GUIDANCE TO FINANCIAL INSTITUTIONS AND DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS ON THE RISK BASED APPROACH TO IMPLEMENTATION OF ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM OBLIGATIONS

January 2021

This guidance supersedes and replaces the ***Guidelines on Anti-Money Laundering and Combating Financing of Terrorism, of 2006***

Contents

DEFINITIONS

These definitions must be read together with the definitions set out in section 2, section 13 and section 16 of the Money Laundering and Proceeds of Crime Act. In the event of conflict between a definition in this guidance and that in the Act, the latter prevails.

TERM	DEFINITION
Beneficial Owner (or Ultimate Beneficial Owner)	Refers to the natural person(s) who ultimately51 owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise 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. DNFBPs, along with financial institutions are required to implement AML/CFT obligations as set out in the MLPC Act and as elaborated in this Guidance.
Financial Institution	Means a financial institution as defined in section 2 of the MLPC Act
Financial Intelligence Unit (FIU)	Refers to the Financial Intelligence Unit, established under section 6A of the MLPC Act
High risk countries	Refers to countries listed in a circular or directive issued by the FIU in terms of section 26A. These are normally countries that would have been identified by the FATF as non-compliant for AML/CFT purposes. Financial institutions and DNFBPs are required to exercised enhanced due diligence, proportionate to the identified risks, when conducting business relationships with persons or institutions in such countries.
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, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering	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. See section 9 of the MLPC Act
MLPC Act	Money Laundering and Proceeds of Crime Act [Chapter 9:24]
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.
Senior management	Refers to any person(s) having authority and responsibility for planning, directing or controlling the activities including the management and administration of a financial Institution or DNFBP.

Cross-border wire transfer	Refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *wire transfer* in which at least one of the financial institutions involved is located in a different country.
Domestic wire transfer	Refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in the same country.
Financial Inclusion	Financial inclusion refers to the access to, and usage of, a range of financial products and services provided by formal financial service providers to specific target groups or all segments of the population, as well as the quality of these products and services
Proportionate measures	Refers to AML-CFT measures that are aligned with the level of risks. Enhanced measures are required for identified higher risk customers / transactions / situations while simplified measures may be implemented for lower risk situations.
Inclusive integrity	Refers to implementation of AML-CFT in a way that aligns with financial inclusion.
Money Laundering risk	The risk that a country, financial institution or business unit could be used for Money Laundering
Terrorist Financing risk	The risk that a country, financial institution or business unit could be used for Terrorism Financing.
Compliance Risk	This refers to the current and prospective risk of damage to the organisation's business model or objectives, reputation and financial soundness arising from non-adherence to regulatory requirements and expectations. Compliance risk is an institutional-level concern and revolves around non-adherence to AML-CFT regulatory requirements
Financial exclusion risk	This refers to the risk of excluding significant portions of population (mostly low-income customers as well as semi-formal and informal institutions serving the low-income customers) from the financial

	system This exclusion opens up opportunities for more money laundering

PART I – INTRODUCTION AND BACKGROUND

1. INTRODUCTION

1.1. Background

1.1.1. This guidance is issued by the Financial Intelligence Unit to assist Financial Institutions (as defined in section 2 of the MLPC Act) and Designated Non-Financial Businesses and Professions (as defined in section 13 of the MLPC Act) to understand and implement their statutory obligations on Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT).

1.1.2. The guidance must, therefore, be read together with –

(a) the Money Laundering and Proceeds of Crime Act (MLPC Act) (https://www.fiu.co.zw/amlcft-framework) which sets out in detail the AML/CFT statutory obligations of financial institutions and DNFBPs;

(b) all current directives or circulars issued under the MLPC Act;

(c) other applicable laws, including Statutory Instruments 76 of 2014 and 56 of 2019 on the implementation of targeted financial sanctions to combat financing of terrorism and financing of proliferation of weapons of mass destruction, respectively.

1.1.3. In the event of any conflict between what is set out in this Guidance and what is set out in the MLPC Act or any applicable law, the relevant legal provision prevails.

1.1.4. The Guidance reflects the shift from a previous rule based, "tick-box" approach, to a risk based approach (RBA) to combating money laundering and financing of terrorism.

1.1.5. Section 12B of the MLPC Act requires every financial institution or DNFBP to –

(a) **identify**, **assess** and **understand** the money laundering (ML) and terrorism financing (TF) risks to which the financial institution or DNFBP is exposed; and

(b) put in place and implement effective measures to mitigate the risks.

1.1.6. Implementation of most of the AML/CFT requirements under the MLPC Act, therefore, starts with an assessment and understanding of the money laundering risks to which the institution or business / profession is exposed.

1.1.7. The rule based approach, which was enforced prior to 2012, required financial institutions and DNFBPs to implement AML/CFT obligations uniformly in respect of all customers, to all transactions and to all situations, regardless of the level of money laundering or terrorism financing risk.

1.1.8. This "tick box" and "one-size-fits-all" approach resulted in unfocused and inefficient deployment of resources. Resources were wasted on customers, transactions and financial products / services that presented little ML/TF risks. This rigorous uniform enforcement of AML/CFT requirements on all customers, all transactions and all situations also resulted in the exclusion of a significant segment of the population who failed to meet the stringent requirements to open bank accounts or to access other financial services.

1.1.9. The risk based approach seeks to strike a balance between protecting the integrity of the financial system, through implementation of measures to deter, detect and report ML and TF, on the one hand, and promoting financial inclusion, on the other hand.

1.1.10. This balanced approach is sometimes referred to as "inclusive integrity". The risk based approach achieves this balance by giving financial institutions and DNFBPs the leeway to assess the different levels of ML/TF risks presented by different types of customers and by different financial products or services.

1.1.11. Having thus identified and assessed the ML /TF risks, financial institutions and DNFBPs are **required** to apply **enhanced due diligence** in respect of all high risk

customers and high risk products / services. Conversely, the financial institutions and DNFBPs are **permitted** to implemented reduced or simplified customer due diligence on low risk customers and low risk financial products / services.

1.1.12. There are some classes / types of customers, transactions that are deemed by law to be high risk, where a financial institution or DNFBP has no discretion to determine otherwise.

- For example, every **politically exposed person** referred to in section 20 of the MLPC Act is, by law, deemed as high risk and must be treated accordingly regardless of the financial institution's own assessment of the level of risk presented by any such customer.

1.1.13. This Guidance supersedes and replaces the ***Guidelines on Anti-Money Laundering and Combating Financing of Terrorism for Financial Institutions and Non-Financial Businesses and Professions,*** of 2006.

1.2. Application: to whom does the Guidance apply?

1.2.1. The Guidance applies to every financial institution and every DNFBP as defined in sections 2 and 13, respectively, of the MLPC Act.

