified with sufficient AML/CFT/CPF knowledge;

ii) not conflicted on AML/CFT/CPF issues and, if possible, independent of all operational and business functions;

iii) ordinarily resident in Zimbabwe;

iv) of sufficient level of seniority and authority within the organisation;

`

v) provided with regular direct access to senior management to ensure that senior management are satisfied that the statutory obligations are being met and that the business is taking sufficient effective measures to protect itself against ML/TF/PF risks;

vi) fully conversant with the organisation's statutory and regulatory requirements and the ML/TF/PF risks arising from its business;

vii) capable of timely accessing all available information (both from internal sources such as CDD records and external sources such as directives from the IPEC or FIU); and

viii) equipped with sufficient resources, including staff when absent from official duty (i.e., an alternate or deputy AML/CFT/CPF Compliance Officer who should, where practicable, have the similar status).

9.21 The AML/CFT Compliance Officer's responsibilities include:

(a) developing and reviewing the entity's AML/CFT/CPF Systems, including any group-wide AML/CFT/CPF Systems, to ensure they remain up to date, meet current statutory and regulatory requirements, and are effective in managing ML/TF/PF risks arising from its business;

(b) overseeing all aspects of the organisation's AML/CFT/CPF Systems including monitoring effectiveness and enhancing the controls and procedures where necessary;

(c) communicating key AML/CFT/CPF issues with board and senior management, including, where appropriate, significant compliance deficiencies;

(d) ensuring AML/CFT staff training is adequate, appropriate and effective;

(e) acting as the main point of contact with the FIU and law enforcement agencies;

(f) identification and reporting of suspicious transactions;

`

(g) review of internal documents using available relevant information, determining whether or not it is necessary to make a report to the FIU;

(h) maintenance of all records related to such internal reviews; and

(i) provision of guidance on how to avoid tipping off.

C. Employee Screening

9.22 A registered entity should have adequate and appropriate screening procedures to ensure that only fit and proper staff are recruited when hiring employees. *Section 25(1)(b) of the MLPC Act*.

D. Staff Training Obligations

9.23 It is the registered entity's sole responsibility to provide adequate training for its staff guided by the following pointers:

(a) The scope and frequency of training should be tailored to the specific risks faced by the organisation;

(b) The course content should also be sensitive to the job functions, responsibilities, and experience of the staff.

(c) New staff should be required to attend initial training as urgent as possible soon after being hired or appointed.

(d) A registered entity should also provide refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF/PF.

9.24 A registered entity should implement a clear and well-articulated policy for ensuring that relevant staff receive adequate AML/CFT/CPF training. Staff should be made aware of:

(a) their organisation's and their own personal statutory obligations and the possible consequences for failure to comply AML/CFT/CPF requirements under the MLPC Act which include customer due diligence, recordkeeping, suspicious transactions, and threshold reporting;

`

(b) their organisation's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under United Nations Security Council Resolutions namely:

- 1267 and its Successor Resolutions
- 1373 and its Successor Resolutions

(c) any other statutory and regulatory obligations that concern their organisation and the possible consequences of breaches of these obligations;

9.25 Training should be designed to cater for various roles and duties being performed by staff members within the entity.

9.26 A registered entity should consider using a mix of training techniques and tools in delivering training, depending on the available resources, and learning needs of their staff. These techniques and tools may include on-line learning systems, focused classroom training, relevant videos as well as paper or intranet-based procedures manuals. A registered entity may consider including available FATF papers and typologies as part of the training materials. The registered entity should be able to demonstrate to IPEC that all materials are up-to date and in line with current requirements and standards.

9.27 A registered entity should maintain records of who has been trained, when the staff received the training and the type of the training provided. Ideally these training records should be maintained for a minimum of 5years.

9.28 A registered entity should monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of the organisation's policies and procedures to combat ML/TF/PF, the understanding of the statutory and regulatory obligations, and their ability to recognize suspicious transactions;

(b) monitoring the compliance of staff with the organisation's AML/CFT/CPF Systems;

(c) the quality and quantity of internal reports so that further training needs may be identified, and appropriate action can be taken; and

(d) monitoring attendance and following up with staff who miss such training without reasonable cause.

E. Independent Audit function

9.29 A registered entity should establish an independent audit function which should have a direct line of communication to the senior management of the organisation. The function should have sufficient expertise and resources to enable it to carry out its responsibilities, including independent reviews of the entity's AML/CFT/CPF Systems.

9.30 The audit function should regularly review the AML/CFT/CPF Systems to ensure effectiveness. The review should include, but not be limited to:

(a) adequacy of the entity's AML/CFT/CPF Systems, ML/TF/PF risk assessment framework and application of RBS;

(b) effectiveness of suspicious transaction reporting systems;

(c) effectiveness of the compliance function; and

(d) level of awareness of staff having AML/CFT responsibilities.

9.31 The frequency and extent of the review should be commensurate with the nature, size and complexity of its businesses and the ML/TF/PF risks arising from those businesses. Where appropriate, the entity should also seek a review from external parties.

Group Wide AML/CFT/CPF Systems

9.32 A registered entity with cross-border branches or subsidiary undertakings that carry on the same business as a financial institution as defined in the MLPC Act should implement group-wide AML/CFT/CPF systems to apply the requirements set out in this Guideline to all its foreign branches and subsidiary undertakings in its financial group (*Section 25 (4) to (6) of the MLPC Act*).

`

9.33 A locally-incorporated entity should, through its group-wide AML/CFT/CPF systems, ensure that all of its foreign branches and subsidiary undertakings that carry on the same business as a financial institution as defined in the MLPC Act, have procedures in place to ensure compliance with the CDD and record-keeping requirements similar to those imposed in the MLPC Act, to the extent permitted by the laws and regulations of that place.

9.34 An entity should (through its group-wide AML/CFT/CPF systems) also provide for:

(a) sharing information required for the purposes of CDD and ML/TF/PF risk management; and

(b) provision to the registered entity's group-level compliance, audit and/or AML/CFT functions, of customer, account, and transaction information from its foreign branches and subsidiary undertakings that carry on the same business as an FI as defined in the MLPC Act, when necessary for AML/CFT/CPF purposes.

9.35 If the AML/CFT/CPF requirements in the host jurisdiction of the foreign branch or subsidiary are different to local requirements, the registered entity should require that branch or subsidiary to apply the higher of the two sets of AML/CFT/CPF requirements, to the extent that host jurisdiction's laws and regulations permit.

9.36 If the host jurisdiction's laws and regulations do not permit the branch or subsidiary to observe local AML/CFT/CPF standards, a registered entity shall apply the higher AML/CFT/CPF requirements, particularly the CDD and record-keeping requirements imposed in the MLPC Act. The registered entity should:

(a) document the different requirements;

(b) inform the IPEC of such failure;

(c) take additional measures to effectively mitigate ML/TF/PF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the requirements.

`

9.37 The institutional risk assessment should include all the different countries requirements within their vulnerability assessment.

10. CUSTOMER DUE DILIGENCE

A. IDENTIFICATION AND VERIFICATION OF THE CUSTOMER'S IDENTITY

10.1 All registered entities are required in terms Section 15 of the MLPC Act to identity every one of their customers and verify the customer's identity by means of an identity document when:

(a) opening an account for or otherwise establishing a business relationship with a customer; or

(b) the customer, who is neither an account holder nor in an established business relationship with the entity, wishes to carry out a transaction in an amount equal to or exceeding five thousand United Sates dollars or equivalent of local or other foreign currencies (or such lesser or greater amount as may be prescribed, either generally or in relation to any class of financial institution), whether conducted as a single transaction or several;

(c) transactions that appear to be linked; or

(d) doubts exist about the veracity or adequacy of previously obtained identity documents; or

(e) there is a suspicion of money laundering or financing of terrorism involving the customer or the customer's account.

