National Bank of Rwanda
Banki Nkuru y'u Rwanda

KN 6 Av.4/P.O. Box 531 Kigali-Rwanda
Tel: (+250) 788199000 /
Website: www.bnr.rw /
E-mail: info@bnr.rw /
Swiftcode: BNRWRWRW /
Twitter: @CentralBankRw

The Governor

GENERAL GUIDELINES Nº 4230/2023–00076 [614] ON ANTI-MONEY LAUNDERING, COMBATING TERRORIST FINANCING, AND COUNTER FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION FOR REGULATED INSTITUTIONS

October, 2023

CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AML /CTF	Anti-Money Laundering and Combating Terrorism Financing
AML/CTF LAW	Law nº 028/2023 of 19/05/2023 on the prevention and punishment of money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction
ATM	Automated Teller Machine
CDD	Customer Due Diligence
CRB	Credit Reference Bureau
EFT	Electronic Funds Transfer
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FFI	Foreign Financial Institutions
FIC	Financial Intelligence Centre
FSRBs	Financial Action Task Force Style Regional Bodies
IMF	International Monetary Fund
KYC	Know Your Customer
LCTR	Large Currency Transaction Reporting
MER	Mutual Evaluation Report
MIS	Management Information System
MOU	Memorandum of Understanding
NBR	National Bank of Rwanda
NCCT	Non-Cooperative Countries and Territories
PEP	Politically Exposed Person
RRA	Rwanda Revenue Authority
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication

1. CHAP 1: GENERAL INFORMATION

1.1. Introduction

Over the last couple of decades, the world has experienced phenomenal growth of financial services. Countries have globalized services to easy business conduct. This globalization has consequently led to increased cross-border activities pursuing global financial intermediations. Subsequently, this development has been accompanied by a wave of transnational organized crimes including Money Laundering, Terrorist Financing (ML/TF) and Financing of Proliferation of Weapons of Mass Destruction perpetuated by enigmatic persons. It is worth noting that Money Laundering, Terrorist Financing (ML/TF) and Financing of Proliferation of Weapons of Mass Destruction affect financial life globally and negatively impact the entire economic, political and social development of the world including Rwanda. These grave financial and inhumane crimes have imposed numerous serious challenges to all countries in 2021 than ever.

After experiencing a huge gravity of these crimes, the whole world is now more than ever before placed in situation where there is a serious need for all countries to adopt strong Money Laundering, Terrorist Financing (ML/TF) and Financing of Proliferation of Weapons of Mass Destruction mechanisms that are coupled with the enhancement of transparent financial integrity. Like so many other countries, Rwanda is also determined to strive for a sound and stable financial system. In doing so, the latter is demanded to join global efforts to minimize the plague of the three mentioned crimes.

In line with the above background, the Government of Rwanda has demonstrated willingness in the global fight against the mentioned Crimes. The AML/CTF Law was adopted in 2018 and amended in 2020 to created obligations on reporting persons to establish a regime of preventive measures to manage the risk of abuse in the context of three mentioned crimes. The mentioned Law requires regulated institutions to undertake due diligence on their customers, maintain appropriate records, monitor customer transactions, report suspicious transactions, and develop internal system of controls to effectively manage their AML/CTF programs.

In the effort to eradicate and where possible surpass financial crimes practices in Rwanda and elsewhere in the world, the country has joined different blocks both regional and global. Currently Rwanda is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force (FATF) Fashioned Regional Body whose sole objective is to combat Money Laundering, Terrorist Financing (ML/TF) and Financing of Proliferation of Weapons of Mass Destruction by implementing FATF 40 Recommendations.

Extensively, the objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. The International standards and regulatory instruments would remain unproductive if they are not properly enforced. There is therefore a comprehensive need that all stakeholders in the financial sector play their part in enforcement of these responsibilities.

Furthermore, in pursuit of the above goal and in order to dissuade the risk of ML/TF, the Central Bank issued these general guidelines to be enforced by all regulated institutions under its supervisory purview and to guide them in the course to combat the crimes of Money Laundering, Terrorist Financing (ML/TF) and Financing of Proliferation of Weapons of Mass Destruction and fully implement international regulatory standards.

1.2. Interpretation

With reference to AML/ CTF Law and FATF standards, the following terms and expressions used in these general guidelines shall have the following meanings.

1. Centre:	Center in charge of financial intelligence.
2. Central Bank:	National Bank of Rwanda
3. Beneficiary Institution:	refers to the institution which receives the wire transfer from the ordering institution directly or through an intermediary institution and makes the fund available to the beneficiary.
4. Correspondent Financial Institution Service:	is the provision of financial services by one financial institution (the correspondent financial institution) to another financial institution (the respondent financial institution).
5. Cross-Border Wire Transfer:	Refers to any wire transfer where the ordering reporting entity and beneficiary institutions are in different countries. This term also refers to any chain of wire transfer in which at least one of the institutions involved is located in a different country.
6. Domestic Wire Transfer:	Refers to any wire transfer where the ordering financial institution and beneficiary financial institution are in Rwanda. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of Rwanda, even though the system used to transfer the payment message may be located outside Rwanda.
7. Non-Face to Face:	Identification of an individual when that individual is not present. The individual's information must be consistent and/ & or corresponds with that is recorded;
8. Occasional Customer:	occurring or appearing of a customer at irregular or infrequent basis, who appears now and then.

9. **Originator*:***	the originator is the account holder, or where there is no account, the (natural or legal) person that places the order with the financial institution to perform the wire transfer.
10. **Respondent Bank:**	refers to bank or reporting institution outside Rwanda to which correspondent banking services in Rwanda are provided.
11. **Wire/Fund Transfer:**	For the purposes of this Directive, wire transfer and funds transfer refer to any transaction carried out on behalf of an originator person through a licensee by electronic means for availability to a beneficiary person at another financial institution. The originator and beneficiary may be the same person.
Other terms that are in these guidelines have the same meaning as provided for in the AML/CFT Law.	

1.3. Objectives

These general guidelines intend to assist regulated institutions understand and comply with applicable AML/CTF requirements and measures contained in the AML/CTF Law and related legal instruments as well as AML/CTF international best practices.

They are also intending to help regulated institutions meet Central Bank and FIC's expectations regarding implementing AML/CFT risk management practices.

1.4. Scope

These general guidelines set out among others the:

a. Obligations of regulated institutions with respect to the requirements imposed under the AML/CTF Law and FIC Regulations and Directives as well as FATF recommendations.

b. Requirements imposed to regulated institutions in implementing a comprehensive risk-based approach in managing ML/TF risks; and

c. Roles of the regulated institutions' Board of Directors, Senior Management and staff in putting in place the relevant AML/CTF measures.

1.5. Applicability

These general guidelines are applicable to the institutions supervised by the Central Bank notably banks, life insurances and intermediaries, deposit taking microfinance institutions, payment services providers, forex bureaus, non-deposit taking financial service providers,

Trust and Company Service Providers where applicable as well other financial service providers regulated by Central Bank. The Central Bank may issue specific guidelines to specific sector where deemed necessary.

1.6. Relationship with Existing Policies

These general guidelines shall be read together with existing laws, regulations and Directives issued by The Central Bank and/ or FIC concerning prevention of Money Laundering, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction and as well as FATF recommendations and International Standards regarding the latter.

CHAP 2: MONEY LAUNDERING AND TERRORIST FINANCING

2.1. The Meaning of Money Laundering

Money Laundering is a process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities in order to avoid prosecution, conviction, and confiscation of the illegally obtained funds.

2.1.1. Money Laundering Possible Stage

The laundering process is typically accomplished in three stages, which may comprise numerous transactions by the launderer that could trigger suspicion on ML. The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, they may overlap.

a. **Placement** - the physical disposal of the initial proceeds derived from illegal source.

b. **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

c. **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

2.2. The Meaning of Terrorist Financing

The terrorist financing is defined in article 2 of the AML/CFT Law and is criminalised by the same law.

2.2.1. Understanding of the Terrorism Financing Processes

The methods used by terrorists and their associates to generate funds from illegal sources slightly differ from those used by traditional criminal organisations. Terrorists and their support organisations generally use the same methods as criminal groups to launder funds. Terrorist's ultimate aim is not to generate profit from his fundraising mechanisms but to obtain resources to support their operations. When terrorists obtain their financial support

from legal sources (donations, sales of publications, etc.), there are certain factors, outlined below, that make the detection and tracing of these funds more difficult. The apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

The size and nature of the transactions involved - the funding needed to mount to a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex, and many involve the movement of small sums through wire transfers. Enhanced due diligence techniques are therefore required to identify transactions related to terrorism financing. Terrorist financing is an offence in itself and also a predicate offence for money laundering. Thereafter, it would be noted that the most basic difference between terrorist financing and money laundering involves the origin of the funds in question. The chat below describes the preliminary differences of the two alarming concepts.

2.2.2. Difference between Money Laundering & Terrorism Financing

Comparisons	Money Laundering	Terrorist Financing
Source of Funds	Internally from within criminal organizations	Internally from self-funding cells (increasingly centred on criminal activity) Externally from benefactors and fundraisers
Motivation	Profit	Ideological
Conducts	Favours formal financial system	Favours cash couriers or informal financial systems such as currency exchange bureaus
Detection Focus	Suspicious transactions, such as deposits uncharacteristic of customer's wealth or the expected activity, which lead to relational links	Suspicious relationships, such as wire transfers between seemingly unrelated parties, which lead to transactional links
Transaction Amounts	Large amounts often structured to avoid reporting requirements	Small amounts usually below reporting thresholds
Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares, and offshore secrecy havens	No workable financial profile of operational terrorists exists
Money Trail	Circular - money eventually ends up with person who generated it	Linear - money generated is used to propagate terrorist group and activities.