1.2.2. Annexures "A" and "B" to the Guidance re-states / lists the types of services that qualify one as a financial institution or as a DNFBP, respectively, as defined under section 2 and section 13 of the MLPC Act.

PART II – THE RISK BASED APPROACH

2. THE RISK-BASED APPROACH TO AML/CFT

2.1. Overview

2.1.1. Having looked at the key AML/CFT obligations of financial institutions and DNFBPs above, this part of the Guidance focuses on the principles that should help financial institutions and DNFBPs to implement the requirements effectively.

2.1.2. This is where the risk based approach (RBA) to AML/CFT comes in. The risk based approach requires financial institutions, DNFBPs and competent authorities to **identify, assess** and **understand** the money laundering risks to which they are respectively exposed, and to take commensurate measures to **mitigate** such risks.

2.1.3. The risk based approach is based on the premise that one cannot effectively combat that which you have not properly identified and understand. It is also based on a recognition that resources to combat ML and TF are invariably finite and the limited resources can be deployed more efficiently and effectively if a FI or DNFBP focuses more on the high risk customers or products and services and devotes less resources to lower risk situations. Put differently, the risk based approach enables a FI / DNFBP to save compliance resources (human, financial and material resources, etc) by applying less stringent measures to low risk situations and to then deploy such savings towards enhanced measures for higher risk situations.

2.1.4. In practice, a ML and / or TF risk assessment by financial institutions and DNFBPs involves an assessment of the following types of risks, in a risk matrix format –

(a) customer risk;

(b) financial product risk;

(c) delivery channel risk; and

(d) geographic risk;

2.1.5. Thus, in respect of customer risk, the financial institution or DNFBP would assess and classify its customers by risk levels, i.e. Low Risk, Medium Risk and High Risk (or any similar risk scoring method).

2.1.6. The financial institution or DNFBP will do the same for the various products / services it offers to its customer. It has to identify those products / services that are most likely to be abused to launder proceeds of crime (high risk products / services) and those that are less likely to be favoured by launderers.

2.1.7. Having assessed the ML/ TF risks to which the business is exposed, the financial institution or DNFBP must come up with appropriate and effective measures to mitigate those risks, i.e. applying enhanced measures for high risk customers, products or situations, and simplified measures for low risk customers, products or situations.

2.1.8. The results of the financial institution's or DNFBP's risk assessment must lead to the design and implementation of a risk-based compliance program.

2.2. Risk Identification, Assessment and Mitigation: The Process

2.2.1. Section 12B of the MPLC Act requires every financial institutions and every DNFBPs to assess the money laundering and terrorist financing risks to which it is exposed and, thereafter, to and put in place measures to mitigate the identified risks.

2.2.2. The law does not prescribe a particular method or process of carrying out the money laundering and / or terrorism financing risk assessment process.

2.2.3. What is important is for the financial institution or DNFBP to choose or come up with its own methodology, provided the chosen methodology incorporates the

principles explained in this guidance and achieves the end objective i.e. to ensure that the institution has identified and assessed the ML and TF risks it faces and, based on that assessment, has put in place effective mitigating measures.

2.2.4. The risk-mitigating measures must be commensurate with the identified risk levels, i.e., enhanced measures for higher risks and simplified / reduced measures for lower risks.

2.2.5. This guidance will, therefore, not attempt to prescribe or recommend a particular methodology for assessing ML / TF risks, as doing so goes against the very essence of the risk-based approach, which seeks to move away from the "one-size-fits-all" prescriptive approach of old.

2.2.6. The diversity of financial institutions and DNFBPs in terms of the services they offer, the types of customers they serve, the ML / TF risks to which they are exposed as well as the different sizes and different levels of complexities of businesses will necessarily demand different approaches and different methodologies to assessing and mitigating the risks. A bank or other large financial institution or financial group would, naturally be expected to invest in an equally sophisticated and appropriate IT-based risk assessment tool, either developed in-house or acquired from external service providers.

2.2.7. On the other hand, a small-sized DNFBP such as a small law firm, accounting firm or estate agent is unlikely to need a sophisticated IT-based risk assessment tool but may just need to demonstrate that –

(a) it is aware of the different money laundering risk factors (customer risk, product risk, geographic risk and delivery channel risk) and how they apply to its specific business;

(b) the business has a system and training to identify which type of customers and which types of transactions / services offered by the business, present higher risks;

(c) the business applies enhanced due diligence in respect of the higher risk customers / transactions (e.g. seeking more in depth information on the nature of business or source of funds / wealth of the customer); and

(d) the business is able to identify and report suspicious transactions,

2.2.8. Without prescribing or endorsing any particular methodology for use to assess ML / TF risks, this section of the guidance seeks to set out and explain the principles that should guide a financial institution or DNFBP in implementing AML/CFT obligations using the risk based approach.

2.2.9. As a guide, there are four key steps involved in implementing the risk based approach by a financial institution or DNFBP, namely:

Step 1: Risk identification;

Step 2: Risk assessment /measurement;

Step 3: Risk mitigation; and

Step 4: Risk Monitoring and evaluation.

2.2.10. ***Step 1: Risk identification***

2.2.10.1. This involves identifying the **inherent risks** to which the institution / business is exposed. Inherent risk refers to the ML / TF risks faced by the institution / business, before one considers the controls and other measures already in place to mitigate the risk.

2.2.10.2. There are 4 main types of risks that a financial institution / DNFBP would normally face, and which, in most cases, would be covered in a risk assessment, namely:

- Customer risk

- Products / services risks
- Geographic risk
- Delivery channel risk

2.2.11. ***Step 2: Risk assessment / measurement***

2.2.11.1. This involves measuring the magnitude of the risk and each of the risk types identified under Step 1, above.

2.2.11.2. In relation to each risk type, the business / institution must assign risk-rating score. Smaller businesses, especially the DNFBPs may not need an elaborate / complex risk scoring model as would be expected of a bank.

2.2.11.3. Most DNFBP businesses in Zimbabwe that are involved in straightforward occasional transactions may be content with a simple risk scale that distinguishes between high and low risk situations, while banks and most financial institutions may, depending on size and complexity of business have a risk scale with three or more categories, e.g. Low risk, Medium risk, Medium-Low risk, Medium High risk, High Risk, etc.

(a) Customer risk

2.2.11.4. Under customer risk, the institution / business assesses 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 / support terrorism.

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

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

- Non-resident customers in general;
- Non-resident customers connected with countries known to present high ML or TF risks;

(b) Products / services risk

2.2.11.6. Assessment of this risk factor looks at the services / products offered by the institution / business and estimates the likelihood that a particular product would be abused to launder proceeds of crime or to finance terrorism.

2.2.11.7. Examples of products or services that are normally considered as high risk include:

- Cash (applies mostly to banks, casinos);
- Wire transfers (applies mostly to banks and money transfer service providers);
- Private banking (mostly applies to banks);
- International debit cards (mostly offered by banks);
- High value goods / services, especially where they are paid for in cash (real estate, vehicles, jewelry, etc); and
- Products and services or transaction methods that allow a degree of anonymity of the customer, e.g. crypto assets, nominee accounts, complex and opaque corporate structures, etc.)