Sources of Identification

10.2 An identity document means:

(a) a document issued to a person in terms of section 7(1) or (2) of the National Registration Act [Chapter 10:17], or a passport or drivers licence issued by or on behalf of the Government of Zimbabwe; or

(b) any visitor's entry certificate or other certificate or permit issued to a person in terms of the Immigration Act [Chapter 4:02], or in terms of any enactment relating to refugees; or

(c) any passport, identity document or drivers licence issued by a foreign government.

Identification of a Natural Person

10.3 For a customer that is a natural person, a registered entity should identify the customer by obtaining at least the following identification information:

(a) full name;
(b) date of birth;
(c) nationality; and
(d) copy of national identification document (e.g., copy of identity card, valid passport or driver's licence).

NB: The identification document obtained by a registered entity should contain a photograph of the customer.

Identification of Legal persons

10.4 For a customer that is a corporate body/legal person, a registered entity should identify the customer by obtaining at least the following identification information:

(a) Copy of a certified certificate of incorporation or registration
(b) Copy of a partnership agreement or deeds;
(c) Copy of constitutional document for a trust;
(d) Names and addresses of the directors or members of the board or other governing body and copies of their national identity certificates;
(e) Copy of memorandum and articles of association of a corporate body or equivalent documents constituting the corporate body;
(f) Names and addresses of the founding members, shareholders or stakeholders of the corporate body and copies of their national identity certificates;
(g) Full name of corporate body;
(h) Date of incorporation, establishment or registration; and

(i) Principal place of business (if different from the address of registered office).

10.5 In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, a registered entity should satisfy itself as to the legitimate purpose of the organization, e.g., by requesting sight of the constitution.

Identification of a Trust and other Legal Arrangements

10.6 In respect of trusts, a registered entity should identify and verify the trust as a customer in accordance with the requirements set out in 10.4 above. The registered entity should also regard the trustee as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust. In such a case, the registered entity should identify and verify the identity of the trustees and beneficiaries of the trust.

10.7 For a customer that is a trust or other similar legal arrangement, a registered entity should identify the customer by obtaining at least the following identification information:

(a) name of the trust or legal arrangement;
(b) date of establishment or settlement;
(c) the jurisdiction whose laws govern the trust or legal arrangement;
(d) unique identification number (if any) granted by any applicable official bodies and document type (e.g., tax identification number or registered charity or non-profit organization number); and
(e) address of registered office (if applicable).

Reliability of Documents, Data, or Information

10.8 In verifying the identity of a customer, a registered entity needs to apply risk-based supervision principles. A registered entity needs to establish accuracy of only the most critical identification documents rather than the entire list of identification particulars submitted. However, a registered entity should ensure that documents, data, or information obtained for

`

the purpose of verifying the identity of a customer is current at the time they are submitted.

10.9 If a natural person customer or a person representing a legal person, a trust or other similar legal arrangement is physically absent during the CDD process, the registered entity should take appropriate measures to ensure the reliability of identification such as requesting copies of identity documents for the registered entity's records including the authorised representative's copy of personal identification documents.

10.10 Where the documents, data or information being used for the purposes of identification are in a foreign language, appropriate steps should be taken by the registered entity to be reasonably satisfied that the documents, data. or information in fact provide evidence of the customer's identity.

Identification and Verification of a Person Purporting to Act on Behalf of the Customer

10.11 If a person is an authorised representative of the customer, a registered entity should identify the person and take reasonable measures to verify the person's identity.

10.12 A registered entity should verify the authority of such authorised representative by appropriate documentary evidence (e.g., board resolution, affidavit or similar written authorization).

B. IDENTIFICATION AND VERIFICATION OF A BENEFICIAL OWNER

10.13 A registered entity should identify any beneficial owner in relation to a customer and take reasonable measures to verify the beneficial owner's identity so that the registered entity is satisfied that it knows who the beneficial owner is.

10.14 In determining what constitutes reasonable measures to verify the identity of a beneficial owner of a customer, a registered entity should consider and give due regard to the ML/TF risks posed by the customer and the business relationship.

`

10.15 Where a natural person is identified as a beneficial owner, the registered entity should endeavour to obtain copies of identification information as far as possible.

Beneficial Owner in Relation to a Natural Person

10.16 In respect of a customer that is a natural person, there is no requirement on a registered entity to make proactive searches for beneficial owners of the customer except upon payment of benefits.

10.17 The registered entity should only make appropriate enquiries where there are indications that the customer is not acting on his own behalf.

Beneficial Owner in Relation to a Legal Person

10.18 A registered entity should identify any natural person who ultimately has a significant or controlling ownership interest in the legal person and any natural person exercising control of the legal person or its senior management and take reasonable measures to verify their identities.

10.19 A registered entity may obtain an undertaking or declaration from the customer on the identity of, and the information relating to, its beneficial owner. Nevertheless, in addition to the undertaking or declaration obtained, the registered entity should take reasonable measures to verify the identity of the beneficial owner (e.g., verifying with publicly available information).

10.20 If the ownership structure of a customer involves different types of legal persons or legal arrangements, in determining who the beneficial owner is, a registered entity should pay attention to the individual who has ultimate ownership or control over the customer, or who constitutes the controlling mind and management of the customer.

Beneficial Owner in Relation to a Trust or Other Similar Legal Arrangement

10.21 A registered entity should identify the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership) and take reasonable measures to verify their identities.

`

10.22 For a beneficiary of a trust, a registered entity should obtain sufficient information concerning the beneficiary to satisfy the registered entity that it will be able to establish the identity of the beneficiary at the time of paying out or when the beneficiary intends to exercise their vested rights.

C. IDENTIFICATION AND VERIFICATION OF A BENEFICIARY

10.23 Whenever a beneficiary is identified or designated by the policy holder of an insurance policy, a registered entity should verify:

(a) if the beneficiary is identified by name, record the name of the beneficiary;

(b) if the beneficiary is designated by description (e.g., under a will), obtain sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary:

i) at the time the beneficiary exercises their rights under the insurance policy; or

ii) at the time of pay-out or, if there is more than one pay-out, the time of the first pay-out to the beneficiary in accordance with the terms of the insurance policy whichever is the earlier.

10.24 Where the beneficiary is a natural person, take reasonable measures to verify the person's identity.

If Beneficiary is A Legal Person or Trust or Other Similar Legal Arrangement

10.25 Where the beneficiary is a legal person or trust or other similar legal arrangement, a registered entity should identify its beneficial owners.

10.26 If there is a high risk of ML or TF due to the particular circumstances of the beneficial owners, the entity must take reasonable measures to verify the beneficial owners' identities so that the registered entity knows who the beneficial owners are.

If Beneficiary is a Politically Exposed Person or High-Risk Customer

10.27 If the beneficiary is a politically exposed person or any similarly higher risk client, a registered entity should:

(a) inform senior management before the pay-out of the policy proceeds;

(b) conduct enhanced scrutiny on the whole business relationship with the policy holder; and

(c) consider making a suspicious transaction report.