2.3. Financing of the Proliferation of Weapons of Mass Destruction

Financing of the Proliferation of Weapons of Mass Destruction is defined in Article 2 of the AML/CFT Law and is criminalised by the same law.

2.3.1. Assessing Proliferation Financing (PF) risk

Regulated institutions are required to take appropriate steps, to identify and assess their proliferation financing risks. This may be done within the framework of their existing targeted financial sanctions and/or compliance programs.

They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of proliferation financing risks should be appropriate to the nature and size of the business. Regulated institutions should always understand their proliferation financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

2.3.2. Mitigating PF risk

Regulated institutions should have policies, controls and procedures to manage and mitigate effectively the risks that have been identified. This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

2.4. Risks Associated with ML/ FT and the Need for Compliance

ML/TF can pose various risks to regulated institutions. There are five major risks associated with ML/ TF which include: compliance and legal risk, operational or transactional risk, reputational risk, credit risk, and liquidity risk. It is worth noting that all these risks are interconnected, and each can have a direct influence upon any of the others causing significant financial loss to institutions.

2.4.1. Compliance and Legal Risk

Legal risk is the potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an institution, or even closure of such an institution. Regulated institution faces increased compliance and legal risk when it violates or ignores laws, rules, and regulations designed to prevent either ML or TF. Compliance and legal risk often blend with and increases operational risks and risks associated with transaction processing.

2.4.2. Operational Risk or Transactional Risk

Operational risk is defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. The risk can arise in instances in which there is a failure in the institution's systems designed to protect it from ML/ TF risk.

2.4.3. Reputational Risk

Reputational risk is defined as the potential that adverse publicity regarding a regulated institution's business practices, whether accurate or not, will cause loss of confidence in the integrity of the institution. A regulated institution can easily become a victim for illegal activities perpetrated by its customers or employees. Incidences of fraud may indicate that the concerned institution is not managed with integrity and skills expected of a regulated institutional organization. Public perception that the institution is not able to manage its operational risks effectively can damage its reputation.

Public confidence in regulated institutions can also be undermined, and their reputation may be damaged, as a result of association with illicit activity. Loss of confidence may adversely affect the business of regulated institution and the integrity of the entire financial system. In view of this, every institution needs to protect itself by means of continuous vigilance through an effective AML/CTF programs.

2.4.4. Credit and Concentration Risk

Credit and concentration risk is the potential for loss resulting from too much credit or loan exposure to one borrower. Credit and Concentration risk applies both to the asset and liability sides of the balance sheet.

Restrictions are normally imposed to prevent an institution's exposure to single borrowers or group of related borrowers from exceeding prescribed limits. An institution could be exposed to credit risk where the money launderer's assets have been frozen and is no longer able to service the loan facility.

2.4.5. Liquidity Risk

A financial institution's liquidity can be detrimentally affected by adverse publicity related either to ML violations or involvement in TF activities. Customers, upon hearing of the financial institution's involvement, may decide to withdraw funds or to discontinue transacting with Financial Institutions. In addition, correspondent financial institutions may cut off business relationships which will impact on the institution's ability to operate in international financial markets.

CHAP 3: AML/CFT RISK BASED APROACH

3.1. The Meaning of Risk Based Approach (RBA)

The RBA to AML/CTF means that regulated institutions are expected to identify, assess and understand the ML/TF risks to which they are exposed to and take AML/CTF measures commensurate with those risks in order to mitigate them effectively.

When assessing ML/TF risk, regulated institutions shall analyse and seek to understand how the ML/TF risks they identify affect them. The risk assessment therefore provides the basis for the risk-sensitive application of AML/CTF measures. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CTF risks, but it is still used for ML or TF purposes. A Risk Based Approach does not exempt regulated institutions from mitigating ML/TF risks where these risks are assessed as low.

3.2. AML/CTF Risk Assessment Process

Regulated institutions should assess and identify the ML/TF risks to which they are exposed. These risks are associated with the regulated institutions' corporate structure, and business models and more specifically arise from its products & services, customers, geographic regions and distribution channels. Regulated institutions must therefore understand the economic, business, and criminal environments in which they operate.

Regulated Institutions need to undertake a formal ML/TF risk assessment and document the findings of this exercise. The assessment shall be commensurate with the size, nature, and complexity of the corporate structures and business models.

The outcomes of the risk assessment shall be communicated to the Board and Management involved in managing ML/TF risks. Regulated Institutions must have compliance programs in place and must initiate and document a review of relevant policies procedures and risk assessment processes in order to evaluate their effectiveness. An internal or external auditor must review the adequacy and completeness of risk assessment and risk management practices every year.

3.3. Identifying Specific Risk Categories

Regulated institutions should also be aware of the ML/TF risks that exist in Rwanda in general. At a national level, this process requires the identification of risk factors associated with ML/TF threats and vulnerabilities. Threats are a function of the general levels of criminal and terrorist activity to which a country is exposed. Vulnerabilities are a function of political, (the characteristics of the political system), economic, (the nature of economic activity) social, (demographic characteristics), technological (level of technological advancement), environmental (issues related to the physical environment) and legislative (the coverage, maturity and effectiveness of the legislative system) factors.

Regulated institutions must first identify the specific products, services, individual and corporate customers, delivery channels, and geographic locations that pose ML/TF risk to the financial institution. When preparing risk assessments, specifically regulated institutions shall consider factors such as the number and volume of transactions, the nature of the customer relationships, and whether interaction with customers is face-to-face or via electronic banking (non-face-to-face) means (for example, internet banking, mobile banking).

An effective risk assessment is an ongoing process. Risk levels may change as new products are offered, new markets are entered, high-risk customers open or close accounts, or as the regulated institution's products, services, policies, and procedures

change. The regulated institution shall therefore update its risk assessment annually to take account of these changes and this updated risk assessment must be presented to the Board.

3.4. Products and Services Risk

A regulated institution's level of exposure to ML/TF risk is likely to vary depending on the nature of its products and services. A higher degree of risk may exist in cases where, for example, regulated Institutions are involved in international transactions, or high volumes and value transactions. Some of these products and services are listed below, but the list is not all inclusive:

a. Electronic funds transfer services:

b. electronic cash such as stored value cards or payroll cards, domestic and international funds transfers, and third-party payment processors;

c. remittance activity;

d. automated clearing house (ACH) transactions;

e. automated teller machines (ATMs); and Mobile Phone Financial Services;

f. Electronic Banking;

g. Foreign exchange and funds transfers;

h. Private banking;

i. Trust services;

j. Foreign correspondent accounts and foreign currency dominated accounts and Trade finance;

k. Lending activities, particularly loans secured by cash collateral and marketable securities;

l. Account services such as non-deposit investment products or insurance products that allow large one-time or regular payments, pre-payments or deposits, to be made and subsequently withdrawn, as well as the provision of safety boxes;

m. Underwriting insurance policies and Placement of life insurance and other investment related insurance.

3.5. Customer Risk

All types of customers may, in certain circumstances, be involved in ML/ TF activities. Certain customers may pose specific risks depending on the nature of the business, the occupation of the customer, or the nature of anticipated transaction activity. As not all categories of customers pose the same level of risk, regulated institutions must always use

sound judgment to determine and define the level of risk for each individual customer.

To assess customer risk accurately, regulated institutions shall consider such variables as the customers' geographical location and the services they seek. The following list, although not exhaustive, indicates customers that are likely to pose a higher level of risk to the regulated institution:

a. Foreign financial institutions, including foreign money services providers such as foreign exchange bureaus, currency exchanges, and money transmitters;

b. Non-bank financial institutions such as money services businesses, casinos and card clubs, brokers & dealers in securities, and dealers in precious metals, stones, or jewels;

c. Politically Exposed Persons (PEPs), which includes their immediate family members and close associates;

d. Non-residents and accounts held by foreign individuals;

e. Foreign corporations and domestic business entities, and international business corporations located in high-risk geographic locations;

f. Foreign deposit brokers;

g. Businesses that, while not normally cash-intensive, generate substantial amounts of cash from certain lines of activity;

h. Non-Governmental Organizations, Religious Organisations and charities;

i. Professional service providers such as attorneys, accountants, or real estate brokers;

j. Second hand motor car dealers;

k. Customers conducting their business relationship or transactions in unusual circumstances, such as geographic distance from their financial institution for which there is no reasonable explanation;

l. Customers whose nature, structure or relationships make it difficult to identify the ultimate beneficial owner(s) of significant or controlling interests;

m. Dealers in precious metals and stones.

3.6. Delivery Channel Risk

This is the risk associated with how regulated institution's products and services are delivered to customers including services delivered to customers through face to face or non-face-to-face means. Categories of delivery channels that may indicate a higher risk could include:

a. Use of intermediaries or third parties, which may not be subject to AML/CTF laws and measures and who, are not adequately supervised;

b. The internet and electronic banking customers.

3.7. Geographic Location Risk

Regulated institution shall identify both domestic and international geographic locations that may pose a higher risk to its AML / CTF compliance program. Regulated institutions shall evaluate cases individually when assessing the risks associated with doing business, such as opening accounts or facilitating transactions, in certain geographic locations.