(c) Geographic / country risk

2.2.11.8. Geographic and country risks looks at the ML / TF risks associated with the country or geographic location of the financial institution / DNFBP as well as the ML/TF risks associated with a customer or a transaction.

2.2.11.9. Thus the financial institution / DNFBP must always have regard to the ML/TF types and level of risks to which the country is exposed and which could impact on the institution / business's own ML / TF risks.

2.2.11.10. In this regard, the institution or business may be guided by the national ML /TF risk assessment, if any, done by the authorities, as well as the institution / business's own understanding of the national ML / TF risks.

2.2.11.11. Similarly, when dealing with customers or transactions associated with a foreign country, the financial institution / DNFBP should pay regard to the ML / TF risks associated with the particular country, e.g. countries that are known to present high terrorism or terrorism financing risks, countries that are associated with high levels of corruption, or countries that are identified by the Financial Action Task Force (FATF) as not sufficiently implementing AML/CFT requirements.

(d) Delivery channel risk

2.2.11.12. This is closely associated with, and can be assessed as part of products / services risks. Delivery channel risk refers to the method of delivering a financial or other product or service to a customer.

2.2.11.13. Assessment of delivery channel risk normally looks at whether a service / product is delivered to a customer face-to-face i.e. where the business / institution directly interfaces with a customer, or whether it is delivered through a non-face-to-face medium, such as the internet or through agents.

2.2.11.14. Some types of non-face-to-face methods of delivering services present higher ML and / or TF risks, e.g. –

- Where an account or other business relationship can be established online;

- Where a financial institution / DNFBP relies on agents to identify and verify identities of customers or to deliver services to customers;

2.2.12. ***Step 3: Risk mitigation***

2.2.12.1. Having identified the different types of risks and assessed the inherent risks, the institution / business should implement controls and measures to mitigate the identified risks, with more focus on the higher risks.

2.2.12.2. Enhanced controls and measures are required for higher risk customers and situations, while simplified / reduced measures may be implemented for lower risk situations.

2.2.12.3. Every financial institution and every DNFBP is required to have in place an AML/CFT compliance program that takes into account and addresses the identified risks and the risk levels.

2.2.12.4. An AML/CFT compliance program will consist of policies and procedures.

2.2.13. **Monitoring of risks and review**

2.2.13.1. Risk assessment is not a once-off event but an ongoing process. Financial institutions and DNFBPs must, therefore, ensure that the risk assessment is kept current and up to date with the evolving risks.

2.2.13.2. A financial institution / DNFBP's risk assessment should be reviewed at intervals determined by the institution / business, usually annually.

2.2.13.3. A review may be triggered by lapse of the set time period or, at any other time, if there are material events or changes, that have a bearing on the entity's ML/TF risks.

2.2.13.4. Some trigger events / changes may affect only some parts or components of the assessment, and may not always require a review of the whole assessment.

2.2.13.5. As with the original assessments, the risk assessment updates and any adjustments to the controls and measures necessitated by such review should be documented.

PART III – SPECIFIC AML/CFT OBLIGATIONS IN THE CONTEXT OF THE RISK BASED APPROACH

3. AML/CFT COMPLIANCE PROGRAM

3.1. The various obligations imposed by the MLPC Act require every financial institution and every DNFBP to have in place an AML/CFT compliance program, which must be continuously reviewed and developed to respond to the evolving ML / TF risks.

3.2. The MLPC Act does not specifically mention the term "compliance program" but section 25 of the Act sets out and prescribes a set of requirements that are recognized as the four pillars of an AML/CFT Compliance Program. It requires financial institutions and DNFBPs to have the following in place:

- **Internal procedures, policies and controls** to fulfil the requirements of the Act;
- Appointment of a **compliance officer**, at senior management level, who is responsible for day to day AML/CFT compliance;
- AML/CFT **training program** for staff;
- **Independent audit** to review and verify effectiveness of the measures in place to comply with the requirements of the Act.

3.2.1. **Internal procedures, policies and controls**

3.2.1.1. A reference to AML/CFT policies, procedures and controls is in fact a reference to a financial institution's entire AML/CFT Compliance Program.

3.2.1.2. Policy is a document that 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.

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

I. Risk assessment
II. Customer due diligence, including –
    - Customer identification and verification;
    - Ongoing monitoring
III. Enhanced customer due diligence and transaction monitoring for high risk customers, including Politically Exposed Persons
IV. Detection and reporting of suspicious transactions

3.3. Among other things, the institution / business's policies and procedures must cover the following aspects of AML/CFT compliance.

4. CUSTOMER DUE DILIGENCE

4.1. Aside from the overarching AML/CFT obligation to identify, assess and mitigate ML/TF risks, one of the most basic and critical measures to combat ML and TF is the implementation of **customer due diligence** requirements.

4.2. Customer Due Diligence (CDD) also loosely referred to as Know Your Customer (KYC) consists of a number of distinct but connected elements, namely –

- Identifying and verifying a customer's identity;
- Establishing the nature of business and source of funds / wealth of the customer;
- Undertaking ongoing due diligence and monitoring;

4.3. This Guidance demonstrates the important interplay between risk assessment and customer due diligence. The institution / business's assessment and understanding of the risks presented by different customers and financial products and services,

informs the level of due diligence required for each customer category or product type.

I. Customer identification and identity verification (Section 15 – 23 of the Act)

4.4. The starting point for customer due diligence is for the financial institution / DNFBP to identify and verify the identity of a customer.

4.5. Section 15(1) of the MLPC Act obliges financial institutions and DNFBPs to identify and verify the identity of their customers by means of an official identification document.

To identify a customer and to verify the customer's identity are two separate but related requirements under this provision.

- To identify a customer is to ascertain and record the name of the customer.
- To verify the identity is to confirm the customer's identity by obtaining the official identification document of the customer, i.e. national identity document, driver's license or passport, in the case of individuals, or certificate of incorporation or other document evidencing the creation and legal status of the entity.

4.6. The obligation to identify and verify the identity of a customer arises in each of the following circumstances –

(a) Where a financial institution or DNFBP intends to open an account for, or establish a business relationship with a customer; or
(b) In the case of a proposed occasional once-off transaction, which does not involve the opening of an account or establishment of an ongoing business relationship, if the proposed transaction is valued at US$5,000 or more; or
(c) In every case where the customer intends to carry out a wire transfer, whether domestic or international, valued at US$1,000 or more; or
(d) Regardless of the amount involved, if doubt exists regarding the correctness of previously obtained customer identification information; or
(e) Regardless of the amount involved, where there is suspicion of money laundering or terrorism financing, regarding in relation to the customer.