Beneficiaries Who Are Not Directly Linked to the Customer

10.28 As a general rule, if payments made under the terms of the policy are to be paid to persons or companies other than the customers or beneficiaries, then the proposed recipients of these moneys should also be subjected identity verification.

Requirements for Reinsurance Companies

10.29 Reinsurers are subject to the CDD, and record-keeping requirements set out in Sections 13-26 of MLPC Act.

10.30 The customers in relation to whom the reinsurers should carry out the CDD measures are the ceding insurers and reinsurance brokers.

Purpose and Intended Nature of Business Relationship

10.31 A registered entity should understand the purpose and nature of the requested business relationship. The registered entity shall obtain information in this regard using proposal forms or any other means which is most relevant to the risk profile of the customer (including legal persons such as trusts and corporates) and its nature of business.

https:www.fatf-gafi.org/media/fatf/documents/Best-practices-Beneficial-Ownership-Legal-Person.pdf.

`

11. TIMING OF VERIFICATION OF CUSTOMER IDENTIFICATION PARTICULARS

(Section 16 of MLPC Act)

11.1 Depending on the risk profile of the customer, timing of identity verification can be varied.

(a) If the customer is high risk in nature, customer identification and beneficial ownership should be done before the business transaction is effected.

(b) If, however, customer is low risk in nature, customer identification and beneficial ownership can be done after the business transaction is done on condition that:

i) there are effective policies and procedures to manage any risk of ML/TF/PF arising from the delayed verification of the customer's or beneficial owner's identity;

ii) it is undesirable to interrupt the normal conduct of business with the customer for example in life assurance, identification and verification can be delayed but should occur at or before the time of paying out.

Conditions Applicable in Cases of Delayed Customer Identification

11.2 Appropriate risk management policies and procedures should already be in place in cases where registered entity opts to effect customer identification after establishing the business transaction. These policies and procedures should include:

(a) pre-authorised reasonable timeframe for the completion of the identity verification measures and any necessary appropriate including conditions under which the business relations can be suspended or terminated or reported to the FIU;

(b) clear pre-authorised limits on the number, types and/or amount of transactions that can be performed before verification;

(c) documented procedures for the monitoring and possible reporting of suspicious transactions which are inconsistent with the normal occupation of the customer;

(d) frequency and timing of escalation to senior management of any pending verification cases; and

(e) ensuring that no payments are made to any third party, with an exception for cases where:

i) there is no suspicion of ML/TF/PF;

ii) the risk of ML/TF/PF is assessed to be low;

iii) the payment is approved by senior management after due diligence was carried out in relation to the nature of the customer's business; and

iv) the recipients of the funds are neither PEPs nor appear on the UN Security Council blacklist or local watch lists.

11.3 If identity verification cannot be completed within the reasonable timeframe set in the entity's risk management policies and procedures, the entity should terminate the business relationship as soon as reasonably practicable and refrain from carrying out further transactions (except to return funds or other assets in their original forms as far as possible).

12. SIMPLIFIED DUE DILIGENCE (SDD)

(Section 15-19 of MPLC Act)

12.1 In general, a registered entity shall carry out all CDD measures before entering a business transaction as well as carrying out ongoing obligations of monitoring the business relationship using risk-based measures.

12.2 After carrying out a commensurate risk assessment and establishing that the business contract presents a low ML/TF/PF risk, the registered entity may apply SDD measures.

12.3 SDD measures shall be discontinued where:

(a) the registered entity's risk assessment concludes that ML/TF/PF risk is now high;

(b) the ML/TF/PF risk is yet to be proven, but the registered entity now suspects ML or TF or PF; or

(c) the accuracy of documents or information previously supplied is now in doubt.

12.4 To enhance effectiveness, any categorisation to "low risks" should be demonstrated by an appropriate analysis of ML/TF/PF risks by the registered entity.

12.5 The SDD measures applied should be commensurate with the nature and level of ML/TF/PF risk, based on the lower ML/TF/PF risk factors identified by the registered entity. Documentation on the analysis conducted to demonstrate the low risk must be maintained and reviewed periodically.

12.6 Even when a registered entity used SDD measures, the obligations to continuously monitor its business contracts still apply (i.e., ongoing CDD and transaction monitoring) in line with section 24-27 of the MLPC Act.

12.7 Examples of potentially lower risk factors include:

(a) Customer risk factors:

i) public bodies such as a government entity or quasi government body, local authority, municipal council in Zimbabwe or in an equivalent jurisdiction;

ii) a corporation listed on a stock exchange(s) which impose adequate disclosure requirements to ensure transparency of beneficial ownership; or

iii) financial institution as defined in the MLPC Act in Zimbabwe established in an equivalent jurisdiction and is subjected to mandatory compliance with AML/CFT/CPF requirements consistent with standards set by the FATF.

(b) Product, service, transaction, or delivery/distribution channel risk factors:

i) a pension or provident fund, retirement scheme set up for the provision of retirement benefits to employees, where contributions to the scheme is payroll-based and the scheme does not have extra voluntary contributions OR the rules disallow assignment of a member's interest under the scheme;

`

ii) an insurance policy that does not contain a surrender clause and cannot be used as a collateral; or

iii) a life insurance policy in respect of whose benefits are very low below the bulk-cash limit imposed by the FIU.

(c) Country risk factors:

i) countries or jurisdictions with effective AML/CFT/CPF Systems as identified by credible sources, such as FATF and FATF-Style bodies; or

ii) countries or jurisdictions identified by credible sources as having a lower level of corruption or other criminal activity.

12.8 Examples of possible SDD measures include:

i) relaxing the frequency of updates of customer identification information;

ii) reducing the degree of ongoing scrutiny of transactions below a reasonably low monetary threshold; or

iii) not querying to understand the purpose and intended nature of the business relationship. Instead, registered entity regards the purpose and intended nature of transactions to be consistent with normal business activities of the customer.

13. ENHANCED DUE DILIGENCE (EDD)

(Section 19-20 of MLPC Act)

13.1 A registered entity shall apply EDD measures to a business transaction with a high ML/TF risk to mitigate and manage the risk where:

(a) the customer is a politically exposed person;

(b) the customer is not physically present;

(c) customer comes from a blacklisted or grey-listed jurisdiction;

(d) customer is specified by the FIU and is on local watch list; and

(e) as guided by regulations and from the FIU from time to time.

`

13.2 A registered entity should apply risk-based approach when using EDD measures. The measures applied shall always be proportionate with the nature and level of ML/TF/PF risk factors identified by the registered entity.

13.3 To establish or continue with a business relationship that is a high ML/TF/PF risk, a registered entity should obtain approval from its senior management.

13.4 A registered entity should conduct enhanced monitoring of a business relationship that presents a high ML/TF/PF risk continuously, for example, by increasing the number and timing of controls applied. In addition, a registered entity, shall also isolate and select the appropriate types and patterns of transactions that need further scrutiny.

13.5 Examples of potentially higher risk factors include:

(a) Customer risk factors:

i) customer who appears on the sanctioned or watch list;

ii) cash intensive business;

iii) companies that have nominee shareholders or shares in bearer form;

iv) the customer or the beneficial owner of the customer is a politically exposed person;

v) Transaction with shell companies that does not have a clear legitimate commercial purpose;

vi) Insurance transaction is conducted in unusual circumstances (e.g., business from unusual geographic regions transacted between the customer and the registered entity);

vii) Business from legal persons with an unusually complex ownership structure.