Categories of individuals and/or entities that indicate a higher risk include countries or jurisdiction: The United Nations website designates, and issues lists of individuals or entities suspected to be linked to terrorism as per United Nations Security Council Resolution 1373 on combating terrorism and 1267 Sanction Committee and FIs should screen customers/transactions against these lists of designated persons;

a. Persons identified as non-cooperative by the Financial Action Task Force on ML (FATF);

b. Persons identified by credible sources as providing funding or support for terrorist activities or the proliferation of weapons of mass destruction;

c. Persons identified by credible sources as having significant levels of corruption or other criminal activity;

d. Persons identified by the regulated institution as high risk because of its prior experiences or other factors such as legal considerations or allegations of official corruption.

3.8. Updating the Risk Assessment

An up-to-date AML/CTF risk assessment helps control the risks associated with the regulated institutions' activities as they relate to its products, services, customers, delivery channels and geographic locations. To keep the regulated institution's risk assessment current, the regulated Institution's management shall subject them to, at least annual review and make appropriate changes that reflect the regulated institution's true risk profile.

In addition, regulated institution management shall review the risk assessment's adequacy when the regulated institution adds new products or services, opens accounts with high-risk customers, expands through mergers or acquisitions or opens new branches or subsidiaries and when there is an occurrence of relevant domestic or international events. Even in the absence of such changes, it is a sound practice for regulated institutions to periodically reassess their AML/CTF risks at least every year.

3.9. Analysis of Specific Risk Categories

The second step of the regulated institution's risk assessment process includes a detailed

analysis of the data obtained during the identification stage, allowing the regulated institution to assess ML / TF risk more accurately. The regulated institution evaluates data pertaining to its activities, which shall be considered in relation to both the regulated institutions' Customer Identification Program (CCI) and Customer Due Diligence (CDD) information. This more detailed analysis is important as a step in the assessment process because individual account holders will pose varying levels of risk depending on the products or services that they intend to use together with their geographic location and which delivery channel(s) is used.

The analysis also provides management with a better understanding of the regulated institution's risk profile and will assist management in developing appropriate policies, procedures, and processes to mitigate the overall ML/TF risk to the regulated institution.

While the level and sophistication of the specific risk categories will vary from regulated institution to regulated institution, analysis of the data pertaining to the regulated institution's activities shall specifically take into account, as appropriate, the following:

a. Purpose of the account;

b. Actual or anticipated activity in the account;

c. Nature of the customer's business;

d. Customer's location;

e. Types of products and services a customer uses; and

f. The method by which the customer interacts with the institution, i.e., delivery channels.

3.10. Group-wide ML/ TF Risk Assessment

Financial institutions are required to implement programs against money laundering and terrorist financing. Financial groups shall be required to implement group-wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions are required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programs against money laundering and terrorist financing.

In such cases, FI shall assess individual risk within business lines and the group-wide risk across all activities and legal entities. The holding company shall frequently update and reassess the ML/TF risks throughout the organization and shall communicate any changes to appropriate business units, functions, and legal entities. A risk or deficiency that exists in one part of the organization may increase concerns in other parts, and financial institution management shall quickly and diligently address these concerns throughout the organization.

3.11. Rating and Ranking

An appropriate methodology shall assign appropriate ML and TF risk levels to the pertinent activities of the regulated institution and in so doing, identify the higher risks to which enhanced due diligence and ongoing monitoring must be applied. The criteria used for rating and ranking shall have a rational basis in ML and TF risk and address ML and TF risk factors that are unique to specific business lines, areas and jurisdictions, and other general risk factors such as products and services and delivery channels.

3.12. Using Assessment of Inherent Risks as the Basis for Risk Mitigants

Results of the assessment of inherent risk assessment shall inform the development of risk mitigants, and the allocation of resources, commensurate with levels of ML and TF risk in the regulated institution. Certain risk mitigants measures are prescribed by regulatory requirements and for example:

a. Identifying and verifying customer identification documents;

b. Determining under prescribed circumstances whether a customer is a Politically Exposed Person;

c. Reporting suspicious transactions and attempted suspicious transactions;

d. Reporting large currency transactions;

e. Reporting large EFTs;

f. Applying enhanced due diligence measures to business relationships and transactions with legal and natural persons and FIs from countries for which this is called by the FATF or by the FIU or competent authorities in Rwanda; and

g. Record keeping.

3.13. Development of the regulated institution's AML & CTF Programs using the Risk Assessment

An effective risk management process will enable regulated institution management and the board to develop AML/CTF programs that both address and mitigate any gaps in the regulated institution's controls. Accordingly, regulated institution management should use the risk assessment results to develop appropriate policies and procedures that address the risks posed to the regulated institution by potential ML and TF activities. The regulated institution's monitoring system shall then focus on those high-risk products, services, customers, delivery channels and geographic locations that have been identified through its ML/TF risk assessment.

A regulated institution shall validate its ML/TF risk management practices by requiring an independent review of its compliance program. The internal or external auditor shall, as part of the audit, independently test the regulated institution's policies, procedures, and overall compliance with its AML/CTF programs.

3.14. Cross Border Correspondent Banking Relationships.

For the purpose of these Guidelines, "correspondent banking" is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank'). Correspondent banking relationships with foreign financial institutions (FFIs) are identified by the FATF as a specific higher risk area, and consequently the AML / CTF law prescribes measures to be applied by financial institutions enter into that correspondent relationships with FFIs and their customers. Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

a. gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

b. assess the respondent institution's AML/CFT controls;

c. obtain approval from senior management before establishing new correspondent relationships;

d. clearly understand the respective responsibilities of each institution; and

e. with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

Financial institutions shall check that their correspondent banks don't allow their accounts to be used by shell banks. Requests for correspondent financial institutions services received from an institution incorporated in a jurisdiction in which it has no physical presence, shall be declined. Shell financial institutions can be easily purchased by criminals and used for ML. In deterrence, Financial Institutions shall:

a. Review the FFI's ownership and background;

b. Be satisfied that the FFI's activities are authorized, regulated and supervised by the relevant regulatory authority in its home country;

c. Meet or otherwise communicate with senior representatives of the FFI to understand their commitment to effective control of ML and TF and understand key provisions of the FFI's AML/ CTF policies and procedures such as customer CDD; and

d. Use the services of credible third parties (such as those providing a document

repository or AML/CTF rankings) as a source of additional information on the FFI and its regulatory environment.

Where a financial institution ascertains that there are civil or criminal sanctions imposed against an FFI in respect of AML/CTF requirements; or ascertains that an FFI does not have in place AML/CTF policies and procedures as specified in the AML/CTF law or AML/CFT best practices, the relationship shall be terminated.

3.15. Electronic Funds Transfers (EFTs)

Investigations of major ML and TF cases over the past years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the originator is not clearly shown in an electronic payment message instruction.

To ensure that EFT systems are not used by criminals as a means to break the audit trail; financial institutions conducting ETFs of EUR/USD 1,000 or more shall obtain and maintain the following information relating to the originator of the wire transfer:

a. The name of the originator,

b. The originator ‘s account number (or a unique reference number if no account number exists); and

c. The originator ‘s address (the address can be substituted with a national identity number, customer identification number or date and place of residence or domicile).

For all wire transfers, the ordering financial institutions shall verify the identity of the originator in accordance with the CDD requirements contained in the Guideline.

For cross-border wire transfer, the ordering financial institutions shall include the full originator information above in the message or the payment form accompanying the wire transfer. Where however, several individual cross-border wire transfers from a single originator are bundled in a batch-file for transmission to beneficiaries in another country, the ordering financial institution shall only include the originator ‘s account number or unique identifier on each individual cross-border wire transfer, provided that the batch-file (in which the individual transfers are batched) contains full originator information that is fully traceable within the recipient country. For domestic wire transfers, the ordering financial institution shall either:

a. Include the full originator information in the message or the payment form accompanying the wire transfer; or

b. Include only the originator ‘s account number or a unique identifier, within the message or payment form.

Nonetheless, the preceding option (b) must be permitted by the financial institution only if full originator information can be made available to the beneficiary financial institution and

to the appropriate authorities within three (3) business days of receiving the request. Each intermediary and beneficiary financial institution in the payment chain shall also ensure that all originator information that accompanies a wire transfer is transmitted with the transfer.

Where technical limitations prevent the full originator information accompanying a cross-border wire transfer (during the necessary time to adapt payment systems), a record must be kept for ten (10) years by the receiving intermediary financial institution of all the information received from the ordering financial institution. Beneficiary financial institutions also shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. The lack of complete originator information is considered as a factor in assessing whether a wire transfer or related transactions are suspicious.

Financial Institutions shall take reasonable measures to ensure that incoming EFTs include originator information. Financial institutions that act as intermediary shall develop and implement reasonable policies and procedures for monitoring payment message data subsequent to processing. Such measures shall facilitate the detection of instances where required message fields are completed but the information is unclear, or where there is meaningless data in message fields. Reasonable measures shall include:

a. Contacting the originator's financial institution or precedent intermediary financial institution to clarify or complete the information received in the required fields;

b. Considering (in the case of repeated incidents involving the same correspondent or in cases where a correspondent decline to provide additional information) whether the relationship with the correspondent or the intermediary financial institution shall be restricted or terminated and filing a suspicious transaction report;

c. Financial institutions shall conduct enhanced scrutiny of, and monitor for suspicious transaction, incoming funds transfers which do not contain complete originator information.

d. The beneficiary financial institution shall, based on its assessment of ML/TF risk, consider restricting or even terminating its business relationship with financial institutions that fail to meet the above requirements. The reasons for decisions taken shall be documented.