Customer identification obligations of legal practitioners

4.7. The customer identification and verification obligations of a legal practitioner arise when the legal practitioner is acting for a client in the following types of transactions, regardless of value, and whether it is an ongoing business relationship or a once-off transaction –

(i) the buying or selling of immovable property or any interest in immovable property;
(ii) the management of money, securities or other assets;
(iii) the management of bank, savings or securities accounts;
(iv) the organisation of contributions for the creation, operation or management of companies;
(v) the creation, operation or management of legal persons or arrangement, and buying and selling of business entities;

Customer identification obligations of various DNFBPs

4.8. The below listed designated businesses and professionals are required to identify and verify the identity of their customers in the following situations –

(a) every legal, accounting or corporate service professional involved in any transaction concerning the buying or selling of immovable property or any interest in immovable property that is not mediated through a financial institution or estate agent;
(b) every estate agent, in relation to the vendor and purchaser involved in any transaction concerning the buying or selling of immovable property or any interest in immovable property;
(c) every gaming operator, in relation to any of their customers who opens an account or engages in any financial transaction the value of which is equal to or exceeds three thousand United Sates dollars (or such lesser or greater amount as may be prescribed);
(d) every precious stones dealer and every precious metals dealer, in relation to any of their customers from whom or on behalf of whom they receive a payment in

currency equal to or exceeding fifteen thousand United Sates dollars (or such lesser or greater amount as may be prescribed).

4.9. With respect to (c) and (d), above, the obligation to identify and verify the identity of a customer arises, regardless of the value involved, if there is suspicion of money laundering or terrorism financing in relation to the customer or the transaction.

Requirement to identify ultimate beneficial owners of legal entities: s. 15(3) of Act

4.10. Over and above the obligation to identify and verify the identity of a customer who is a legal person, financial institutions and DNFBPs are also required to identify and verify the identity of the ultimate beneficial owner of the entity.

4.11. Beneficial owner(s) refers to the natural person(s) who ultimately owns or exercises effective control over a legal person, including the person who ultimately enjoys the fruits or dividends of the legal entity.

4.12. A beneficial owner is not necessarily the same person / entity listed as legal owner (shareholder) in official company documents. In the context of money laundering / terrorism financing, criminals may use nominees and proxies (individuals, trusts or corporate vehicles) as shareholders in an effort to disguise or conceal the true ownership of ill-gotten assets.

4.13. To establish who the beneficial owner(s) is / are, the financial institution is required to "pierce the veil" of the entity. This may involve "peeling off" various corporate layers in the shareholding structure, until the natural person(s) who is/ are identified.

4.14. Where the corporate entity has a number of corporate shareholders, it may not be practical or beneficial to try to establish the beneficial owners of all the corporate shareholders. As a general guide, it would be sufficient to identify the beneficial owners of only those entities that hold 10% or more shareholding in the customer.

4.15. Beneficial ownership information can be obtained from a variety of sources, including:

- The entity customer itself (the one seeking to transact or open an account) should be asked to disclose its beneficial owners. But such information may still need to be verified through other independent means;
- The deeds and companies' registry. Companies in Zimbabwe, are by law, required to maintain beneficial ownership information and file same with the Registrar of Companies. Similarly trustees of registered trusts are required to maintain and file with the Registrar of Deeds information identifying all the trustees, found / settlor and beneficiaries;
- Open information sources from the internet concerning the entity, including from the entity's own website, if any.

4.16. Identifying the ultimate beneficial owners of legal entities can be a difficult exercise especially where the entity has a complex shareholding structure and even more so where some of the shareholders of the entity are incorporated in offshore jurisdictions.

4.17. The extent and expense to which a financial institution / DNFBP should go to identify the ultimate beneficial owner should be guided by the financial institution or DNFBPs assessment of the ML / TF risk involved.

4.18. Where a financial institution / DNFBP has failed to get sufficient reliable information identifying the beneficial owner(s) of a legal entity, and does not have sufficient confidence as to who the customer is, it is not advisable to proceed with the business relationship, especially where the risk of money laundering appears to be high.

Timing of customer identification and verification (s. 16 of MLPC Act)

4.19. As a general rule, identification and identity verification of a customer as required under section 15 of the Act, must be undertaken prior to the opening of the account or establishment of the business relationship.

4.20. The law, however, recognizes that there are exceptional instances where it may not be possible or practical from a business continuity point of view to undertake the customer verification before establishing the business relationship.

4.21. Financial institutions and DNFBPs are thus permitted to allow a customer to utilize a business relationship subject, strictly, to meeting the following conditions:

(a) Where a delay in verification is unavoidable in the interest of not interrupting the normal conduct of business, and

(b) The financial institution or DNFBP adequately manages the ML / TF risk through adoption of risk management procedures under which the customer may utilize the business relationship pending identity verification.

4.22. Both conditions (a) and (b) above, must be met, before a financial institution or DNFBP avails itself of this exceptional dispensation.

4.23. Possible risk management measures would be for a financial institution /DNFBP to impose restrictions on the nature of transactions that may be undertaken before full identity verification, e.g. allowing inflows into an account and restricting any outflows.

4.24. The appropriate risk management conditions in each case should depend on the nature and level of ML / TF risk.

Particulars of customer identification (s. 17 of MLPC Act)

4.25. Section 17 lays down the minimum information required as part of customer identification and verification, both for individual and corporate customers.

4.26. Over and above identifying a customer and verifying his / her identity by means of an identity document – the following customer identification particulars are required –

(a) for a customer who is an individual, his or her full name and date and place of birth;

(b) for a legal person the corporate name, head office address, identities of directors, proof of incorporation or similar evidence of legal status and legal form, provisions governing the authority to bind the legal person, and such information as is necessary to understand the ownership and control of the legal person;

(c) for legal arrangements, the names of every trustee, settlor, and beneficiary of an express trust, and of any other party with authority to manage, vary or otherwise control the arrangement;

(d) in addition to the identity of the customer, the identity of any person acting on behalf of a customer, including evidence that such person is properly authorised to act in that capacity;

(e) information on the intended purpose and nature of each business relationship;

(f) sufficient information about the nature and business of the customer to permit the financial institution or designated non-financial business or profession to fulfil its obligations under the MLPC Act.

4.27. For higher risk customers and situations, in line with the risk based approach, more information would need to be obtained.

4.28. Similarly, for low risk customers and financial products, the FIU is empowered to grant exemptions to dispense with some of the identification requirement, although a person's official identification document is normally a non-negotiable minimum requirement.

4.29. The financial institution DNFBP should have clear written AML/CFT procedures, detailing how it implements the different levels of customer due diligence, in respect of low risk, medium risk and high risk customer categories.

4.30. The procedures should set out which customers are subject to simplified customer identification requirements, based on their low risk status, and what those requirements would be. The procedures should similarly set out enhanced identification requirements for the higher risk customers.