(b) product, service, transaction, or delivery/distribution channel risk factors:

i) huge cash transactions which are inconsistent with the usual occupation of the customer

ii) frequent payments received from unknown third parties; or

iii) anonymous transactions (which may involve cash).

(c) Country risk factors:

i) countries, jurisdictions, or geographical areas identified by credible sources like FATF as providing funding or support for terrorist activities, or that have designated terrorist organizations operations; or

ii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or

iii) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML/CFT/CPF Systems; or

iv) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

Examples of Possible EDD Measures

13.6 The following measures can be done independently or jointly if they are proportionate and appropriate to the ML/TF/PF risk:

(a) obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;

(b) obtaining information on the source of wealth or source of funds of the customer;

(c) obtaining additional information on the intended nature of the business relationship;

(d) obtaining information on the reasons for intended or performed transactions; or

(e) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

`

14. POLITICALLY EXPOSED PERSONS (PEPs)

(*Section 20 of MLPC Act*)

14.1 PEPs are a special class of customers, who are deemed, by law, as presenting a high money laundering risk, arising from the power and influence they wield, which can, potentially be abused for personal enrichment through corruption and embezzlement. A full definition of PEPs is given under Section 13 of the Act (see table on definition of terms).

14.2 Section 20(1) (b) of the Act requires that a registered entity should have in place measures to identify if a customer or a beneficial owner is a politically exposed person be it domestic or foreign.

14.3 If a customer or beneficial owner is identified as a PEP, enhanced due diligence measures must be applied.

14.4 Effective procedures and processes should be put in place for determining whether a customer (or beneficial owner) of a customer is a foreign PEP e.g., through referring to open sources of information and or using third-party consultants to screen out possible foreign PEPs. An entity may use publicly available information such as relevant reports and databases on corruption risk published by national, international, non-governmental and commercial organizations to determine countries which are most vulnerable to corruption e.g., Transparency International's 'Corruption Perceptions Index.

14.5 A registered entity should apply the EDD measures in any of the following situations:

(a) before doing business with a customer who is or whose beneficial owner is a domestic PEP or an international organization PEP;

(b) when continuing an existing business contract with a customer who is or whose beneficial owner is a domestic PEP or an international organization PEP where the relationship subsequently becomes high risk;

(c) when continuing an existing high risk business relationship where the registered entity subsequently knows that the customer or the

beneficial owner of the customer is a domestic PEP or an international organization PEP.

(d) If a domestic PEP or an international organization PEP is no longer entrusted with a prominent public function, a registered entity shall use a risk-based assessments not necessarily dependant on the time that the customer has been relieved from the public office.

14.6 Possible risk factors to consider include:

i) the seniority of the position that the individual held as a PEP.

ii) The level of informal influence that the individual still possesses.

iii) Whether previous functions of the PEP had any influence (formally or informally) to the appointment of the PEPs successor.

iv) Whether current functions of the PEP had any influence (formally or informally) to the appointment of the PEPs successor.

14.7 For any such decisions outlined above, the registered entity should obtain approval from its senior management.

Source of Wealth

14.8 Source of wealth refers to the predominant origin of the PEP's total assets not necessarily related to the business transaction in question. Whilst this is an indicator of how the individual acquired their wealth, it is also a reliable sign of the size of his wealth.

14.9 Although it may be hard to get the complete information, a registered entity should proceed to gather general supporting information from the individual, commercial databases, or other open sources to establish source of wealth.

Source of Funds

14.10 Source of funds is defined as the origin of specific money which is directly connected to the business contract (business relationship) between an individual and the registered entity (e.g., the amounts being invested, deposited, or wired as part of the business relationship) including the specific activity that generated the funds. The information obtained should be enough to connect the funds to their origin and proving that

`

the funds are legitimate otherwise it should be reported to the FIU as a suspicious transaction.

14.11 For non-PEP customers, financial institutions and DNFBPs have the obligation to assess the ML/TF/PF risk and decide each customer's risk category, e.g., low, medium, or high risk. PEPs, however, are, by law, automatically deemed as high risk and financial institutions and DNFBPs do not have the discretion to assess the risk differently.

N/B: *International organizations referred above are entities established by formal political agreements between their member states that have the status of international treaties; their existence is recognized by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations are World Bank, International Monetary Fund, World Health Organisation and United Nations.*

15. CUSTOMER NOT PHYSICALLY PRESENT FOR IDENTIFICATION PURPOSES

(Section 19 (1) and (2) of MLPC Act)

15.1 The MLPC Act recognises instances where a registered entity can do business with customers who are not physically present for purposes of identification. To ensure smooth conduct of business, a registered entity should ensure that appropriate ML/TF/PF risk mitigation measures are in place for all customers who are not physically present for identification purposes.

15.2 When a customer is not present for identification purposes, the registered entity should mitigate the ML/TF/PF risks posed through any applicable ways which are most effective including:

(a) verifying the customer's identity through open sources including the internet;

(b) verifying the customer's identity from independent data sources such as the registrar of births and deaths, registrar of companies and deeds among others;

`

(c) Use of intermediaries or other third parties to verify the customer's identity; or

(d) ensuring that the first premium payment made by the customer from a bank account in the customer's name with an authorized bank or institution legally operating in an equivalent/foreign jurisdiction that has measures in place to ensure compliance with requirements similar to the local AML/CFT laws. Such a foreign bank should be supervised for compliance with those requirements by a banking regulator in that jurisdiction.

N/B: *In carrying out the above measures or any other most effective risk mitigation measures, the registered entity should always be able to demonstrate to the IPEC or FIU that the additional customer identification measure(s) taken adequately addresses the risk of impersonation by the unidentified customer.*

16. RELIANCE ON CUSTOMER DUE DILIGENCE PERFORMED BY INTERMEDIARIES

General Use of Intermediaries

16.1 Licenced insurers, reinsurers, individual insurance agents, licensed multiple agencies and insurance broker companies all have the responsibility to comply with the requirements relating to CDD in line with MLPC Act. However, intermediaries are normally the first line of defence as they meet the customers well before the customer is known, introduced, or referred to an authorized insurer.

16.2 A registered entity may rely upon its intermediaries (brokers and agents) to perform its CDD measures under the MLPC Act. However, the ultimate responsibility for such CDD requirements rests with the registered entity.

16.3 The insurer shall ensure that all its intermediaries have adequate processes and procedures in place to prevent ML and TF by ensuring that:

(a) the CDD procedures of its intermediaries are equivalent with its own and are implemented in an identical manner to its own standards;
(b) the insurer is satisfied that its intermediaries possess the reliable procedures which comply with the applicable CDD requirements.
(c) the insurer shall capacitate its intermediaries on CDD issues (and AML/CFT/CPF in general).

16.4 When relying on an intermediary, a registered entity should:
(a) obtain written confirmation from the intermediary that the intermediary agrees to act as the registered entity's intermediary and perform the CDD measures required by the MLPC Act and regulations; and
(b) be satisfied that the intermediary will provide any CDD information to the registered entity on demand.

16.5 A registered entity should conduct sample tests from time to time to ensure CDD information and documentation is timely produced by the intermediary upon demand.

16.6 Whenever a registered entity has doubts about the reliability of the intermediary, it should review and correct any deficiencies discovered in the intermediary's CDD duties. In situations where the registered entity intends to terminate its intermediary agreement with the broker or agent, it should immediately obtain, review, and redo all CDD information from the intermediary including correcting any identified deficiencies.

