ANTI-MONEY LAUNDERING AND COMBATING TERRORISM FINANCING GUIDELINES FOR FINANCIAL INSTITUTIONS IN THE GAMBIA

2015

TABLE OF CONTENTS

I: LIST OF ACRONYMS

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CTF	Counter Terrorist Financing
CTR	Cash Transaction Report
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIs	Financial Institutions
FIU	Financial Intelligence Unit
GIABA	Inter-governmental Action Group Against Money Laundering in West Africa
KYC	Know Your Customer
ML	Money Laundering
MVTS	Money or Value Transfer Services
NPO	Non-Profit Organisations
PEP	Politically Exposed Persons
RBA	Risk-Based Approach
RE	Reporting Entities
STR	Suspicious Transaction Report
TF	Terrorist Financing
UN	United Nations
UNSCRs	United Nation Security Council Resolutions
WTR	Wire Transfer Report

II: LIST OF PREDICATE OFFENCES

1. Participation in an organized criminal group and racketeering;
2. Terrorism, including terrorist financing;
3. Trafficking in human beings and migrant smuggling;
4. Sexual exploitation, including sexual exploitation of children;
5. Illicit trafficking in narcotic drugs and psychotropic substances;
6. Illicit arms trafficking;
7. Illicit trafficking in stolen and other goods;
8. Corruption and bribery;
9. Fraud;
10. Counterfeiting currency;
11. Counterfeiting and piracy of products;
12. Environmental crime;
13. Murder, grievous bodily injury;
14. Kidnapping, illegal restraint and hostage-taking;
15. Robbery or theft;
16. Smuggling;
17. Extortion;
18. Forgery;
19. Piracy; and
20. Insider trading and market manipulation

1.0: GUIDELINE I- GENERAL INTRODUCTION

1.1 Fight against crimes

1.2 The counter money laundering and terrorism financing laws across the globe and in particular in The Gambia have now extended broad range of obligations on the financial institutions to design, develop and deploy preventive, detection and reporting measures so as to help the law enforcement agencies and competent authorities to fight the menaces of these crimes. And protect the economic and financial systems from abuse. The private sector especially the financial institutions are obliged to combat these crimes by designing and implementing adequate policies and internal operational procedures, to ensure that money launderers, terrorist financiers and other criminals find it difficult to exploit them to perpetrate their criminal activities.

1.3 Towards this end, international response has been to enhance the capacity of the financial institutions in the methods and techniques to use in preventing and deterring money launderers and terrorist financiers in having access to the financial system globally. Given that the aforementioned activities go beyond borders, The Gambia has joined many other countries in the world in recognizing the importance of strengthening capacity to discourage illicit activities in the world and indeed in The Gambia.

1.4 Being mindful of international standards and best practices, the Financial Intelligence Unit in collaboration with the Central Bank of The Gambia is issuing these guidelines to serve as a guide to all financial institutions licensed by the Central Bank of The Gambia. The guidelines are aimed at providing financial institutions with requisite knowledge, deeper interpretation and understanding of the requirements and financial institutions' obligations under the Anti-Money Laundering and Combating Terrorism Financing (AML/CTF) Act, 2012 and its attendant legislations. The guidelines would enhance the AML/CFT regime of The Gambia in implementing the Financial Action Task Force (FATF) 40 Recommendations. The guidelines will also serve as a standard reference document to financial institutions in building robust AML/CFT measures in the combat of money laundering and terrorist financing.

1.5 SCOPE

1.6 The Guidelines lay down the minimum standards expected of all Financial

Institutions (FIs) in The Gambia in combating money laundering, terrorist financing and other criminal conducts in The Gambia in accordance with the requirements of the AML/CTF Act 2012. Furthermore, the guidelines incorporate requirements of the revised Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and Terrorist Financing and best practice papers issued by the FATF and other international organizations including the World Bank and the International Monetary Fund (IMF), the Basel Committee on Banking Supervision and other international best practices.

1.7 APPLICATION

1.8 All banks and financial institutions licensed under the Central Bank of The Gambia are obligated to comply with the guidelines, which contains both advisory and obligatory requirements. It should be noted that within these guidelines advisory matters are expressed using the term "may" while mandatory requirements are referred to using the term "should". Banks, Microfinance Institutions, Foreign Exchange Bureaus (including money transfer operators), and Insurance Companies should allocate adequate resources to mitigate money laundering, terrorism financing and other related financial crimes risks in their institutions. Financial institutions should also ensure that, at a minimum, the guidelines are implemented in their branches and subsidiaries abroad, where applicable. When implementation is outside the jurisdiction of The Gambia, they should abide by the standards of the countries they operate in if the standards in those countries are higher than the ones in The Gambia. Furthermore, they should inform FIU of The Gambia and the Central Bank of The Gambia if the local laws in the country of operation prohibit the implementation of these guidelines as a whole or any part of.