Reliance on customer identification by third parties / intermediaries (s. 18 of Act)

4.31. The obligation to comply with customer identification and verification requirements prescribed by the Act rests squarely with the financial institution or DNFBP concerned.

4.32. It is permissible for a financial institution / DNFBP to rely on customer identification and verification performed by third parties or intermediaries / agents, but only under the following conditions –

(a) only where there is no suspicion of ML or TF, and

(b) provided that information on the identity of each customer or beneficial owner is obtained immediately on opening the account or establishing the business relationship, and

(c) the financial institution or DNFBP is satisfied that the third party is –

  (i) in a position to provide, without delay, copies of the relevant identification and other required documents,

  (ii) is established, domiciled or ordinarily resident in a compliant jurisdiction.

4.33. The financial institution /DNFBP relying on a third party for customer identification remains ultimately responsible for any non-compliance with the identification and verification requirements set out by the Act.

4.34. Some financial institutions rely on agents to recruit / onboard customers. In such cases, it is the financial institution's responsibility to ensure that every such agent is adequately trained on, and complies with the identification / verification requirements of the Act and should have written procedures on conducting the process.

Identification and identity verification of non-face-to-face customers

4.35. A financial institution or DNFBP may find itself in a situation where it is necessary or expedient to establish a business relationship with a customer who is not or cannot be physically present for purposes of identification and identity verification.

4.36. Such a situation presents a heightened money laundering / terrorism financing risk and the financial institution or DNFBP must take reasonable and adequate measures to satisfy itself that the customer is who he / she / it presents itself to be.

4.37. Section 19 of the MLPC Act provides that –

(1) designated non-financial businesses and professions shall take adequate measures to address the specific risk of money laundering and financing of terrorism in the event they conduct business relationships or execute transactions with a customer who is not physically present for purposes of identification.

(2) Such measures shall ensure that the due diligence is no less effective than where the customer appears in person, and may require additional documentary evidence, or supplementary measures to verify or certify the documents supplied, or confirmatory certification from financial institutions or other documentary evidence or measures, as may be prescribed in directives.

Enhanced Identification and due diligence requirements for high risk customers

4.38. Section 20 (1) (a) of the MLPC Act requires financial institutions and DNFBPs to put in place risk management systems -

"to identify customers whose activities may pose a high risk of money laundering and financing of terrorism and shall exercise enhanced identity verification and ongoing due diligence procedures with respect to such customers;

4.39. This provision should read in association with section 12B of the Act which requires financial institutions and DNFBPs to identify, assess and mitigate the ML and TF risks to which their businesses are exposed.

4.40. The obligations in section 12B are wider, encompassing assessment of all ML/TF risk factors, including customer risk, product risk, delivery channel risk and geographic risk.

4.41. Section 20, on the other hand, emphasizes customer risk, i.e. the need to identify which customers present the highest ML/TF risk and the need to exercise enhanced customer identification, verification and ongoing due diligence and monitoring.

Identification and due diligence requirements for politically exposed persons

4.42. Section 20 (1) (b) requires financial institutions and DNFBPs to put in place risk management systems to determine if a customer or beneficial owner of an account is a ***politically exposed person (PEP).***

4.43. If a customer or beneficial owner is identified as a PEP, a financial institution or DNFBP is required to –

(a) Obtain senior management approval **before establishing a business relationship** with the customer; or, if the customer is identified as a PEP after a business relationship had already been established, senior management approval is required to continue with the business relationship; and

(b) Take all reasonable measures to identify the source of wealth and funds and other assets of the customer or beneficial owner of the customer.

4.44. A politically exposed person is defined under section 13 of the MLPC Act as –

(a) any person who is or has been entrusted in Zimbabwe with prominent public functions, including but not limited to, a Head of State or of government, a senior government, judicial or military official, a senior executive of a state-owned corporation, or a senior official of a political party; or
(b) any person who is or has been entrusted with prominent public functions by a foreign country, including but not limited to, a Head of State or of government, a senior government, judicial or military official, a senior executive of a state-owned corporation, or a senior official of a political party; or
(c) any person who is or has held a position as a member of senior management of an international organisation, including the position of director, deputy director, member of the board or equivalent functions; or
(d) any close associate, spouse or family member of a person referred to in paragraphs (a) to (c);

4.45. 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.

4.46. For non-PEP customers, financial institutions and DNFBPs have the obligation to assess the ML/TF 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.

What to do if customer identification obligations cannot be fulfilled

4.47. Section 22 of the Act prohibits a financial institution or a DNFBP from establishing or continuing a business relationship with a customer, if the identification and verification requirements set out above cannot be fulfilled.

4.48. In addition to declining or discontinuing the business relationship / transaction, the financial institution or DNFBP is required to ***immediately*** report the matter to the FIU.

4.49. Section 22 provides as follows –

A financial institution or designated non-financial business and profession that cannot fulfil the requirements of this Part with respect to any customer or beneficial owner shall not establish an account for or maintain the business relationship with that customer and shall immediately make a report on the matter to the Unit.

II. Ongoing Due Diligence and Monitoring (Section 26 of the Act)

4.50. Customer Due Diligence is not a once-off exercise, confined only to customer identification and identity verification at the time of establishing a business relationship with the customer.

4.51. Customer identification and verification requirements only represent the first stage of an ongoing process that continues for the entire duration of the business relationship.

4.52. Just as is the case with the initial customer identification and verification stage, the level of ongoing due diligence and monitoring depends on the risk category of the customer.

4.53. For low risk customers and low risk financial products, only simplified / reduced due diligence and monitoring is required, while for higher risk customers and / or higher risk products and services, enhanced due diligence (EDD) and monitoring is mandatory.

4.54. A financial institution / DNFBP should have written AML/CFT procedures that detail how the business entity implements risk based customer due diligence. The procedure should set out and describe the different levels of due diligence for each customer risk category.

4.55. It should be noted that the law does not allow a financial institution / DNFBP to dispense with customer due diligence and monitoring requirements for any customer or for any financial product on the grounds that the ML/TF risk is nil. ML/TF risk can never be zero, but can only be low, hence the need for reduced level of monitoring for low risk situations.

4.56. A customer's risk profile can change when there are some material changes in the customer's or other relevant circumstances, e.g., if there are changes in the customer's line of business, source of funds, volume / value of transactions etc. It is thus important for a financial institution / DNFBP to not only monitor each customer's activities and circumstances on an ongoing basis, guided by the customer's risk category, but also to undertake periodic risk assessment reviews for the entire customer base.