International/Overseas Intermediaries

16.7 A registered entity may rely upon an overseas intermediary carrying on business in an equivalent jurisdiction to perform any part of the CDD measures set in section 14-22 of the MLPC Act, provided the intermediary:
(a) resides in an equivalent jurisdiction to that of IPEC/FIU/ESAAMLG and is subjected to compliance requirements similar to the local AML/CFT/CPF standards by an authority similar to those of IPEC or its equivalent regulatory body(ies).

(b) an institution that carries on a business similar to that carried on by a registered entity or financial intermediary and is registered under the law of that jurisdiction concerned.

(c) has policies and procedures in place to ensure compliance with AML-CFT-CPF requirements similar to those imposed locally.

Related Foreign Financial Institutions as Intermediaries

16.8 A registered entity may also use a related foreign financial institution (related foreign branch, head-office, associated company, bank etc) to perform CDD measures on its behalf provided the related foreign institution:

(a) Carries on, in a place outside Zimbabwe, a business similar to that carried on by a registered entity or intermediary FI; and falls within the following categories:

i) it is within the same group of companies as the registered entity;

ii) if the registered entity is incorporated in Zimbabwe, it is a branch of the registered entity;

iii) if the registered entity is incorporated outside Zimbabwe:

(A) it is the head office of the registered entity; or

(B) it is a branch of the head office of the registered entity;

(b) Is required under group policy:

i) to have measures in place to ensure AML/CFT/CPF compliance in a similar manner to local requirements; and

ii) to implement programmes against ML/TF/PF.

Failure to Satisfactorily Complete Customer Due Diligence

(Section 28 of the MLPC Act)

16.9 Where the registered entity is unable to comply with relevant CDD requirements set out in the Act and the ongoing due diligence requirements, it should not enter into an insurance relationship with the customer and or de-risk (terminate business relationship as soon as

`

reasonably practicable), and where reasonable, make an STR to the FIU for investigation.

16.10 Failure to do the above attracts a jail term of 3years or a fine of USD$100,000 or both such fine and jail term. The penalty may be applied on the entity, its' directors, principal officer, employees, or agents.

17. PROHIBITION OF ANONYMOUS ACCOUNTS

(*Section 14 of MLPC Act*)

17.1 A registered entity should not maintain anonymous insurance accounts or those in fictitious names for any new or existing customer. The registered entity should always perform its due diligence duties through effective identification and verifications of all its customers in accordance with the MLPC Act and this Guideline.

17.2 In all cases, all customer identification and verification records should be available on demand by authorities such as IPEC, FIU, law enforcement agencies among others.

17.3 Failure to do the above attracts a jail term of 3 years or a fine of USD$100,000 or both such fine and jail term (section 23). The penalty may be applied on the entity, its' directors, principal officer, employees, or agents.

18. EQUIVALENT JURISDICTION

18.1 Equivalent jurisdiction means a jurisdiction that imposes AML/CFT/CPF requirements and standards similar to those imposed locally.

18.2 A registered entity may need to assess and determine for itself which jurisdictions other than other FATF members apply requirements and standards similar to those imposed locally for jurisdictional equivalence purposes. The registered entity should document its assessment of the jurisdiction and may consider the following factors among others:

(a) whether the jurisdiction concerned is a member of ESSAMLG or other FATF-style regional bodies and recent mutual evaluation report published by the FATF-style regional bodies;

(b) whether the jurisdiction concerned is identified by the FATF as having strategic AML/CFT/CPF deficiencies and the recent progress of improving its AML/CFT/CPF regime;

(c) any advisory circular issued by IPEC or FIU from time to time alerting registered entities to jurisdictions with poor AML/CFT/CPF controls;

(d) any other AML/CFT/CPF-related publications published by specialized national, international, non-governmental or commercial organizations.

18.3 Because the AML/CFT/CPF regime of a jurisdiction changes over time, a registered entity should review the jurisdictional equivalence assessment on a regular basis and/or upon trigger events.

18.4 A directive prescribing jurisdictions that the Director of the FIU considers to be compliant jurisdictions may be issued from time to time.

19. ONGOING CUSTOMER DUE DILIGENCE AND MONITORING

19.1 Ongoing monitoring is an essential component of effective AML/CFT/CPF Systems. A registered entity should continuously monitor its business relationship with a customer in two aspects (1) ongoing CDD and (2) transaction monitoring.

19.2 Ongoing CDD refers to periodic reviewing of on-file documents, data and information relating to the customer that have been obtained by the registered entity for the purpose of complying with CDD and EDD with a view to make sure that they are up-to-date, accurate and relevant.

19.3 Transaction monitoring involves:

i) Conducting appropriate scrutiny of financial transactions carried out for the customer to ensure that they are consistent with the registered entity's knowledge of the customer, the customer's business, risk profile and source of funds.

`

ii) Identifying suspicious transactions that are complex, unusually large in amount or of a suspicious pattern, have no apparent economic or lawful purpose.

iii) Examining the background and purposes of those transactions and setting out the findings.

A. ONGOING CDD

19.4 To ensure on-file documents, data and information of a customer are current and relevant, a registered entity should periodically review its existing CDD records of customers or upon some trigger events occurring. Clear policies and procedures should be developed, especially on the frequency of periodic review or a clear definition of a trigger event.

19.5 Trigger events may include the following events:

(a) when the registered entity realises that it has insufficient information about the customer;

(b) when a huge cash transaction is due to occur;

(c) when the registered entity's customer identification details changes substantially; and

(d) when the way the customer's insurance account is operated changes materially.

Customer Due Diligence on Pre-Existing Customers

19.6 A registered entity should perform the CDD measures under the MLPC Act and this Guideline in respect of pre-existing customers where:

(a) a suspicious transaction which is inconsistent with the occupation or business profile of the customer occurs;

(b) the registered entity doubts the authenticity and adequacy of any previously obtained information for the purpose of customer identification;

(c) a material change occurs in the way in which the customer's account is operated; or

(d) the registered entity suspects that the customer is involved in ML/TF/PF.

19.7 All customers that present high ML/TF/PF risks should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary by the registered entity, to ensure the CDD information retained remains up-to-date and relevant.

B. TRANSACTION MONITORING

(Section 26 (1b) and (2) of MLPC Act)

Transaction Monitoring Systems and Processes

19.8 A registered entity should put in place and maintain systems and processes to properly monitor transactions. Transaction monitoring systems and processes should be set up taking into consideration the following factors:

(a) the nature of the products and services provided;

(b) Delivery channels in use and modes of communication;

(c) the size and complexity of its business;

(d) the ML/TF/PF risks arising from its business;

(e) the nature of its systems and controls;

(f) the monitoring procedures that are already in existence to satisfy other business needs such as proposal forms.

N/B: *There are various methods by which these objectives can be met including exception reports (e.g., large transactions exception report or manual spreadsheets).*

19.9 A registered entity should put in place measures to ensure that the transaction monitoring systems and processes are accessible to all the relevant staff to enable them to perform transaction monitoring analysis, investigation, and risk mitigation timely and with sufficient information.

19.10 A registered entity should ensure that the transaction monitoring systems and processes can support the ongoing monitoring of insurance contracts including possibility of analysis of transaction information per customer, customer type or intermediary basis.