1.9 Money Laundering Definition

1.10 The Anti-Money Laundering and Combating of Terrorism Financing (AML/CTF) Act, 2012 defines money laundering as;

i. the conversion or transfer of property knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the proceeds or helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her actions;
ii. the concealment or disguise of the true nature, source, location, disposition, movement or ownership of rights in respect of property knowing that such property is the proceeds of crime;

iii. the acquisition, possession or use of property knowing at the time of receipt that such property is the proceed of crime or
iv. participation in, association with or conspiracy to commit, aiding and abetting, facilitating or counseling the commission of any of the above offences.

1.11 Offence of money laundering

1.12 A person who is involved in money laundering commits an offence and is liable in the case of-

i. an individual, including a director, employee or agent of a reporting entity, to imprisonment for a term of not less than ten years; or
ii. a body corporate a fine of not less than Ten Million Dalasi or an order for the revocation of the license of the corporate body or both.

1.13 Stages of Money Laundering

1.14 Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through series of transactions; in this way the funds are "cleaned", so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

Placement: The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement agents. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. It may also include, dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g. money orders) that are then collected and deposited into accounts at another location or financial institution.

Layering: The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in simple or complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or

transferring funds to and through numerous accounts in one or more financial institutions.

Integration: This is the third stage of laundering process, where the illicit funds are reinvestigated in the legate economy. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples integration scheme include the purchase and resale of real estate, investment securities, or other assets.

1.15 Importance of combating money laundering

1.16 Most criminals engage in criminal activities to earn benefits or profits. There is a direct relationship between the profitability of most types of crime and their prevalence. Thus, in order to combat crimes that generate money and other illegal activities, there is a need to make the crimes uninteresting, by taking the profits out the crimes. Apart of engaging in illegal activities, criminals use money laundering techniques to protect their illegally obtained wealth.

1.17 In The Gambia, though the quantum of laundered funds are not precisely known, it is believed huge amounts of illegal funds are laundered annually. If money laundering is allowed to be perpetrated by criminals; the proceeds of crime will provide financial support to drug dealers/traffickers, terrorists and terrorist organizations, human traffickers, corrupt officials, arms dealers and other criminals to operate and expand their criminal activities. This will undermine the rule of law and destroy the very fabric of a civilize society.

1.18 Money laundering activities can distort economic fundamentals, causing improper economic planning with dire consequences on the economic and financial system of the country. To this end, The Gambia is serious on rooting out all forms of crimes in society, as demonstrated in the domestication and implementation of international and regional requirements on the combat of money laundering and other related financial crimes.

1.19 International efforts to combat money laundering

1.20 Money laundering can occur within a single jurisdiction, however, most of the funds laundered involved multiple jurisdictions. This therefore, requires global

response to combat the crime. Thus, the international community have taken giant steps to help countries to fight against money laundering. One of the most important institution in the fight against money laundering is Financial Action Task Force (FATF), which was established by G-7 countries in 1989. FATF is an intergovernmental body, established to develop and promote policies to combat money laundering and terrorist financing.

1.21 Initially, FATF developed 40 Recommendations on the combat against money laundering, and later developed 9 Special Recommendations in combating terrorism financing. However, in February 2012, FATF issued 40 Recommendations on money laundering, terrorism financing, replacing the 40 + 9 Recommendations. These Recommendations are widely recognized as the minimum standards which countries should adopt and implement to fight money laundering, terrorism financing and other criminal conducts.

1.22 The Egmont Group of Financial Intelligence Units, established in 1995, is an association of Financial Intelligence Units globally. It was established as result of meeting held at the Arenberg Palace in Brussels, calling on the establishment of a networks of FIUs to foster exchange of information among FIUs.