4.57. Section 26 of the Act sets out the obligations of financial institutions and DNFBPs in relation to ongoing due diligence. It provides thus –

(1) Financial institutions and designated non-financial businesses and professions shall exercise ongoing due diligence with respect to business relationships that are or may become subject to the requirements of customer identification and verification, including –

(a) maintaining current information and records relating to the customer and beneficial owner concerned; and

(b) closely examining the transactions carried out in order to ensure that such transactions are consistent with their knowledge of their customer, and the customer's commercial or personal activities and risk profile; and

(c) ensuring the obligations pursuant to sections 19, 20 and 21 relating to high risk customers, politically-exposed persons, and correspondent banking relationships are fulfilled.

(2) Financial institutions and designated non-financial businesses and professions shall –

(a) pay special attention to all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(b) pay special attention to business relations and transactions with persons, including legal persons and arrangements, from or in non-compliant or insufficiently compliant jurisdictions; and

(c) examine as far as possible the background and purpose of transactions under paragraphs (a) and (b) and set forth in writing their findings; and

(d) take such specific measures as may be prescribed by directive from time to time to counter the risks with respect to business relations and transactions specified under paragraph (b).

(3) The findings referenced in subsection (2)(c) shall be maintained as specified in section 24, and be made available promptly if requested by the Unit or by a foreign counterpart agency, a competent supervisory authority or other authority prescribed by the Minister.

Higher risk countries (section 26A) of the Act

4.58. Financial institutions are required to conduct enhanced due diligence, proportionate to the risk towards business relationships and transactions with any natural or legal person from countries identified as insufficiently compliant in implementing AML/CFT standards.

4.59. The FIU is mandated to communicate such list, as updated from time to time, to financial institutions and DNFBPs.

4.60. The list may include non-compliant countries identified and listed by the Financial Action Task Force or identified by the FIU on its own initiative.

4.61. With respect to some of the countries on the FATF "black list", financial institutions and DNFBPs may be required to take specified counter-measures as set out in the FIU directive. For transactions involving other non-compliant countries where no FATF counter-measures are specified, financial institutions and DNFBPs are simply required to implement enhanced due diligence, having regard to the nature of the AML/CFT shortcomings and risks of each specified country.

5. REPORTING OF SUSPICIOUS TRANSACTIONS

5.1. Obligation to report suspicious transactions

5.1.1. This is another fundamental obligation key to combating ML /TF. A financial institution or DNFBP is required to report every suspicious transaction, in prescribed form through the GoAML platform, to the FIU.

5.2. In terms of timing, the obligation is to submit the report to the FIU **promptly**, but in any case not later than three (3) working days from the time when the suspicion arises.

5.3. A suspicious transaction includes an attempted transaction, i.e. where the transaction was not completed, but was nevertheless suspicious.

5.4. Section 30(1) of the Act provides that -

(1) Subject to subsections (2) and (3), financial institutions, designated non-financial businesses and professionals, and their respective directors, principals, officers, partners, professionals, agents and employees, that suspect or have reasonable grounds to suspect that any property or any transaction or attempt to effect a transaction –

(a) involves or is the proceeds of crime; or

(b) is related or linked to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or those who finance terrorism;

shall submit promptly, but not later than three working days after forming the suspicion, a report setting forth the suspicion to the Unit.

5.4.1. Basic information required for completing the suspicious transaction report template on the GoAML platform is set out as Annexure "C".

5.4.2. Annexure "D" gives a non-exhaustive list of indicators or red flags that are useful in helping a financial institution or DNFBP identify and report suspicious transactions.

5.4.3. Some suspicious transaction red flags / indicators are business-type specific. It is thus important for financial institutions and each DNFBPs and their staff to be

familiar with the common ML / TF red flags associated with their respective types of businesses.

5.5. **Prohibition against tipping-off**

5.5.1. Except where required by law, a financial institution or DNFBP shall not disclose to its customer or to a third party that a suspicious transaction report has been submitted, or will be submitted to the FIU.

5.5.2. Such disclosure has the effect of tipping-off the customer and afford him / her the opportunity to take steps to defeat or undermine any subsequent investigations by law enforcement agencies.

5.5.3. Section 31(2) of the Act provides that -

"No financial institution or designated non-financial business or profession, nor any director, partner, officer, principal or employee thereof, shall disclose to any of their customers or a third party that a report or any other information concerning suspected money laundering or financing of terrorism will be, is being or has been submitted to the Unit, or that a money laundering or financing of terrorism investigation is being or has been carried out, except in the circumstances set forth in subsection (3) or when otherwise required by law to do so."

5.6. **Submission of Large Cash Transaction reports**

5.6.1. In addition to the obligation to report suspicious transactions to the FIU as required under section 30(1), the FIU may, in terms of section 30(6) require financial institutions and DNFBPs to submit threshold-based transaction reports.

5.6.2. Under this requirement, the FIU issues directives from time to time requiring financial institutions and DNFBPs to submit returns in respect of all cash transactions of or above a specified threshold, otherwise referred to as "large cash transaction" reports.

5.6.3. It is important to note the difference between suspicious transaction reports (STRs) and threshold-based cash transaction reports (CTRs).

- STRs must be submitted in terms of section 30 (1) of the Act, regardless of the value involved as long as the transaction is a suspicious one.
- CTRs must be submitted in compliance with any applicable directive issued by the FIU, regardless of whether or not the transaction is suspicious.
- If a transaction is suspicious and also meets the CTR reporting threshold, it must be reported separately, both as an STR and as a CTR.

6. RECORD KEEPING

6.1. Section 24 of the MLPC Act sets out the record-keeping obligations of financial institutions and DNFBPs, prescribing what must be covered by such records as well as the minimum length of time for which such records should be kept.

6.2. The record-keeping obligations are meant to assist the FIU and law enforcement agencies should the need arise to investigate a customer or a transaction.

6.3. Section 24 provides that –

(1) Financial institutions and designated non-financial businesses and professions shall maintain all books and records with respect to their customers and transactions as set forth in subsection (2), and shall ensure that such records and the underlying information are available on a timely basis to the Unit and such other competent authorities as are prescribed by the Minister.

(2) Such books and records shall include, as a minimum—

(a) account files, business correspondence, and copies of documents evidencing the identities of customers and beneficial owners obtained in accordance with this Act, all of which shall be maintained for not less than five years after the business relationship has ended; and

(b) records on transactions sufficient to reconstruct each individual transaction for both account holders and non-account holders which shall be maintained for not less than five years from the date of the transaction; and

(c) the findings set forth in writing pursuant to section 26(2)(c) and related transaction information which shall be maintained for at least five years from the date of the transaction; and

(d) copies of all suspicious transaction reports made pursuant to section 30, including any accompanying documentation, which shall be maintained for at least five years from the date the report was made.

7. OBLIGATIONS RELATING TO WIRE TRANSFERS (FINANCIAL INSTITUTIONS)

7.1. Section 27 of the MLPC Act sets out detailed obligations when financial institutions conduct or process wire transfer obligations on behalf of customers. The requirements are derived from Recommendation 16 of the FATF Recommendations.

7.2. The requirements on wire transfers were developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs.

7.3. The measures aim to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

(a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;
(b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and
(c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions.