3.16. Use of Agents

Some financial institutions rely on introducers, intermediaries or other third parties for customer information gathering and verification purposes. ML and TF risk mitigation can be compromised where financial institutions do not ensure that appropriate customer identification standards are applied by agents.

Accountability for ascertaining the identity of the customer and obtaining the information used to identify the customer remains with the financial institutions when it uses a third party to ascertain the identity of customers. In respect of this accountability, financial institutions shall have an agreement or arrangement in writing with the agent if such person is to be responsible for customer identification and verification.

Documentation of relationships, communications, and customer due diligence of agents shall be complete and current, and customer information shall be placed in the customer's record promptly upon receiving it. Financial Institutions shall consider terminating relationships with agents that do not comply with agreed upon customer identification responsibilities with the requisite customer information on a timely basis. Contracts with agents shall be reviewed and updated as necessary to ensure compliance with the AML/ CTF law and regulations.

Financial institutions that rely upon a third party to conduct its CDD shall satisfy that they shall immediately obtain from third party the necessary information concerning certain elements of the CDD process. FIs should have clear policies and procedures on whether and when it is acceptable and prudent to rely on a third party. Such reliance in no way relieves the financial Institution of its ultimate responsibility for having adequate CDD policies and procedures and other AML/CFT requirements on customers, such as understanding expected activity, whether customers are high-risk, and whether transactions are suspicious.

3.17. New and Developing Technologies

Developments in technology frequently drive the creation of new financial institution products and services. Such developments can lower costs, improve customer service and expand markets.

Financial institutions shall have policies and procedures in place to ensure that new and developing technologies are included in the financial institutions inherent risk assessment process. In this way financial institutions can ensure that appropriate AML/CTF controls are in place, and, where appropriate, develop or amend controls to take new risks into account.

Financial institutions shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Such risk assessment shall take place prior to the launch of the new products, business practices or the use of new or developing technologies. Thus, financial institutions shall take appropriate measures to manage and mitigate these risks.

3.18. Trade Finance

Trade-based ML and TF refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities.

Financial institutions that outsource trade finance services to other financial institutions shall ensure that this outsourcing is included in the financial institution's inherent risk assessment. If the assessment indicates that the risk of ML and TF is elevated, the financial institutions shall implement reasonable measures to control the risk. Reasonable measures could include:

a. Conducting an analysis of the provider's policies and practices; and

b. Communicating to the provider what AML/CTF control measures the financial institution expects the provider to have in place;

c. The financial institution shall have the right to audit such measures.

The Central Bank recognizes that financial institutions whose services are used to make trade finance payments on an open account basis may not have an opportunity to review the nature of a customer's underlying trade transaction. Reasonable measures to address this risk could include:

a. Periodic verification, using credible open-source material or information, of the business of the customer that triggers the need for such payments;

b. Periodic review of EFT data to determine whether the customer's business includes significant trade activity;

c. Periodic review of the customer's transactions compared to the financial institutions' record of the intended purpose of the account;

d. Meeting or other interaction with the customer; or

e. Periodic confirmation that the customer is not in a type of business to which the financial institution has decided, as a matter of policy, not to provide financial institution services.

The FATF has advised that the laundering of funds through under and over-invoicing is one of the oldest methods of fraudulently transferring value across borders and remains a common practice. The key element of the technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

By invoicing the same good or service more than once, a money launderer may be able to justify multiple payments for the same shipment of goods or delivery of services, especially if more than one financial institution is used. Multiple invoicing avoids the need to misrepresent prices.

Where the assessed risk of ML/TF in trade finance services is elevated, financial institutions shall take reasonable measures designed to mitigate the risk of misuse of trade financing mechanisms. Reasonable measures could include:

a. Conducting periodic on-site assessments of the risks posed by customers and the procedures they follow;

b. Reviewing the routing of shipments and note ports of call or transhipment points that are inconsistent with a standard commercial transaction, or where the routing or the carrier is located in a high risk country;

c. Subjecting requests involving letters of credit to cover shipments of goods that are not consistent with the Applicant’s normal business patterns to more detailed review and noting the results in the customer’s records;

d. Identifying significant differences (either between different customers, different shipments or market quotes) in prices of a good or commodity being financed under a letter of credit and determining the business rationale for the differences.

3.19. Politically Exposed Persons (PEPs)

Politically exposed persons has the same meaning ascribed to it in article 2(w) of AML/CTF Law. The FATF Recommendations state that PEPs are potentially more susceptible to financial crime than other customers of financial institutions. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a financial institution to significant reputation and/ or legal risks.

Such PEPs be it local or foreign, are individuals who are or have been entrusted with prominent public functions, including heads of state or of Government, senior politicians; senior Government; judicial or military officials; senior executives of publicly owned corporations; important political party officials; their family members and their close associates.

The possibility exists that such persons may abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. Accepting and managing funds from local or foreign corrupt PEPs will severely damage the financial institutions' own reputation and can undermine public confidence in the ethical standards of an entire financial system, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove; article 21 of AML/CTF outlines requirements for identifying a Politically Exposed Person. Financial institutions shall put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is PEP. It can reduce risk by conducting detailed due diligence at the out-set of the relationship including requiring a declaration of beneficial ownership and enhanced ongoing monitoring where a business relationship has been established with a PEP.

Financial institutions shall also take reasonable measures to establish the source of wealth and funds of the customer and beneficial owners identified as PEPs.

The source of wealth, for purposes of these guidelines, shall refer to the origin of a PEP's volume of wealth or total assets which shall include information on how much wealth a PEP would be expected to have accumulated, and how the PEP acquired such wealth. A Financial Institution shall conduct ongoing CDD measures on the business relationship with a PEP to ensure that the level and type of transactions are consistent with the reporting entity's knowledge of the PEP's sources of funds and sources of wealth. When conducting ongoing CDD, a financial institution shall take the following factors into account to ensure that the business relationship is commensurate with what could be reasonably expected from a PEP in particular circumstances:

a. The current income of a PEP;

b. Sources of funds;

c. Sources of wealth;

d. Business undertaking; and

e. Family businesses.

A Financial Institution may use different sources of information for verifying the accuracy of a PEP's sources of funds and sources of wealth, which may include but not limited to, public property registers, land registers, asset disclosure registers, past transactions, or information about legal and beneficial ownership where available.

There shall be no limit on the length of time the person, family member, or close associate needs to be treated as a PEP. Financial institutions are encouraged to consider the ongoing PEP status of their customers on a case-by-case basis using a risk-based approach. If the risk is low, financial institutions may consider declassifying the relationship, but only after careful consideration of continuing anti-money laundering risks and approval by senior management.

Financial institutions should assess which countries of origin of PEPs, with which they have banking relationships, to determine if they are vulnerable to corruption. Financial institutions which are part of an international group might also use the group network as another source of information and where financial institutions have business in countries vulnerable to corruption, they shall establish who are the senior political figures in that country and, shall seek to determine whether or not their customer has any connections with such individuals (for example their immediate family or close associates). Financial institutions shall note the risk that individuals may acquire such connections after the business relationship has been established.

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

In relation to life insurance policies, financial institutions should be required to take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, financial institutions should be required to inform senior management before the pay-out of the policy proceeds, to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.

CHAP 4: AML/ CTF GENERAL COMPLIANCE PROGRAMME

4.1. AML/CTF General Compliance Programme Overview

The AML/CTF compliance program is the key vehicle for establishing and maintaining effective control over ML and TF risks in all relevant areas of the RIs' operations.

The AML/CTF compliance program must be written, approved by the board of directors,

and noted in the board minutes. The compliance program should also be subject to regular review reflecting changes in the RI's risk assessment/profile.

A regulated Institution must have an AML/CTF compliance program commensurate with its respective AML/CTF risk profile.

The AML/CTF compliance program must provide for the following minimum requirements:

a. Internal controls to ensure ongoing compliance;

b. Designate an officer responsible for managing AML/CTF compliance at senior management level;

c. AML/CFT Training and awareness for relevant personnel;

d. Independent testing (Internal &External Audit) of AML/ CTF compliance;

e. On-going monitoring and reporting;

f. Record keeping and retention; and

g. Regulatory reporting and cooperation.

4.2. Risk Management Practices

The risk management practices incorporate the regulated institution's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the AML/CTF laws, regulations and the directive. The level of sophistication of the risk management framework shall be commensurate with the size, structure, risks, and complexity of the regulated institution.

The board is ultimately responsible for ensuring that the regulated institution maintains an effective AML/CTF risk management framework, including suspicious transaction monitoring and reporting. The board of directors and management shall create a culture of compliance to ensure staff adherence to the regulated institution's AML / CTF policies and procedures.

4.3. Governance

Regulated institutions are required to implement programmes to mitigate against ML/TF, which correspond to its ML/TF risks and the size of its business.

4.4. Board of Directors

Members of Board of Directors (Board members) shall understand their roles and responsibilities in managing ML/TF risks faced by the regulated institution. The board should establish the institution's overall risks appetite and should ensure that mechanisms are in place to effectively mitigate risk.

Board members must be aware of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services.