1.23 International and regional bodies across the world have taken positive steps to curb the menace of money laundering and terrorism financing. Such efforts include the coming into force; the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime; establishment of regional groups such as Asia Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force on Money Laundering (CFATF), Inter-governmental Action Group Against Money Laundering in West Africa (GIABA), Middle East and Northern Africa Financial Action Task Force (MENAFATF), East and Southern Africa Money Laundering Group (ESAMLG). Series of UN Conventions have come to force including the United Nations Single Convention on Narcotic Drugs, United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, United Nations Convention Against Transnational Organized Crime, United Nation Convention for the Suppression of International Financing of Terrorism and United Nations Convention against Corruption.

1.24 Offence of Terrorism Financing

1.25 The Anti-Money Laundering and Combating of Terrorism Financing (AML/CTF) Act 2012 provides that a person who directly or indirectly;

i. provides, whether by giving, lending or otherwise making available, or collects funds or property with the intention that they should be used, or having reasonable grounds to believe that they are to be used, in full or in part, in order to carry out a terrorist act;
ii. organises or directs others to commit, attempts to commit or conspires to commit an offence under this section, commits the offence of financing of terrorism and is liable in the case of-
iii. an individual, including a director, employee or agent of a reporting entity, to imprisonment for a term of not less than ten years; or
iv. a body corporate to a fine of not less than Ten Million Dalasi.

1.26 Terrorism Financing

1.27 Terrorist financing is the provision of funds to facilitate terrorist activity. Terrorists finance their activities through both lawful and unlawful sources. Unlawful activities, such as extortion, kidnapping, narcotics trafficking, arms trafficking, etc. have been found to be a major sources of funding. Other sources of terrorist funding include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable donations. Fund raising activities from donations have been found to be an effective means of collection for terrorist financing. In this case, donors may have no knowledge that their donations have been diverted to support terrorist causes. Some legitimate sources of terrorist funds include foreign government sponsors and private businesses. These legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations.

1.28 Terrorism financing process is not any different from the money laundering process except for its intentions. While the intent of money launderers is to profit in terms of enjoying the proceeds of the criminal act, the terrorist financier is the emotional satisfaction they drive from getting their acts noticed and obtaining what they want, being political, ideological, religious grounds and many more.

1.29 The terrorist activities are meant to intimidate a population or compel a government or international organization to do something. The terrorist intentionally kill, seriously harm or endanger individuals or groups or cause substantial damage to property. Terrorism can be perpetrated by seriously interfering with or disrupting essential services, facilities or systems.

1.30 Financial support

1.31 Initially, some states and government used to provide funds and other forms of support to terrorists and terrorist groups.

1.32 Revenue generating activities

1.33 The revenue generating activities of terrorist groups may include criminal acts, and therefore may appear similar to other criminal organizations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds.

1.34 Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues and subscriptions, sale of publications, speaking tours, cultural and social events, as well as solicitation and appeals within the community. This fundraising might be in the name of organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate good cause. The non-profit organisations can be used to finance terrorist activities. Terrorist use the charities to receive donations of varying forms.

1.35 Laundering of terrorist-related funds

1.36 The methods used by terrorist groups to generate funds from illegal sources are often very similar to those used by "traditional" criminal organizations. Like criminal organizations, they have to find ways to launder these illicit funds to be able to use them without drawing the attention of the authorities. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering.

1.37 Stages of terrorism financing

1.38 The stages of terrorist of financing include;

i. Raising funds through donations, self-funding or criminal activity.
ii. Transferring funds to individual terrorist, terrorist network, organization or cell.
iii. Using funds to purchase weapons or bomb-making equipment, payment to insurgents, or covering living expenses for terrorist cell.

1.39 Importance of combating terrorist financing

1.40 The heinous attacks perpetrated by terrorists on civilian population across the

world is a serious threat against peace and security. The Gambia is committed to rooting out the vices of terrorism. Though no terrorist attacks took place in The Gambia and no terrorist activity has been perpetrated in the country, there is a need for vigilance at all times.

1.41 The increased terrorist activities in West Africa and the trade links of the region with countries where terrorist activities may be perpetrated, posed a threat which the authorities are not oblivious of. Certainly, fighting terrorism will protect the financial system from abuse, increase soundness of the financial sector, in terms of maintaining and improving on the reputational and operational capacities of the financial institutions, promoting vibrant financial institutions free from being used as conduits to commit crimes.

1.42 Implementing robust AML/CFT Regime

1.43 The Gambia has enacted series of laws to strengthen its Anti-Money Laundering and Counter Money Laundering regime. This is aimed at bringing the country in line with international and regional standards in the fight against the menace of money laundering and terrorism financing.