`

19.11 In designing transaction monitoring systems and processes, including setting of parameters and thresholds, a registered entity should consider the transaction characteristics, which may include:

(a) the nature and type of transactions (e.g., abnormal size or frequency);

(b) the nature of a series of transactions (e.g., structuring a single transaction into a number of cash deposits);

(c) the counterparties of transactions;

(d) the geographical origin/destination of a payment or receipt; and

(e) the customer's normal account activity or turnover.

N/B: *A regulated entity should regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including parameters and thresholds adopted. The parameters and thresholds should be properly documented and independently validated to ensure that they are appropriate to its operations and context.*

Risk-Based Approach (RBA) to Transaction Monitoring and Review of Transactions

19.12 A registered entity should conduct transaction monitoring in relation to all its business relationships in line with the principles of RBA. The frequency and intensity of monitoring should depend on the ML/TF/PF risk profile of the customer. In low-risk cases, the registered entity must reduce the extent of monitoring. On the other hand, where the ML/TF/PF risks are high e.g., a PEP customer, the registered entity should conduct enhanced transaction monitoring.

19.13 A registered entity should take appropriate steps such as examining the background and purposes of the transactions; (making appropriate enquiries to or obtaining additional CDD information from a customer) to identify if there are any grounds for suspicion, when:

(a) the customer's transactions are not consistent with the registered entity's knowledge of the customer, the customer's business, risk profile or source of funds; or

(b) the registered entity identifies transactions that (i) are complex, unusually large in amount or of an unusual pattern, and (registered entity) have no apparent economic or lawful purpose.

19.14 Where registered entity conducts enquiries and there are no grounds for suspicion, no further action may be taken updating the customer risk profile based on any relevant information obtained.

19.15 However, where the registered entity has reasonable grounds for suspicion, an STR should be filed with FIU.

19.16 A registered entity should note that proper enquiries done in good faith on customers does not constitute tipping off. However, if the registered entity reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The registered entity should document the basis for its assessment and file an STR to the FIU.

19.17 The above CDD process, the findings and outcomes should be properly documented in writing and be available on demand by the IPEC, FIU or other competent authorities and auditors.

19.18 Where cash transactions and transfers to third parties are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, a registered entity should approach such situations with caution and make relevant further clarification. Where the registered entity is satisfied that any cash transaction or third-party transfer is suspicious and unreasonable, it should make a suspicious transaction report (STR) to the FIU.

20. REPORTING OF SUSPICIOUS TRANSACTIONS

20.1 Section 30 (1) of MLPC Act requires that any person who knows or suspects that any property: (a)directly or indirectly represents any person's proceeds (b) was used in connection with, or (c) is intended to

`

be used in connection with ML/TF/PF activities must file an STR with the FIU within 3 days.

20.2 The STR should be made together with any evidence forming the basis of the knowledge or suspicion. Under the MLPC Act, any person who neglects or fails to file such an STI is liable for a fine of US $100 000 or to imprisonment for a period not exceeding three years, or both such fine and such imprisonment.

20.3 Knowledge includes:

(a) actual knowledge;

(b) knowledge of circumstances which would indicate convincing facts to a reasonable person; and

(c) knowledge of the true circumstances which would convince a reasonable person on inquiry.

20.4 Suspicion is subjective, relies on personal judgement or "gut feeling" and falls short of tangible proof and firm evidence. As far as a registered entity is concerned, when a transaction or a series of transactions of a customer is not consistent with the registered entity's knowledge of the customer, or is unusual (e.g., in a pattern that has no apparent economic or lawful purpose), the registered entity should take appropriate steps to further examine the transactions and identify if there is any suspicion.

Suspicious Transactions - Red Flags

20.5 The following are examples of situations which might give rise to suspicious transactions. More examples are provided in Annexure II.

(a) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;

(b) transactions, instructions, or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient, or secure way to do business;

(c) where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services

normally requested, or is outside the experience of the financial services business in relation to the particular customer;

(d) where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;

(e) where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;

(f) where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;

(g) the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services; and

(h) transfers to and from jurisdictions subject to a watch list by the FATF without reasonable explanation, which are not consistent with the customer's declared business dealings or interests.

(i) Cash payments on insurance policies.

(j) Use of multiple currency equivalents (e.g., cashier's checks and money orders) different sources to make insurance policy or annuity payments.

(k) Purchases of products that appear outside the customer's normal range of financial wealth or estate planning needs.

(l) Refunds requested during a policy's "legal cancellation period" or "free-look period."

(m) Policy premiums paid from abroad, especially from an offshore financial center.

(n) A policy calling for the periodic payment of premiums in large amounts.

(o) Changing the named beneficiary of a policy to a person with no clear relationship to the policyholder.

(p) Lack of concern for significant tax or other penalties assessed when cancelling a policy.

(q) Redemption of insurance bonds originally subscribed to by an individual in one country by a business entity in another country.

NB: *A registered entity should also be aware of elements of individual transactions and situations that might give rise to suspicion of terrorist financing in certain circumstances. The FATF and FIU publishes studies of methods and trends of terrorist financing from time to time, and registered entities may refer to the FATF website for additional information and guidance***.**

20.6 Once knowledge or suspicion has been formed:

(a) a registered entity should file an STR even where no transaction has been conducted by or through the registered entity; and

(b) the STR should be made within 3 working days after the suspicion was first identified.

Prohibition of Tipping Off

20.7 It is an offence to reveal to any unauthorised person any information which might prejudice an investigation. If the customer was told that a report has been made, this would prejudice the investigation and an offence would be committed. The tipping off provision includes circumstances where a suspicion has been raised internally within a registered entity but has not yet been reported to the FIU.

AML/CFT Systems in Relation to Suspicious Transaction Reporting

20.8 A registered entity should implement appropriate AML/CFT/CPF systems in order to fulfil its statutory reporting obligations, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR. The AML/CFT/CPF Systems should include:

(a) appointment of an AML/CFT Compliance Officer;

`

(b) implementing clear policies and procedures over internal reporting, reporting to the FIU, post-reporting risk mitigation and prevention of tipping off; and

(c) keeping proper records of internal reports and STRs.

20.9 A registered entity should have measures in place to check, on an ongoing basis, that its AML/CFT/CPF Systems comply with relevant legal and regulatory requirements as regards to suspicious transaction reporting and that the systems operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF/PF as well as the nature and size of its business.

Identifying Suspicious Transactions and Internal Reporting

20.10 A registered entity should provide adequate training and guidance to its staff to enable them to effectively form reasonable suspicion or to recognize the signs when ML/TF/PF is taking place. The guidance should be sensitive to various factors such as the type of product or service, type of customers, the nature of the transactions and customer instructions that staff is likely to encounter, and the means of service delivery.

20.11 A registered entity should have a transaction monitoring system.

20.12 A registered entity may adopt a "SAFE" approach, which involves:

(a) screening the account for suspicious indicators;

(b) asking the customers appropriate questions;

(c) finding out the customer's records; and

(d) evaluating all the above information.

20.13 A registered entity should put in place and maintain clear policies and procedures to ensure that:

(a) all staff are aware of the identity of the AML/CFT Compliance Officer and of the procedures to follow when making an internal report; and

(b) all internal reports should reach the AML/CFT Compliance Officer without unjustified delays for onward transmission to the FIU within 3 days whenever necessary.