4.5. Roles and Responsibilities

The Board of Directors (Board) have the following roles and responsibilities:

a. Maintain accountability and oversight for establishing AML/ CTF policies and minimum standards;

b. Approve policies regarding AML/CTF measures within the regulated institution, including those required for risk assessment, mitigation and customer profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism and compliance;

c. Establish appropriate mechanisms to ensure the AML/ CTF policies are periodically reviewed and assessed in line with changes and developments in the regulated institution's products and services, technology as well as trends in ML/TF;

d. Establish an effective internal control system for AML/CTF and maintain adequate oversight of the overall AML/ CTF measures undertaken by the regulated institution;

e. Define the lines of authority and responsibility for implementing the AML/CTF measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

f. Ensure an effective independent audit function, in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

g. Assess the implementation of the approved AML/CTF policies through regular reporting and updates by the Senior Management and Audit Committee; and

h. Establish MIS that is reflective of the nature of the regulated institution's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

4.6. Senior Management

Senior Management is accountable for the implementation and management of AML/CTF compliance programmes in accordance with policies and procedures established by the Board, requirements of the law, regulations, general guidelines and the industry's standards and best practices.

4.7. Roles and Responsibilities

The Senior Management have the following roles and responsibilities:

a. Be aware of and understand the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services

offered and to be offered including new products, new delivery channels and new geographical coverage;

b. Formulate AML/CTF policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the regulated institution and its geographical coverage;

c. Establish appropriate mechanisms and formulate procedures to effectively implement AML/CTF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

d. Undertake review and propose to the Board the necessary enhancements to the AML/ CTF policies to reflect changes in the regulated institution's risk profiles, institutional and group business structure, delivery channels and geographical coverage;

e. Provide timely periodic reporting to the Board on the level of ML/TF risks facing the regulated institution, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CTF which may have an impact on the regulated institution;

f. Allocate adequate resources to effectively implement and administer AML/CTF compliance programmes that are reflective of the size and complexity of the regulated institution's operations and risk profiles;

g. Appoint a compliance officer at management level at Head Office and designate a compliance officer at management level at each branch or subsidiary;

h. Provide appropriate levels of AML/CTF training for its employees at all levels throughout the organization;

i. Ensure that there is a proper channel of communication in place to effectively communicate the AML/CTF policies and procedures to all levels of employees;

j. Ensure that AML/CTF issues raised are addressed in a timely manner; and

k. Ensure the integrity of its employees by establishing appropriate employee assessment system.

4.8. General Compliance and Management Arrangements

As provided in the AML/CFT Law its article 27 a reporting person shall establish the compliance functions (compliance Officer CO) at the management level and the CO shall be an independent oversight and to whom all internal suspicious transaction reports will be made. The Compliance Officer acts as the reference point for AML/CTF matters within the reporting institution.

The Compliance Officer must have sufficient stature, authority and seniority within the reporting institution to participate and be able to effectively influence decisions relating to

AML/CTF. In this regard, he/she shall have access to all records/files to effectively carry out his/her activities.

The Compliance Officer is required to be "fit and proper" to carry out his AML/CTF responsibilities effectively.

The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF techniques and the AML/CTF measures undertaken by the industry.

Regulated Institutions should encourage the Compliance Officer to pursue professional qualifications in AML/CTF so that they are able to carry out their obligations effectively.

Regulated Institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented. The Compliance Officer has a duty to ensure the following:

a. The regulated institution's compliance with the AML/CTF requirements;

b. Proper implementation of the AML/ CTF policies;

c. The appropriate AML/CTF procedures, including CDD, record-keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism, are implemented effectively;

d. The AML/CTF mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;

e. The channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;

f. All employees are aware of the reporting institution's AML/CTF measures, including policies, control mechanism and the channel of reporting;

g. Internally generated suspicious transaction reports by the branch or subsidiary compliance officers are appropriately evaluated before submission to the FIC, NBR; and

h. The identification of ML/TF risks associated with new products or services or arising from the reporting institution's operational changes, including the introduction of new technology and processes.

i. Regulated institutions are required to inform, in writing, the Financial Intelligence Unit and National Bank of Rwanda, within ten (10) working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as may be required.

4.9. Employee Screening Procedures

The screening procedures shall apply upon hiring the employee and throughout the course of employment. Regulated institutions are required to establish an employee assessment system that is commensurate with the size of operations and risk exposure of regulated institutions to ML/TF. The employee assessment system shall include an evaluation of an employee's personal information, including criminal records, employment and financial history.

4.10. Employee Training and Awareness Programmes

Regulated institutions are required to conduct awareness and training programmes on AML/CTF practices and measures for their employees. Such training must be conducted regularly and supplemented with refresher courses.

The employees must be made aware that they may be held personally liable for any failure to observe the AML/CTF requirements.

The regulated institution must make available its AML/CTF policies and procedures for all employees and its documented AML/CTF measures must contain at least the following:

a. The relevant documents on AML/CTF issued by NBR or relevant supervisory authorities; and;

b. The reporting institution's internal AML/CTF policies and procedures;

c. The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by reporting institutions;

d. Employees who deal directly with the customer shall be trained on AML/CTF prior to dealing with customers; and

e. Training for all employees may provide a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.

In addition, training may be provided to specific categories of employees.

4.11. Front-Line Employees

Front-line employees may be trained to conduct effective on-going CDD, detect suspicious transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training may also be provided on factors that may give rise to suspicion, such as dealing with occasional customers transacting in large cash volumes, PEPs, higher risk customers and the circumstances where enhanced CDD is required.

4.12. Employees that Establish Business Relationships

The training for employees who establish business relationships may focus on customer

identification, verification and CDD procedures, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with a new customer until CDD is completed satisfactorily.

4.13. Supervisors and Managers

The training on supervisors and managers may include overall aspects of AML/ CTF procedures, in particular, the risk-based approach to CDD, risk profiling of customers, enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures related to the financing of terrorism.

4.14. Compliance Officer

The AML/CTF CO shall receive periodic in-depth training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall AML / CTF risk profile of the regulated institution, typologies and emerging trends in ML/TF.

The CO will require extensive initial and ongoing instruction on the validation and reporting of suspicious transactions, on feedback arrangements, and on new trends and patterns of criminal activity.

4.15. Account Opening Staff

Account Opening Staff must receive training in respect of the need to verify a customer's identity and on the account opening and customer verification procedures available in the financial institutions. Account Opening Staff must also be familiarised with the recognition and handling of suspicious transactions and internal suspicious transaction reporting procedures.

4.16. International Trade Services Staff

International Trade Services Staff require special emphasis on trade-based ML and TF.

4.17. New Employees

New Employees must be given an overview of the AML/CTF requirements during orientation.

4.18. Refresher Training

It will be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities. Training shall be ongoing and incorporate current developments and changes to the AML/CTF and any related Laws and guidelines. Changes to internal policies, procedures, and monitoring systems shall also be covered during training. The program shall reinforce the importance that the board and senior management place on the regulated institutions' compliance with the AML/CTF and ensure that all employees understand their role in maintaining an effective AML/ CTF compliance program.

4.19. Staff Awareness

Regulated Institutions must take appropriate measures to make employees aware of:

a. Results of the regulated institutions' ML/TF risk assessment. Policies and procedures put in place to prevent ML and TF including those for identification, record-keeping, the recognition and handling of suspicious transactions and internal reporting.

b. The legal requirements contained in the FATF recommendations, the AML/CTF Laws and regulations and all other related legal documents e.g. Guidelines.

c. Their own personal statutory obligations and the fact that they can personally be liable for failure to report information in accordance with the law.

d. New developments, including information on current ML/TF techniques, methods and trends.

4.20. Records of Training Documents

Regulated institutions shall keep records of their training materials delivered to their employees and be available for regulatory review. These shall include:

a. Training and testing materials;

b. The dates of training sessions;

c. Attendance records, and

d. Participants' designations.

4.21. Independent Audit Function

As required by Article 27 (c) of the AML/CFT Law, independent audit shall be conducted by the internal audit department or external auditors, consultants, or other qualified independent parties. A sound practice is for the regulated institutions to conduct independent audit generally annually, commensurate with the AML/CTF risk profile of the regulation institution. The persons conducting the AML/ CTF testing shall report directly to the board or to a designated board committee.

Officers responsible for conducting an objective independent evaluation of the written AML /CTF compliance program shall perform audit for specific compliance with the ML/TF Laws and regulations as well as evaluate pertinent MIS.

The audit shall be risk based and evaluate the quality of risk management for all financial institution operations, functions, and subsidiaries.

Risk-based audit programs will vary depending on the regulated institution' size, complexity, scope of activities, risk profile, quality of control functions, geographic

diversity, and use of technology; an effective risk-based auditing program will cover all of the regulated institution' activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment.

Risk-based auditing enables the board and auditors to use the regulated institutions' risk assessment to focus the audit scope on the areas of greatest concern.

The audit shall assist the board and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls; the scope of independent audit shall include, at a minimum:

a. Compliance with AML/CFT law, FIC regulations and Directives as well as regulations and general guidelines of supervisory authority;

b. Compliance with the reporting institution's internal AML/CFT policies and procedures;

c. Adequacy and effectiveness of the AML/CFT compliance programme; and

d. Reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

Auditors shall document the audit scope, procedures performed, transaction testing completed, and findings of the review. All audit documentation and work papers shall be available for regulatory review. Any violations, policy or procedures exceptions, or other deficiencies noted during the audit shall be included in an audit report and reported to the board of directors or a designated committee in a timely manner. The Financial Institution shall track audit deficiencies and document corrective actions taken by management.

Reporting to Senior Management and the Board, Senior Management and the Board shall ensure they receive sufficient pertinent information from the CO, the Auditor and other sources as appropriate, to enable them to ensure the overall adequacy and effectiveness of the AML/CTF program.