1.44 The legal framework consists of laws and regulations which seek to protect the economic and financial systems of the country from abuse by money launderers, terrorism financiers and other criminals. It also aims to take profits out of crimes by allowing national authorities to trace, identify and recover proceeds of crimes so as to deter the criminals from enjoying their ill-gotten proceeds of crimes.

1.45 The national legislations have series of provisions which;

i. Criminalise money laundering and terrorism financing
ii. Criminalise all categories of predicate offences
iii. Strengthen law enforcement authorities, regulators and supervisors and other competent authorities to comprehensively deal with crimes
iv. Impose proportionate and dissuasive sanctions against money laundering and terrorism financing
v. Establish asset freezing, seizure and confiscation mechanisms
vi. Establish regulations to implement the requirements of the UN Security Council Resolutions
vii. Establish functional Financial Intelligence Unit
viii. Set up appropriate national coordination and international cooperation framework

ix. Impose requirements on reporting entities when deal with their customers/clients and other persons

i. 1.46 The legal regime is intended to meet the following;
ii. Deter money laundering, terrorism financing and other economic and financial crimes
iii. Detect illicit proceeds of crimes and freeze, seize and confiscate such proceeds
iv. Impose obligations on third parties whose services may be used by launderers and terrorists financiers and other criminals
v. Protect the integrity of the financial and economic systems against abuse by criminals.

1.47 Relevant domestic laws to combat of money laundering and terrorism financing

i. Constitution of The Gambia 1997
ii. Anti-Money Laundering and the Combating of the Financing of Terrorism Act 2012;
iii. Anti-Terrorism Act, 2002
iv. Drug Control Act, 2003 as amended 2014
v. Criminal Code CAP 10, Laws of the Republic of the Gambia
vi. Economic Crimes (Other Specified Offences) Act 1994
vii. Criminal Procedure Code
viii. National Regulations on Terrorist Financing, 2014
ix. Banking Act, 2009
x. Insurance Act, 2003
xi. Insurance Regulations, 2005
xii. Companies Act, 2013
xiii. Central Bank Act, 2005
xiv. Non-Bank Financial Institutions Act 2016

1.48 Financial Intelligence Unit of The Gambia

1.49 The Financial Intelligence Unit (FIU) is a body established under Section 3 of the Anti-Money Laundering and Combating of Terrorism Financing (AML/CTF) Act 2012; task to combat money laundering, terrorism financing and other criminal conducts in The Gambia. The establishment of the FIU is in line with Article 7 (1) (b) of the UN Convention against Transnational Organized Crimes 2000 and Article 14 (1) (b) of the UN Convention against Corruption 2003 and Financial Action Task Force Recommendation 29 of February 2012.

1.50 Objects of the FIU

1.51 The objects of the FIU is divided into three categories are as follows:

i. To assist in the identification of proceeds of criminal conduct and the combat of money laundering and terrorist financing activities;
ii. To make information available to investigating authorities, the intelligence and the revenue agencies to facilitate the administration and enforcement of the laws of this country; and
iii. To exchange information with similar bodies in other countries on issues of money laundering, terrorist financing and other criminal conduct.

1.52 The role of the FIU

i. 1.53 The FIU of The Gambia is a national body on the combat of money laundering, terrorism financing and other criminal conducts. Its functions include, to;
ii. receive reports and information provided to it by reporting entities, an agency of another country, the competent authority, a government institution and any other information voluntarily provided to it about suspicion of a criminal conduct, a money laundering activity or the offence of financing of terrorism;
iii. collect any information that it considers relevant to a criminal conduct, money laundering activity or financing of terrorism that is publicly available, including commercially available data- base or information that is collected or maintained, including information that is stored in databases maintained by the government;
iv. request information from reporting entities, any supervisory agency, self-regulatory organization and any law enforcement agency. analyze and assess all reports and information;
v. carry out examinations of reporting entities;
vi. disseminate information derived from reports or other information it receives to the appropriate law enforcement agency, supervisory authority or self-regulatory organization if on the basis of its analysis and assessment, it has reasonable grounds to suspect that the transaction is suspicious;
vii. instruct any reporting entity to take such steps as may be appropriate in relation to any information or report received by it, to enforce compliance with the AML/CTF Act 2012 Act or to facilitate any investigation anticipated by it;
viii. compile statistics and records and may disseminate information within The Gambia or elsewhere, as well as make recommendations arising out of any