`

20.14 A registered entity should avoid cumbersome reporting procedures and structures. In handling a suspicious case, the aim should be to involve a minimum number of staff as far as possible and the AML/CFT Compliance Officer. This ensures speed, confidentiality, and accessibility to the AML/CFT Compliance Officer.

20.15 Once a staff of the registered entity has reported suspicion to the AML/CFT Compliance Officer in accordance with the policies and procedures established by the registered entity for the making of such reports, the statutory obligation of the staff has been fully discharged.

20.16 The internal report should include adequate details of the customer in question and the relevant information giving rise to the suspicion.

20.17 The AML/CFT Compliance Officer should acknowledge receipt of an internal report and provide a reminder to the staff member about his obligation to ensure that there shall be no tipping off to the customer whatsoever.

20.18 When analysing the internal report, an AML/CFT Compliance Officer should consider all relevant information, including CDD and ongoing monitoring information available. This may include:

(a) making a review of other transaction patterns and volumes through connected accounts, preferably adopting a relationship-based approach rather than on a transaction-by transaction basis;

(b) making reference to any previous patterns of instructions;

(c) the length of the business relationship, and CDD and ongoing monitoring information and documentation; and

(d) appropriate questioning of the customer per the systematic approach to identify suspicious transactions recommended by the FIU.

N/B: *Upon completion of the assessment, if an AML/CFT Compliance Officer is convinced that there are grounds for suspicion, an STR shall be filed together with all relevant supporting grounds and evidence within three working days. Depending on when the suspicion arose, an STR may*

`

be made either before a suspicious transaction or activity occurs (whether the intended transaction ultimately takes place or not), or after a transaction or activity has been completed. The AML/CFT Compliance Officer should always make timely STRS to the FIU no later than 3 working days after forming the suspicion in terms of Section 30(1) of the MLPC Act even if there is further customer information, transactions or relationships to be further interrogated. This review process should be documented and supported with any conclusions drawn.

Reporting to the FIU

20.19 Section 33 of the MLPC Act exonerates an AML/CFT Compliance Officer from any criminal liability whenever he acts in good faith in filing an STR with the FIU. Similarly, no criminal liability attaches to AML/CFT Compliance Officer for genuinely deciding not to report if he or she prudently concludes that there are no grounds for suspicion after considering all available information. It is however vital for the AML/CFT Compliance Officer to keep proper records of the deliberations and actions taken to demonstrate he has acted in reasonable manner and in good faith.

20.20 In case where an extremely urgent reporting is required e.g., a suspected customer is pushing for immediate payment, a registered entity should indicate such further details in its STR including an initial notification by telephone or other swift means to the FIU.

20.21 A registered entity should also indicate its proposed risk mitigation measures as a recommendation to the FIU. Such a recommendation may include termination of the insurance relationship or freezing of the policy among other appropriate measures.

20.22 In all circumstances, a registered entity should ensure that STRs filed to the FIU, are comprehensive, factual, and well-supported by documents and quoting relevant guidance provided by the FIU in its directives or instructions.

Post Suspicious Transaction Reporting

`

20.23 Filing an STR to the FIU provides a registered entity with a sound legal defence against the ML/TF/PF offence disclosed in the STR, provided:

(a) the report is made before the registered entity undertakes the disclosed transaction or corrective measures;

(b) the transaction(s) or corrective measures are undertaken with the consent of the FIU; or

(c) the STR is made voluntarily by the registered entity within a reasonable time frame in cases where the suspicious transaction has already happened.

20.24 Filing of an STR should be followed by an appropriate review of a business relationship and applying appropriate risk mitigating measures irrespective of FIU feedback. In addition, approvals shall be requested from the registered entity's senior management on whether to continue with the business relationship as regards how to mitigate any potential legal or reputational risks posed by the relationship.

Record keeping of Suspicious Transaction Reports

20.25 A registered entity should maintain a record of all STRs made to the AML/CFT Compliance Officer.

Requests from Law Enforcement Agencies

20.26 A registered entity may receive various information requests from law enforcement agencies including search warrants, copies of identification documents or confiscation orders which are crucial to aid their investigations, restraining and confiscating illicit money or property.

20.27 Accordingly, a registered entity shall put in place clear policies and procedures to handle these requests timely and comprehensively e.g., allocation of enough resources and staff as the main point of contact with law enforcement agencies.

20.28 The policies and procedures shall also include measures to enable registered entity to freeze the relevant property or hand-over property to

`

law enforcement officers or comply with restraint orders subject to the laws of Zimbabwe.

21. UNITED NATIONS SECURITY COUNCIL RESOLUTIONS ON TERORRIST AND PROLIFERATION FINANCING

21.1 Registered entities are required to keep updated with the various resolutions passed by the United Nations Security Council (UNSC)on counter terrorism and proliferation financing measures these include:

- *1267 (1999 and successor resolutions);*
- *1373 (2001 and successor resolutions); and*
- *1540 (2004) and successor resolutions.*

21.2 These resolutions require financial institutions to identify and freeze assets of persons/entities listed on United Nations Security Council sanctions lists relating to financing of terrorism and financing of proliferation. Registered entities are required to screen all their customers and the customers' counterparties and ensure that they do not process a transaction connected with a sanctioned person/entity.

21.3 Although the FIU issues directives on UNSCR from time to time, registered entities are required to make reference to the sanctions lists on the UN website (below), as updated from time to time: https://www.un.org/securitycouncil/sanctions/1267.

21.4 Once a positive match is confirmed in the process of sanctions screening, reporting institutions must immediately and without delay:

(a) freeze the customer (or counterparty)'s funds or block the transaction (where applicable), if it is an existing customer;

(b) reject the potential customer if the transaction has not commenced;

(c) submit a suspicious transaction report; and

(d) inform the relevant supervisory authorities.

21.5 Reporting institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the sanctions list.

`

21.6 In practice, financial institutions subscribe to and make use of automated sanctions screening services from reputed sanctions to ensure every customer and every transaction is screened against the sanctions lists.

22. RECORD KEEPING

(Section 24 of MLPC Act)

22.1 Record keeping forms a paper trail of ML/TF/PF risks. Record keeping helps build ML/TF/PF history of funds, transactions, and assets in respect of the suspected person.

22.2 A registered entity should maintain CDD information enough to meet the recordkeeping requirements under the MLPC Act. The registered entity should ensure that:

(a) the paper trail for funds moving through the registered entity should cover both funds' transactions for both the customer and beneficial owner of the customer where necessary.

(b) All CDD information and transaction records must be availed to investigation agencies in a timely and complete fashion; and

(c) The records must demonstrate compliance with any requirements in this Guideline or as may be pronounced by the FIU from time to time.

Retention of records relating to CDD and transactions

22.3 A registered entity should keep:

(a) the original or a copy of identity documents of the customer and/or beneficial owner of the customer or persons who purport to act on behalf of the customer and/or other connected parties to the customer;

(b) all documents or records on file obtained in performing CDD measures and ongoing monitoring process, including SDD and EDD;

(c) original or a copy of proposal forms

(d) original or a copy of the policy schedule

(e) the original or a copy of the records of business correspondence between insurer and policy owner or beneficiaries

`

22.4 All documents and records mentioned above should be kept throughout the lifespan of the business relationship with the customer and for a period of at least five years after the end of the business relationship.

Records Kept by Intermediaries

22.5 Where customer identification and verification documents are held by an intermediary who carried out CDD measures, the registered entity is responsible for compliance with all record-keeping requirements. The registered entity should ensure that the intermediary being relied on has systems in place to comply with all the record-keeping requirements under the MLPC Act and this Guideline.