AML/ CTF reports on effectiveness audit made at different times (for example, during audits of different business areas) shall be collated and consolidated periodically. This will support the goal of assessing overall adequacy and effectiveness; regulated institution shall ensure that AML/CTF reporting to Senior Management and the Board by the CO and by the Internal Auditor is not unduly commingled with reports on other aspects of the RI's activities, in order to differentiate the contents and purpose of the reporting; The reports from the CO shall include information about the regulated institutions notably:

a. Significant patterns or trends;

b. The self-assessment of controls and material changes thereto; and

c. Remedial action plans or recommendations, if any, with milestones and target dates for completion.

Where appropriate, the CO shall draw conclusions, offer advice or make recommendations

about the overall structure and scope of the AML/ CTF program.

4.22. General Reporting Requirements

Regulated Institutions shall accurately and consistently report to Central Bank all the required information as detailed in this guideline and other relevant legal instruments, in the following manner.

4.22.1. On Weekly Basis:

Number of STR and CTRs reported to FIC.

4.22.2. On Monthly Basis:

a. Total Politically Exposed Persons' accounts and related amounts maintained by the financial institutions with their related parties identified.
b. Report all suspicious activities and incidents of fraud when such activities/incidents are material to the safety, soundness, or reputation of the institution.

4.22.3. On Quarterly Basis:

a. Report all staff training undertaken (list of participants, time of the training, summary of the content),

b. Report all staff sanctions that are related to fraudulent activity.

c. Report all the compliance officer reports to the management.

4.22.4. On an annual basis:

a. AML/CFT Risk assessment,

b. AML/CFT Policies and procedures

c. Customer acceptance policy and procedures,

d. Employee training and education program,

e. Reports of adequacy testing of AML/CFT program conducted by an independent entity or by the Internal audit function of the financial institution,

f. Any additional areas of ML/TF risk; (new area of risk identified by the financial institution and controls implemented).

4.22.5. The Central Bank reserves the right to request any information related to AML/CFT compliance.

4.23. Policies and Procedures

Policies and procedures shall identify and implement measures designed to control inherent ML/TF risks.

Regulated institutions shall ensure that policies and procedures are kept up to date to mitigate risks. They must also comply with all other regulatory requirements.

Policies and procedures shall be embedded in business areas commensurate with the risks they are intended to mitigate, and otherwise tailored to the particular circumstances in which they operate.

4.24. Policies

AML/CTF policies shall set risk management standards to govern the approach of the regulated institutions to deterring and detecting ML and TF risks and shall ensure regulatory compliance.

At a minimum AML/CTF policies shall cover the following:

a. Objectives of the AML/CFT program;

b. Key areas of inherent risk;

c. Customer due diligence standards reflecting:

    i. minimum acceptable customer identification requirements, verification standards, information gathering and monitoring;

    ii. prohibition on entering customer relationships or processing transactions if identity cannot be ascertained;

    iii. appropriate or prescribed restrictions on entering customer relationships or processing transactions before identity is established;

    iv. the types of customers considered higher risk or acceptable to the financial institution;

    v. a definition of enhanced due diligence applicable to such higher risk customers;

    vi. reporting; and

    vii. records retention;

d. Identification of customers whose accounts were opened prior to the coming into effect of the new AML/CFT Law, and who have not been identified in accordance with the subsequent laws and regulations on a risk-based approach.

e. The mandates of key risk management control functions such as the Board, Senior Management, the CO, the Internal Auditor, and others.

f. Provide for program continuity despite changes in management or employee composition or structure.

g. Ensure that adequate controls are in place before new products are offered.

h. Meet all regulatory record keeping and reporting requirements and recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.

i. Provide for dual controls and the segregation of duties to the extent possible.

j. Train employees to be aware of their responsibilities under the AML/CFT Law, related regulations and internal policy and guidelines.

k. Provide for transaction monitoring against customer profiles.

4.25. Procedures

Procedures are the tools regulated institutions use to translate AML/ CTF policies into practice. Therefore, it is essential that procedures state clearly what actions are to be taken, by whom, where and when (noting pertinent regulatory deadlines as appropriate). The evolving nature of AML/CTF laws and general guidelines and changes to regulated institutions business require that procedures be updated on a regular basis to ensure their continued effectiveness. The procedures shall include the following:

a. Identify the operations (i.e., products, services, customers, delivery channels, and geographic locations) that are more vulnerable to abuse by money launderers and criminals;

b. Provide for periodic updates to the regulated institution's risk profile; and provide for an AML/CFT compliance program tailored to manage risks;

c. Inform the board, or board sub-committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies and STRs filed;

d. Identify reportable transactions and accurately file all required reports including STRs and CTRs;

e. Provide sufficient controls and systems for filing; and Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious transaction;

f. Provide for adequate supervision of staff that handle large currency transactions; complete reports, grant exemptions and monitor for suspicious transactions;

g. Incorporate AML/CFT laws and related regulations compliance into the job descriptions and performance evaluations of regulated institution staff, as appropriate. The above listed policies and procedures are not designed to be all-inclusive and should be tailored to reflect the regulated institution's AML/CFT risk profile.

CHAP 5: CUSTOMER IDENTIFICATION PROGRAM (CIP) AND CDD

5.1. Customer Identification Programme (CIP)

All regulated institutions must have a written CIP. The CIP rule implements the provisions of the article 11 of AML/CTF Law, which orders reporting persons to check the identification of the customer and beneficial owner. The CIP must be incorporated into the regulated institutions' AML/ CTF compliance program, which is subject to approval by the board.

The CIP is intended to enable the regulated institutions to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each type of customer, i.e., natural or legal person/arrangements. regulated institutions shall conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

a. The types of accounts offered by the financial institutions.

b. The financial institutions methods of opening accounts (i.e., face-to-face or non-face to face).

c. The types of identifying information available.

The CIP must contain account-opening procedures detailing information that must be obtained from each customer as provided for in article 11 of the AML/ CTF Law

5.2. Basic Customer Due Diligence (BCDD)

Regulated Institutions shall apply basic CDD measures before a business relationship is entered into. The basic CDD measures entail:

a. identifying the customer and verifying the customer's identity using reliable, independent source documents, data, or information;

b. identifying the ultimate beneficial owner (UBO) and taking reasonable measures to verify the identity of the UBO such that the reporting entity is satisfied that it knows who the UBOs are;

c. identifying any third parties on whose behalf the customer is acting;

d. determining the purpose and intended nature of the business relationship;

e. Keeping the CDD information up-to-date and monitoring the business

relationship and transactions undertaken throughout the course of the relationship to assure that they are consistent with the institution's knowledge of the customer and the UBO.

Regulated Institutions shall refuse to open an account, establish a business relationship or conduct the transaction, and consider making a STR when they are unable to comply with the CDD requirements.

5.3. Enhanced Customer Due Diligence (ECDD)

Regulated institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, regulated institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

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 additional information on the intended nature of the business relationship.

c. Obtaining information on the source of funds or source of wealth of the customer.

d. Obtaining information on the reasons for intended or performed transactions.
e. Obtaining the approval of senior management to commence or continue the business relationship.

f. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

g. Requiring the first payment to be carried out through an account in the customer's name with a financial institution subject to similar CDD standards.

5.4. Simplified Customer Due Diligence (SCDD)

Where the risks of money laundering or terrorist financing are lower, regulated institutions may to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g., the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

a. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g., if account transactions rise above a defined monetary threshold);

b. Reducing the frequency of customer identification updates;

c. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold;

d. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

5.5. Requirement to Existing Customer

Regulated Institutions are required to apply CDD requirements to existing customer on the basis of materiality and risk.

Regulated Institutions are required to conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. In assessing materiality and risk on the existing customer, regulated institution shall consider the following circumstances:

a. the nature and circumstances surrounding the transaction including the significance of the transaction;

b. any material change in the way the account, transaction or business relationship is operated; or insufficient information held on the customer or change in customer's information; Financial Institutions shall terminate the business relationship with existing customer when they have doubts about the veracity or adequacy of previously obtained customer identification data and when existing customers hold anonymous or accounts in fictitious names.

5.6. Reliance on identification and verification already performed

The CDD measures do not imply that regulated institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information.

Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

5.7. Timing of verification

Examples of the types of circumstances where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

a. Non-face-to-face business.

b. Where may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

Regulated institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilize the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or value of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

CHAP 6: TRANSACTION MONITORING AND RECORD KEEPING AND RETENTION

6.1. Transaction Monitoring

In addition to what AML/CTF law is providing, regulated institutions are required to particularly observe the following:

a. to pay special attention to all complex, unusual patterns of transactions or exceptionally large transactions, which have no apparent economic or visible lawful purpose. They must examine the background and purpose of such transactions, establish the findings in writing and transmit the report to the Centre;

b. to pay special attention to business relationships and transactions between persons in Rwanda with persons residing in countries which do not apply anti-money laundering and terrorism financing regulations, or which apply insufficiently regulations equivalent to those provided for in this Law.

Regulated institutions must determine the extent of monitoring depending on its ML/TF risk profile that appropriately covers products, services, customers, delivery channels and geographic locations. Regulated institution's policies, procedures, and processes must:

a. Ensure timely generation of, review of, and response to reports.

b. Require appropriate research when monitoring reports identifying unusual transactions.

c. Refer unusual transactions from all business lines to the responsible function (the Compliance Officer) for evaluation.

A transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographical location or those that are inconsistent with customer profiles based on the RI's knowledge of the customer) and includes a review of various reports generated by the regulated institutions' MIS or vendor systems. Examples of MIS reports include:

a. Teller transaction reports;

b. Daily transaction reports;

c. Dormant account reactivation report;

d. Funds transfer reports;

e. Structured transaction reports;

f. Large currency transaction reports; and

g. Significant balance change reports.

h. Manual Transaction Monitoring.

Many MIS or vendor systems include filtering models for the identification of potentially unusual transactions. The process may involve the review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used shall be commensurate with the regulated institution' ML risk profile and appropriately cover higher-risk products, services, customers, delivery channels, and geographical locations.
MIS or system-generated reports typically use a discretionary Francs threshold. Thresholds selected by management for the production of transaction reports shall enable management to detect unusual transactions.

Management shall periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. The regulated institution shall evaluate and identify filtering criteria most appropriate for it . The programming of the regulated institutions monitoring systems shall be independently reviewed for reasonable filtering criteria.

6.2. Automated Transaction Monitoring

Automated transaction monitoring systems cover multiple types of transactions and uses various rules to identify potentially suspicious transactions based on rules related, for example, to different types of customer or transactions or origination/destination. In addition, many can adapt over time based on historical transaction, trends, or internal peer comparison.

These systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual Transactions, or deviations from expected transactions. The system can capture a wide range of account transactions,

such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from financial institution's core data processing system. Where a financial institution that is large, operating in many locations, or has a large volume of higher-risk customers, the NBR expects that it will use automated monitoring systems.

Relative to automated monitoring, system capabilities and thresholds refer to the parameters or filters used by financial institutions in their monitoring processes. Parameters and filters shall be reasonable and tailored to the transaction that the financial institution is trying to identify or control. After parameters and filters have been developed, they shall be reviewed by management before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed. For example, a financial institution may discover that its filter for cash structuring is triggered only by a daily cash transaction in excess of 1, 000,000 RWF.

The financial institution may need to refine this filter in order to avoid missing potentially suspicious transactions because common cash structuring techniques often involve transactions that are slightly under the CTR threshold. Once established, the financial institution shall review and test system capabilities and thresholds on a periodic basis.

This review shall focus on specific parameters or filters in order to ensure that intended information is accurately captured and that the parameter or filter is appropriate for the financial institution's particular risk profile. The financial institution's system shall be able to do the following:

a. Aggregate structured transactions and;

b. Flag out/identify unusual transactions.

System filtering criteria shall be developed through a review of specific higher-risk products and services, customers and delivery channels and geographies as well as typologies dealing with ML/TF in Rwanda as identified by the FIC (and in the NRA). System filtering criteria, including specific profiles and rules, shall be based on what is reasonable and expected for each type of account.

Monitoring accounts purely based on historical transactions can be misleading if the transaction is not actually consistent with similar types of accounts. For example, an account may have a historical transaction activity that is substantially different from what would normally be expected from that type of account. The authority to establish or change expected transaction profiles shall be clearly defined and generally require the approval of the Compliance Officer or Senior Management. Controls shall ensure limited access to the monitoring system. The following shall be documented:

a. Filtering criteria;

b. Thresholds used; and how both are appropriate for the financial institutions risk profile;

c. Management shall also periodically review the filtering criteria and thresholds established to ensure that they are still effective. Additionally, the monitoring

system's programming methodology and effectiveness shall be independently validated to detect potentially suspicious transaction.

6.3. Monitoring of Foreign Branches, Subsidiaries and Offices

Reporting entities are required to closely monitor the reporting entities' foreign branches, subsidiaries and offices operating in jurisdiction with inadequate AML/CFT laws and regulations as highlighted by the FATF.

Reporting entities are required to ensure that their foreign branches, subsidiaries and offices apply AML/CFT measures consistent with the home country requirements. Where the minimum AML/CFT requirements of the host country are less stringent than those of the home country, the reporting entities must apply the home country requirements, to the extent that host country laws and regulations permit.

If the host country does not permit the proper implementation of AML/CFT measures consistent with the FIU requirement the reporting entities are required to apply appropriate additional measures to manage the ML/TF risks, and report to FIU and their supervisor on the AML/CFT gaps and additional measures implemented to manage the ML/TF risks arising from the identified gaps.

6.4. Indicators of Suspicious Transactions

Indicators of suspicious transactions provided in the Appendixes (A, B, C & D) of these general guidelines shall serve as guidance in identifying suspicious transactions. Nonetheless, FIC may identify indicators that assist in recognizing suspicious financial transactions as provided in the law establishing the Financial Intelligence Centre. In case indicators provided for in these guidelines are in conflict with those of the FIC, the latter shall prevail.

6.5. Suspicious Transactions (STR) & Cash Transactions Reports (CTR)

Regulated Institutions are required to submit to the FIC the suspicious transactions reports (STRs) and Cash Transaction Reports in the format prescribed by FIC. Both (STR & CTR) shall be submitted to FIC in the manner determined by the latter.

6.6. Record Keeping and Retention

Regulated institutions shall maintain all their records in accordance with the required level of confidentiality. All customer identification, verification, transaction, investment and advisory services records are to be retained by the regulated institution.

The minimum retention period is 10 years from the time of transaction or from when a business relationship is terminated as per Article 20 of the AML/CFT Law. The retention period of any document (word document or soft copy or hard copy or original) relating to a financial transaction shall be in line with the AML/CFT obligations.

Records are to be retained at the regulated institutions to provide and support an audit trail for all reportable transactions or activities, together with any supporting documentation for such periods as prescribed by legislation.

In this regard, the following will be adhered to:

a. All documents (ID records, account files, correspondences and results of analysis undertaken of transactions) completed and obtained during the account opening procedure relating to customer identification and verification will be retained and stored either electronically or any other format in the Customer Identification Files (CIF);

b. All records relating to every transaction that will enable regulated institutions to fulfil its obligations with regard to transaction reporting (SAR and CTR) will be retained;

c. The above-mentioned records are to be kept in a safe place and appropriate disaster recovery procedures will be implemented to ensure that such records are not vulnerable to fire, storm, theft etc.;

d. Shall regulated institutions decide to use third parties for document/ transaction retention, then financial institutions will still be accountable for the safekeeping of these documents.

Regulated institutions shall at all stages of a transaction be able to retrieve without delay any relevant information when requested by competent authorities and where the regulated institution is required by any provision of the law to release any document before the retention period has lapsed, it shall retain a copy of the document and shall maintain a register of the released documents.

Customer Identification Files (CIF) will be maintained for each customer. Such files will be maintained at the branch where the customer holds his/her account, unless alternative arrangements have been made. Such files will be strictly controlled and access to such files limited.

CHAP 7: FINANCIAL SANCTIONS OF TERRORISTS AND TERRORISM FINANCIERS

7.1. Data Base of Terrorists and Terrorism Financier

It is particularly vital that regulated Institutions shall be able to identify terrorist suspects and possible designated parties and detect prohibited transactions.

7.2. National List

Regulated institutions are required to maintain a database of names and particulars of terrorists and terrorism financiers published by the Minister in charge of Justice (National List) as provided for in the law on counter terrorism.

7.3. UNSRC Consolidated List

Regulated institutions are required to keep updated with the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011) and 1989 (2011) which require

sanctions against individuals and entities belonging or related to the Taliban and the Al-Qaida organization.

Regulated institutions are required to maintain a list of individuals and entities (the Consolidated List) for this purpose. The updated UN List can be obtained at: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

Regulated institutions are required to maintain a database of names and particulars of listed persons in the UN Consolidated List and such orders as may be issued by competent authorities. Regulated institutions shall ensure that the information contained in the database is updated and relevant and made easily accessible to its employees at the head office, branch or subsidiary.

7.4. Screening and Enhanced Checking

Regulated institutions are required to conduct checks on the names of new customers, as well as regular checks on the names of existing customers, and potential customers, against the names in the database. If there is any name match, regulated institutions are required to take reasonable and appropriate measures to verify and confirm the identity of its customer; once confirmation has been obtained, regulated institutions must immediately:

a. Freeze the customer'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.

Regulated institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the Consolidated List or orders made by the competent authorities as well as the National List.

Regulated institutions are required to ascertain potential matches with the Consolidated List and the National List to confirm whether they are true matches to eliminate "false positives". The regulated institutions are required to make further inquiries from the customer or counterparty (where relevant) to assist in determining whether the match is a true match. Regulated Institutions may also consolidate their database with the other recognized lists of designated persons or entities issued by other jurisdictions.

CHAP 8: FINAL PROVISIONS

8.1. Compliance with these Guidelines

The Central Bank shall monitor if Regulated institutions are complying with the AML/CFT Law, AML/CFT regulations as well as FIC requirements using these guidelines.

The non-compliance may lead to the applications of administrative sanctions provided in regulation determining administrative sanctions applicable to regulated institutions for non-compliance with the prevention of money laundering, financing terrorism and financing of proliferation of weapons of mass destruction requirements.

8.2. Repealing Clause

General Guidelines No 3160/2021-00026[616] to financial institutions on anti-money Laundering, terrorist financing of proliferation of weapons of mass destruction requirements and all previous provisions contrary to these general guidelines are hereby repealed.

8.3. Effective Dates

This guidance shall take effect from the date of its signature.