7.4. A wire transfer refers to –

any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.

7.5. The requirements do not apply to –

- Credit card or debit card payments for goods and services, provided the credit / debit card number accompanies the payment: However, where a debit / credit card is used to effect a person to person transfer of funds, the requirements apply;
- Financial institution to financial institution funds transfers and settlements, where the financial institutions are acting on their own behalf and not for a customer.

7.6. The requirements apply to both domestic and cross-border wire transfers. The requirements in relation to cross-border wire transfers are, however, more stringent than for domestic wire transfers.

7.7. There are specific obligations for **ordering**, **intermediary** and **beneficiary** financial institutions.

- **Ordering financial institution** refers to the financial institution which initiates the wire transfer on behalf of a customer;
- **Intermediary financial institution** refers to a financial institution that receives and transmits a wire transfer on behalf of the ordering financial institution (or another intermediary financial institution) and transmits the wire transfer to the beneficiary financial institution (or to another intermediary financial institution.
- **Beneficiary financial institution** refers to the financial institution at the end of the wire transfer chain, which receives the wire transfer and makes the funds available to the beneficiary customer.

7.8. The **ordering financial institution** –

(a) Should ensure that the wire transfer contains **required** and **accurate** originator information;

(b) Should ensure that the wire transfer contains **required** beneficiary information;

(c) Should maintain the required information in accordance with the record-keeping requirements set out in section 24 of the Act;

(d) Should not execute a wire transfer that lacks any of the required information.

7.9. The **intermediary financial institution** should –

(a) Ensure that, for cross-border wire transfers, all originator and beneficiary information accompanying the wire transfer is retained when the institution transmits the wire transfer to the beneficiary financial institution (or to another intermediary financial institution);

(b) Take reasonable measures to identify wire transfers that lack required originator or beneficiary information;

(c) Have in place effective risk-based policies and procedures for determining (i) when to execute, reject or suspend a wire transfer that lacks required originator or beneficiary information and (ii) the necessary follow up action;

7.10. The **beneficiary financial institution** should –

(a) Verify the identity of the beneficiary and maintain the identity verification documents in accordance with the record keeping requirements of Section 24 of the Act;

(b) Take reasonable measures to identify wire transfers that lack required originator or beneficiary information;

(d) Have in place effective risk-based policies and procedures for determining (i) when to execute, reject or suspend a wire transfer that lacks required originator or beneficiary information and (ii) the necessary follow up action;

7.11. For all qualifying **cross-border wire transfers**, the following information is required –

(a) the name of the originator;

(b) the originator account number where such an account is used to process the transaction;

(c) the originator's address, or national identity number, or customer identification number or date and place of birth;

(d) the name of the beneficiary; and

(e) the beneficiary's account number, where such account number is used to process the transaction.

7.12. For domestic wire transfers, the same originator information as above, should accompany the wire transfer, **unless** the ordering financial information maintains such information and is in a position to avail same when required (within 3 days) to the beneficiary financial institution or to the FIU or law enforcement authorities.

8. IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS PURSUANT TO UNITED NATIONS SECURITY COUNCIL RESOLUTIONS

8.1. Countries are required to implement the requirements of United Nations Security Council Resolutions (UNSCRs) that are issued in terms of Chapter VII of the United Nations Charter.

8.2. Under these Chapter VII powers, the United Nations has various resolutions in force requiring countries to enforce targeted financial sanctions to combat financing of terrorism and financing of proliferation of weapons of mass destruction.

8.3. The resolutions identify (and require countries to identify) persons and entities involved in financing terrorism or in financing proliferation of weapons of mass destruction.

8.4. Pursuant to its international obligations, Zimbabwe passed the following statutory instruments -

(i) Statutory Instrument 76 of 2014, requiring financing institutions, DNFBPs and other persons, to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the United Nations Security Council for financing or supporting international terrorism; and

(ii) Statutory Instrument 56 of 2019, requiring financial institutions, DNFBPs and other persons to identify, freeze and report funds or other assets of individuals and entities identified by or under the authority of the United Nations Security Council for financing or promoting proliferation of weapons of mass destruction.

8.5. The FIU issues directives and guidance, from time to time, on the implementation of the requirements of the two UN sanctions regimes.

9. PENALTIES FOR NON-COMPLIANCE WITH AML/CFT OBLIGATIONS

9.1. Non-compliance by a financial institution or DNFBP with any of the AML/CFT obligations under the Act or the obligations relating to the implementation of Targeted Financial Sanctions under statutory instruments 76 of 2014 and 56 of 2019, can attract either criminal sanctions or civil penalties (or both) the MLPC Act.

9.2. Criminal and civil penalties are enforceable against the financial institution or DNFBP or against any of its employees, directors or agents, as the case may be or against both the institution / business and the responsible individuals.

9.3. Administrative penalties are enforceable by the FIU under section 5 of the MLPC Act. Under this provision, the FIU can, among other enforcement measures –

- Impose a financial penalty against the institution / business or any of its employees, directors or agents; and / or
- Order the removal of any employee, director or shareholder; and / or
- Require the financial institution / DNFBP to take specified remedial action.

Annexure "A"

Definition of "financial institution" – Section 2 of the MLPC Act

"financial institution" means any person who conducts as a business one or more of the following activities for or on behalf of a customer—

(*a*) acceptance of deposits and other repayable funds from the public, including private financial;

(*b*) lending, including, but not limited to, consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting;

(*c*) financial leasing other than with respect to arrangements relating to consumer products;

(*d*) the transfer of money or value;

(*e*) issuing and managing means of payment, including, but not limited to, credit and debit cards, travelers' cheques, money orders and bankers' drafts, and electronic money;

(*f*) issuing financial guarantees and commitments;

(*g*) trading in –

(i) money market instruments, including, but not limited to, cheques, bills, certificates of deposit and derivatives; or

(ii) foreign exchange; or

(iii) exchange, interest rate and index instruments; or

(iv) transferable securities; or

(v) commodity futures;

(*h*) participation in securities issues and the provision of financial services related to such issues;

(*i*) individual and collective portfolio management;

(*j*) safekeeping and administration of cash or liquid securities on behalf of other persons;

(*k*) investing, administering or managing funds or money on behalf of other persons;

(*l*) underwriting and placement of life insurance and other investment-related insurance, including insurance intermediation by agents and brokers;

(*m*) money and currency changing;

(*n*) 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;

and, without derogating from the generality of the foregoing, includes any of the financial institutions
or classes of financial institution listed in Part I of the First Schedule;

Annexure "B"