22.6 A registered entity should immediately obtain the data or information that the intermediary has obtained while carrying out CDD and EDD measures.

22.7 A registered entity should ensure that an intermediary will pass the documents and records to the registered entity, upon termination of the services provided by the intermediary.

Record-keeping Obligations by Licensed Individual Insurance Agents

22.8 Licensed individual insurance agents shall provide all customer and transaction related documentation to the insurer directly, as they do not have the capacity to maintain records Accordingly, individual insurance agents are considered to have deposited the required records and documents at the premises of the insurer.

22.9 The individual insurance agents remain responsible for compliance with all record-keeping requirements by way of ensuring that:

(a) the insurer to which they provide the records and documents has systems in place to comply with all the record-keeping requirements under the MLPC Act; and

(b) such records and documents are accessible from the insurer without delay upon request by the FIU or IPEC.

`

23. PENALTIES FOR NON-COMPLIANCE WITH AML/CFT/CPF OBLIGATIONS

23.1 Non-compliance by a registered entity with any of the AML/CFT obligations under the MLPC Act or the obligations relating to the implementation of Targeted Financial Sanctions under Statutory Instruments 76 of 2014 and 110 of 2021, as well as any breach of any Directive issued by the Financial Intelligence Unit, or the Supervisor can attract either criminal sanctions or civil penalties (or both).

23.2 The Commission is empowered by Section 5 of the MLPC Act to impose a range of civil, administrative sanctions and remedial actions for AML/CFT/CPF breaches which include the following:

(a) Written warning;

(b) A remedial order;

(c) Requirement to submit returns/ information for monitoring compliance;

(d) Fine up to US$250,000; and

(e) An order barring specified employees of a regulated entity from employment with the entity concerned either for a specified period or permanently.

23.3 Criminal and civil penalties are enforceable against the registered entity or against any of its employees, directors, or agents, as the case may be or against both the institution / business and the responsible individuals with the objective of ensuring compliance.

23.4 Enforcement actions can be instituted based on outcomes of onsite or offsite inspections or when the supervisor gets information from any other sources on possible non-compliance.

23.5 Annexure I provide a list of infringements that will result in the imposition of penalties, though it may not be exhaustive.

End of Guideline

`

`

ANNEXURE I: INFRINGEMENTS AS PER MONEY LAUNDERING AND PROCEEDS OF CRIME ACT

1.	Failure to take reasonable steps to identify the beneficial owner of funds or other property that is the subject matter of a transaction (s.15(3))
2.	Failure to comply with any obligations relating to customer identification and verification (s.15 to 18)
3.	Permitting a customer to open or operate an anonymous account or account under fictitious name (s. 14)
4.	Entering into or continuing a business relationship with a shell bank (s.14)
5.	Failure to take adequate measures as required under Section 19 of the Act when conducting a transaction with a customer who is not physically present.
6.	Failure to implement appropriate risk management systems to identify high risk customers (s. 20)
7.	Failure to implement appropriate risk management systems to determine if a customer or beneficial owner is a politically exposed person (s.20)
8.	Failure to obtain senior management approval before establishing a business relationship with a politically exposed person or to continue an already established business relationship once a customer or beneficial owner is identified as a politically exposed person.
9.	Failure to take all reasonable measures to identify the source of funds and wealth of a customer who is identified as a politically exposed person (s.20)
10.	Failure to exercise enhanced identification, verification, and ongoing due diligence in respect of high-risk customers (s.20)
11.	Failure to comply with any one or more of the requirements provided for in section 21 of the Act relating to correspondent banking relationships.
12.	Failure to comply with requirement of section 22 of the Act relating to obligations of financial institutions in the event of failure to fulfil customer identification and verification requirements.
13.	Failure to maintain books and records as required under section 24 of the Act
14.	Failure to timely avail to FIU, upon request, books or records referred to in Section 24 or any information contained therein (s. 28)

`

15. 16	Failure to develop and/ or implement programmes for the prevention of money laundering and terrorist financing under subsection (1) of Section 25 of the Act
17.	Failure to designate a compliance officer as required under subsection (2) of section 25 of the Act
18.	Failure to exercise ongoing due diligence and monitoring as required under section 26 of the Act
19.	Failure to comply with the requirements relating to wire transfers as set out in section 27 of the Act.
20.	Failure by a financial institution to ensure that its foreign branches or majority–owned subsidiaries implement the applicable requirements of the Act (S. 29)
21.	Failure to advise the FIU of the fact that laws of a foreign country, where a branch or majority –owned subsidiary of the institution is situated, prevent the branch or subsidiary from compliance with (s.29(2))
22.	Failure to report a suspicious transaction as required in terms of section 30 of the Act.
23.	Failure to submit cash transaction report as required in terms of a FIU Directive
24.	Disclosing to a customer or any third party that a suspicious transaction report has been, is being or will be submitted to the Unit or that a money laundering investigation has been, is being or will be carried out (s.31(2))
25.	Except as required or authorised in terms of the Act, disclosing any information that identifies or is likely to identify who prepare or made a suspicious transaction report or handled the underlying transaction (s. 32)
26	Failure to comply with any mandatory requirement of a circular, directive or guidelines issued in terms of the Act.

ANNEXURE II: INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing.
2. A sudden request for a significant purchase of a lump sum contract with an existing client whose current contracts are small and of regular payments only.

`

3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment.
4. A proposal to purchase and settle by cash.
5. The prospective client who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract.
6. A customer establishes a large insurance policy and within a short period of time cancels the policy, requests the return of the cash value payable to a third party.
7. Early termination of a product, especially in a loss.
8. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business.
9. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need.
10. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments.
11. A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.
12. A customer is reluctant to provide normal information when applying for an insurance policy, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify.
13. Delay in the provision of information to enable verification to be completed.
14. Opening accounts with the customer's address outside the local service area.
15. Opening accounts with names similar to other established business entities.
16. Attempting to open or operating accounts under a false name.
17. Any transaction involving an undisclosed party.

18. A transfer of the benefit of a product to an apparently unrelated third party.
19. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy).
20. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder.
21. The customer accepts very unfavourable conditions unrelated to his health or age.
22. An atypical incidence of pre-payment of insurance premiums.
23. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency.
24. The customer who is based in jurisdictions subject to a call by the FATF or in countries where the production of drugs or drug trafficking may be prevalent.
25. The customer who is introduced by an overseas agent, affiliator or other company that is based in jurisdictions subject to a call by the FATF or in countries where corruption or the production of drugs or drug trafficking may be prevalent.
26. A customer who is based in Zimbabwe and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency.
27. Unexpected changes in employee characteristics, e.g., lavish lifestyle or avoiding taking holidays.
28. Unexpected change in employee or agent performance, e.g., the sales person selling products has a remarkable or unexpected increase in performance.
29. Consistently high activity levels of single premium business far in excess of any average company expectation.

`

30. The use of an address which is not the client's permanent address, e.g., utilization of the salesman's office or home address for the despatch of customer documentation.
31. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. (For individual customers, consider customer's age, occupation, residential address, general appearance, type, and level of previous financial activity. For corporate customers, consider type and level of activity.)
32. Any unusual employment of an intermediary in the course of some usual transaction or financial activity e.g., payment of claims or high commission to an unusual intermediary.
33. A customer appears to have policies with several institutions.
34. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.