Done at Kigali, on 16th October 2023

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor

APPENDIX A

GENERAL INDICATORS AND EXAMPLES OF SUSPICIOUS TRANSACTIONS FOR ALL REGULATED INSTITUTIONS

The following acts are the examples of indictors to identify Suspicious Transaction more of the aforementioned elements; the relevant regulated institutions can use the indicators of Suspicious Transactions indicators, which include, among other things:

1. Transactions

1.1. Cash

i. Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.

ii. Transactions conducted in a relatively small amount but with high frequency (structuring).

iii. Transactions conducted by using several different individual names for the interest of a particular person (smurfing).

iv. The foreign currency exchange or purchase in a relatively large amount.

v. The purchase of travelers checks in cash in a relatively large amount.

vi. The purchase of several insurance products in cash in a short period time or at the same time with premium payment entirely in a large amount and followed by policy disbursement prior to due date.

vii. The purchase of securities by cash, transfer, or checks under another person's name.

1.2. Economically Irrational Transactions

i. Transactions having no conformity with the initial purpose of account opening.

ii. Transactions having no relationship with the business of the relevant customer.

iii. Transaction amount and frequency are different from that of normally conducted by the customer.

1.3. Fund Transfers

i. Fund transfers to and from high-risk countries or offshore financial centres without any clear business purposes.

ii. ii. Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.

iii. Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period.

iv. Fund payments for export import activities without complete documents.

v. Fund transfers from or to other high-risk countries.

vi. Fund transfers from or to other high-risk parties.

vii. Receipts/ & payments of funds made by using more than one (1) account, either in the same name or a different one.

viii. Fund transfers using the account of a reporting entity employee in an unusual amount.

2. Behaviors of the Customer

i. Unreasonable behavior of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).

ii. Customer/prospective customer gives false information with respect to his/ & her identity, sources of income or businesses.

iii. Customer/ prospective customer uses identification document that is unreliable or alleged as fake such as different signature or photo.

iv. Customer/prospective customer is unwilling or refusing to provide information/ & documents requested by the officials of the relevant reporting entity without any clear reasons.

v. Customer or his/ her legal representative tries to persuade the officials of the relevant reporting entity in one way or another not to report his/ & her transaction as a Suspicious Transaction.

vi. Customer is unwilling to provide right information or immediately terminating business relationship or closing his/ & her account at the time the officials of the relevant reporting entity request information with respect to his/ her transaction.

3. Additional Indicators to Financial Institutions

The following indicators are for your consideration if you are an institution that opens accounts and holds deposits on behalf of individuals or entities.

3.1. Personal Transactions

Customer appears to have accounts with several financial institutions in one geographical area;

i. Customer has no employment history but makes frequent large transactions or maintains a large account balance;

ii. The flow of income through the account does not match what was expected based on stated occupation of the account holder or intended use of the account;

iii. Customer makes one or more cash deposits to general account of foreign correspondent bank (i.e., pass-through account);

iv. Customer makes frequent or large payments to online payment services;

v. Customer runs large positive credit card balances;

vi. Customer uses cash advances from a credit card account to purchase money orders or to wire/ & electronically transfer funds to foreign destinations;

vii. Customer takes cash advance to deposit into savings or cheque account;

viii. Large cash payments for outstanding credit card balances;

ix. Customer makes credit card overpayment and then requests a cash advance;

x. Customer visits the safety deposit box area immediately before making cash deposits;

xi. Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her address;

xii. Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount;

xiii. Customer deposits large, endorsed cheques in the name of a third-party.

3.2. Corporate and Business Transactions

On opening accounts with the various businesses, a financial institution would likely be aware of those that are mainly cash based. Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity. Below are some of the examples:

i. Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of salaries, invoices, etc.

ii. accounts have a large volume of deposits in bank drafts, cashier's cheques;

iii. money orders or electronic funds transfers, which is inconsistent with the customer 's business;

iv. accounts have deposits in combinations of monetary instruments that are atypical of legitimate business activity (for example, deposits that include a mix of business, payroll, and social security cheques);

v. accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity;

vi. business does not want to provide complete information regarding its activities;

vii. Financial statements of the business differ noticeably from those of similar businesses;

viii. representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them;

ix. deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations;

x. customer maintains a number of trustee or customer accounts that are not consistent with that type of business or not in keeping with normal industry practices;

xi. customer operates a retail business providing cheque-cashing services but does not make large withdrawals of cash against cheques deposited;

xii. customer pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments;

xiii. customer purchases cashier's cheques and money orders with large amounts of cash;

xiv. customer deposits large amounts of currency wrapped in currency straps;

xv. customer makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same Financial institution or elsewhere;

xvi. Customer makes a large volume of cash deposits from a business that is not normally cash intensive.

APPENDIX B

SPECIFIC INDICATORS AND EXAMPLES OF SUSPICIOUS TRANSACTIONS INVOLVING INSURANCE AND INTERMEDIARIES

The following examples may be indicators of a suspicious transaction and give rise to a suspicious transaction report:

1. application for a policy from a potential client in a distant place where a comparable policy could be provided "closer to home";

2. application for business outside the policyholder's normal pattern of business;

3. introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organised criminal activities (e.g., drug trafficking or terrorist activity) or corruption are prevalent;

4. any want of information or delay in the provision of information to enable verification to be completed;

5. an atypical incidence of pre-payment of insurance premiums;

6. the client accepts very unfavourable conditions unrelated to his or her health or age;

7. the transaction involves use and payment of a performance bond resulting in a cross-border payment (wire transfers) = the first (or single) premium is paid from a financial institution account outside the country;

8. large fund flows through non-resident accounts with brokerage firms;

9. insurance policies with premiums that exceed the client's apparent means;

10. the client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment;

11. insurance policies with values that appear to be inconsistent with the client's insurance needs;

12. the client conducts a transaction that results in a conspicuous increase of investment contributions;

13. any transaction involving an undisclosed party;

14. early termination of a product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party;

15. a transfer of the benefit of a product to an apparently unrelated third party;

16. 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);

17. substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder;

18. requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payments;

19. attempts to use a third party cheque to make a proposed purchase of a policy;

20. the applicant for insurance business shows no concern for the performance of the policy but much interest in the early cancellation of the contract;

21. the applicant for insurance business 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;

22. the applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency;

23. the applicant for insurance business is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify;

24. the applicant for insurance business appears to have policies with several institutions;

25. the applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means;

26. the applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party;

27. the applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy;

28. the applicant for insurance business uses a mailing address outside the insurance supervisor's jurisdiction and where during the verification process it is discovered that the home telephone has been disconnected.

APPENDIX C

SPECIFIC INDICATORS AND EXAMPLES OF SUSPICIOUS TRANSACTIONS INVOLVING FOREX BUREAUS

The following examples may be indicators of a suspicious transaction and give rise to a suspicious transaction report:

1. Exchange of large quantities of low denomination notes for higher denominations;

2. Exchange of large amounts or frequent exchanges that are not related to the customer's business;

3. Structuring of large amounts;

4. Repeated requests from an exchange office for foreign exchange purchasing-selling transactions in the amounts slightly less than the transaction limit for identification in a short period of time;

5. The customer requests currency in large denomination notes;

6. The customer buys currency that does not fit with what is known about the customer's destination;

7. The customer buys currency from an unusual location in comparison to his/her own location;

8. The customer apparently does not know the exact amount being exchanged;

9. The customer looks around all the time and does not watch the counting of money;

10. The customer is happy with a poor rate;

11. Currency purchases with large cash amounts;

12. Large exchanges between foreign currencies;

13. Frequent exchange of cash into other currencies;

14. Exchange of primarily one type of currency;

15. The amounts exchanged are significantly higher than usual;

16. There is no link between the amount of money exchanged and holiday periods;

17. High frequency of currency exchange transactions over a period of time;

18. Many currency exchange offices used by the same person;
19. Requests to exchange large amounts of foreign currency, which is not convertible (or not frequently used), another kind of foreign currency.

APPENDIX D

SPECIFIC INDICATORS AND EXAMPLES OF SUSPICIOUS TRANSACTIONS INVOLVING MONEY REMITTANCES AND OTHER PAYMENT SERVICES PROVIDERS

The following examples may be indicators of a suspicious transaction and give rise to a suspicious transaction report:

1. Transferring funds without any apparent economic reason;

2. Unusual large cash payments in circumstances where payment would normally be made by cheque, banker's draft, etc.

3. Transfers of funds without underlying transactions;

4. Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings;

5. Transfers paid by large cash amounts in different sums in a short period of time;

6. Personal remittances sent to jurisdictions that do not have an apparent family or business link;

7. Remittance made outside migrant remittance corridors;

8. Personal funds sent at a time not associated with salary payments;

9. The customer seems only after the counting to know which amount is being transferred;

10. The customer shows no interest in the transfer costs;

11. The customer has no relation to the country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there;

12. The customer has a note with information about payee but is hesitating if asked whether to mention the purpose of payment;

13. Large or repeated transfers between the account of a legal person and a private account, especially if the legal person is not a resident;

14. Large amounts are transferred to companies abroad with a service provider address;

15. Large or frequent transfers of money;

16. Frequent transfer of value that is not related to the customer's business;

17. Use of groups of people to send money;

18. Use of different money remittance businesses;

19. Amounts sent are higher than usual;

20. There is no relationship between the sender and the beneficial owner;

21. The operations are irregular;

22. Receiving money from different parts of the world (developed countries) from different people;

23. Money is received during short periods of time;

24. Money is received from different money remittance companies;

25. Money is withdrawn in cash;

26. Multiple senders toward a single individual.

Done at Kigali, on 16th October 2023

Digitally signed by BNR(GOVERNOR)

RWANGOMBWA John
Governor