Definition of "designated non-financial business or profession" – Section 2 of the MLPC Act
"designated non-financial business or profession" means any of the following — *(a)* a casino licensee, lottery licensee or other person licensed or required to be licensed under the Lotteries and Gaming Act [*Chapter 10:26*]…; *(b)* an estate agent registered or required to be registered under the Estate Agents Act [*Chapter 27:17*]; *(c)* a licensed dealer or permit holder, or person required to be licensed or hold a permit, in terms of the Precious Stones Trade Act [*Chapter 21:06*]… *(d)* any person licensed, permitted or required to be licensed or permitted in terms of the Gold Trade Act [*Chapter 21:03*], to deal in gold, engage in gold recovery works, assay gold or acquire or be in possession or dispose of gold… *(e)* any person engaged in the mining or exportation of, or dealing in – (i) platinum or a platinoid metal in any form whatsoever; or (ii) any article or substance containing platinum or a platinoid metal… if such mining, exportation or dealing is authorised or required to be authorised in any way by or under the Reserve Bank of Zimbabwe Act [*Chapter 22:15*] (No. 5 of 1999) (hereinafter in this Act called a "precious metals dealer"); *(f)* persons registered or required to be registered in terms of the Legal Practitioners Act [*Chapter 27:07*], the Chartered Secretaries (Private) Act [*Chapter 27:03*], the Public Accountants and Auditors Act [*Chapter 27:12*] (No. 13 of 1995), the Chartered Accountants Act [*Chapter 27:02*] and the Estate Administrators Act [*Chapter 27:20*] (No. 16 of 1998) (hereinafter in this Act called a "legal, accounting, corporate service or estate administration professional")— (i) the buying and selling of real estate; (ii) the managing of client money, securities or other assets; (iii) the management of bank, savings or securities accounts; (iv) the organisation of contributions for the creation, operation or management of legal persons; (v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities; (vi) administering deceased or insolvent estates;

(g) trust and company service providers not otherwise registered or licensed or required to be registered or licensed under any law and who, as a business, prepare for or carry out transactions on behalf of customers in relation to any of the following services to third parties –

(i) acting as a formation, registration or management agent of legal persons;
(ii) acting as, or arranging for another person to act as, a director or secretary of a company or a partner of a partnership, or to hold a similar position in relation to other legal persons;
(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
(iv) acting as, or arranging for another person to act as, a trustee of an express trust or other similar arrangement;
(v) acting as, or arranging for another person to act as, a nominee shareholder for another person;

(*g*1) any person who is engaged in the business of buying and selling motor vehicles, whether new or used;

(h) such other person or transaction as may be designated in accordance with section 101;

Annexure "C"

Basic Contents of a Suspicious Transaction Report

a) Reporting Institution Information

i. Name and address of institution

ii. Name and address of Branch where the activity occurred

b) Suspect Information

i. Full Names or Name of Entity

ii. Address

iii. Phone Number, Residence, Work

iv. Occupation / Type of business

v. Date of birth

vi. *Forms of identification* - National registration number

- Valid Passport Number
- Zimbabwean Driver's License

vii. Relationship to financial institution (Employee, Director, Officer, Shareholder, Customer etc.)

c) ***Description of the suspicious activity***

i. Type of transaction

ii. Amount involved

iii. Other details necessary to understand the transaction

d) Action already taken

i. If an insider is involved what action has been taken?

ii. Has any law enforcement agency been advised? If yes, provide name of agency, name and telephone number of person(s) contacted, and by what method (telephone, written communication, etc)

e) Contact person

i. Full names
ii. Title / Designation
iii. Contact telephone number

f) *Date of suspicious transaction and date of preparation of report*

Annexure "D"

Indicators/ Redflags of Suspicious Transactions

Examples of suspicious transactions red flags are listed below. The list is non exhaustive and only provides examples of ways in which money may be laundered.

Unusual Transactions

1. Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.
2. The intensity of transactions for an inactive trading account suddenly increases without plausible reason.
3. Unusually short period of holding securities.
4. Frequent selling of securities at significant losses.
5. Structuring transactions to evade substantial shareholding.
6. Simultaneous transfer of funds to a group of customers' accounts from a third party
7. Request to exchange large quantities of low denominations for higher denominations.
8. Rapid increase in size and frequency of cash deposits without any corresponding increase in non-cash deposits.
9. Transactions for which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Large Cash Transactions

1. Larger or unusual settlements of securities transactions in cash form.

2. The crediting of a customer's margin account using cash and by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.
3. Depositing large cash amounts in the reporting institution's multiple bank accounts in the same day

Transactions Incompatible with Customer's Financial Standing

1. A customer who suddenly starts making investments in large amounts when it is known to the Reporting Institution that the customer does not have the capacity to do so.
2. Transactions that cannot be matched with the investment and income levels of the customer.
3. Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

Irregular Account Movement

1. Abnormal settlement instructions including payment to apparently unconnected parties.
2. Non-resident account with very large movement with subsequent fund transfers to offshore financial centres.
3. A client who authorizes fund transfer from his account to another client's account.
4. A client whose account indicates large or frequent wire transfer and sums are immediately withdrawn.
5. A client whose account shows active movement of funds with low level of trading transactions.

6. Mixing of cash deposits and monetary instruments in an account which such transactions do not appear to have any relation to the normal use of the account
7. A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals running down the transferred amount.
8. Building up large balances, not consistent with the known turnover of the customer's business and subsequent transfer of account(s) held overseas

Suspicious Behavior/Demeanor

1. A customer for whom verification of identity proves unusually difficult and who is reluctant to provide details.
2. A group of unconnected customers who share a common correspondence address.
3. A client who shows unusual concern for secrecy e.g. in identifying beneficial owner of the account, his employment/business or assets or fails to indicate a legitimate source of funds.
4. The excessive or unnecessary use of nominees.
5. The unnecessary granting of wide ranging Powers of Attorney
6. The utilization of a client account rather than the payment of things directly.
7. An unwillingness to disclose the sources of funds

Dealing with High Risk Jurisdictions

1. Investors based in countries where production of drugs or drug trafficking may be prevalent.

2. Funds credited into customer accounts from and to countries associated with the production, processing or marketing of narcotics or other illegal drugs; or other criminal conduct; or wire transfer to or from a banking secrecy-haven country or country generally known for money laundering and terrorist financing.
3. The sending or receipt of frequent or large volumes of wire transfers to and from offshore institutions
4. Customers transferring large sums of money to or from overseas with specific requests for payment in cash.
5. International transfers for accounts with no history of such transfers or where the stated business of the customer does not warrant such activity.
6. Significant changes in currency shipment patterns between correspondent banks.
7. Deposits that are followed within a short time by wire transfers of funds to or through a location of specific concern, such as a country with lax controls

Suspicious Behavior/Demeanor by an Employees of the Reporting Institution

1. There may be circumstances where the money laundering may involve employees of Reporting Institution. Hence, if there is a change in the employees' characteristics e.g. lavish lifestyles, unexpected increase in performance, etc. the Reporting Institution may want to monitor such situations

Issued by the Financial Intelligence Unit

January 2020