information received;

ix. issue (in consultation with regulatory authorities) guidelines to reporting entities in relation to customer identification, record keeping and, reporting obligations and the identification of suspicious transactions;

x. obtain further information on parties or transactions referred to in a report made to it under the AML/CTF Act 2012;

xi. provide training programs for reporting entities in relation to customer identification, record keeping, reporting obligations and the identification of suspicious transactions;

xii. periodically provide feedback to reporting entities and other relevant agencies regarding outcomes relating to the reports or information given under the AML/CTF Act 2012;

xiii. conduct research into trends and developments in the area of money laundering and financing of terrorism and ways of detecting, preventing and deterring money laundering and the financing of terrorist activities;

xiv. educate the public and create awareness on matters relating to money laundering and financing of terrorism;

xv. disclose any report, information derived from such report or any other information it receives to an institution or agency of a foreign state or of an International Organization with similar powers and duties if on the basis of its analysis and assessment, it has reasonable grounds to suspect that report or information would be relevant to investigating or prosecuting a money laundering offence or a terrorist financing offence; and

xvi. enter into any agreements or arrangements with any Government institution or agency regarding the exchange of information.

1.52 Reporting entities

1.53 Reporting entities are private sector entities which are required by the Anti-Money Laundering and Combating of Terrorism Financing (AML/CTF) Act 2012 to implement measures to curb the menaces of money laundering, terrorism financing and other related financial crimes.

1.54 The reporting entities are provided in Schedule I, PART II of the AntiLaundering and Combating of Terrorism Financing (AML/CTF) Act 2012. They include all categories of financial institutions licensed by the Central Bank of The Gambia and Designated Non-Financial Businesses and Professions (DNFBPs). The DNFBPs include casinos, lawyer, notaries and other independent legal professionals, accountants, real estate agents, dealers in precious metals, dealers in precious stones, trust and service company providers.

2.0 GUIDELINE II: MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT

2.1 Risk assessment

2.2 All financial institutions are required to conduct money laundering and terrorist financing risk assessments and adopt appropriate internal control measures to manage and monitor the risks. The results of the risk assessment should be communicated to the Board of Directors, Senior Management and other staff of the financial institution, the appropriate supervisor and the FIU.

2.3 Money Laundering and Terrorist Financing risks

2.4 Money laundering risk is the probability that the financial institution, its products, services could be exploited by money launderers and terrorist financiers to perpetrate illegal activities. Money Laundering and Terrorist Financing Risk Assessment involves identification of risks, risk analysis, risk mitigation and management. Ideally, a risk assessment, involves making judgments about threats, vulnerabilities and consequences.

2.5 Risk can be defined as a function of threat, vulnerability, consequence and impact. The threat is a person or group of people, object or activity with the potential to cause harm to, for example, an entity, the state, society, the economy, etc. In the ML/TF context, this includes criminals, terrorist groups, their facilitators and their funds. Threat is described above as one of the factors related to risk, and typically, it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment. The concept of vulnerabilities as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, vulnerabilities as distinct from threat means focusing on, for example, the factors that represent weaknesses in a repotting

entity's AML/CFT systems or controls. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes. The consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society in general. The consequences of ML or TF may be short or long term in nature and relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

2.6 FIs are required to conduct a business related risk assessment of its ML/TF risks. To execute this, FIs are required to take appropriate steps to identify and assess the ML/TF risks related to its customers, countries or geographic areas, products, services, transactions and delivery channels. Risk assessment is necessary as it enables a reporting entity to focus its AML/CFT efforts and to adopt appropriate measures to optimally allocate the available resources. The FIs are required to document those assessments in writing and keep them up to date. Each reporting entity, regardless of its size and complexity, is expected to develop an adequate risk management system for money laundering and terrorism financing. This risk management system is to ensure that the ML/TF risks is continuously and comprehensively identified, assessed, monitored, managed and mitigated. An adequate system of ML/TF risk management should include but not limited to the following:

i. A risk assessment of money laundering and terrorism financing risks of the business;
ii. Policies and procedures to control money laundering and terrorism financing risks;
iii. An organisational structure to execute these risk management controls; and
iv. A process to systematically check and assess the adequacy of the control systems.

i. 2.7 In order to establish the entity's exposure to ML/TF and the efficient management of that risk, the entity needs to identify every segment of its business operations where a ML/TF threat may emerge and to assess its vulnerability to that threat. The size and complexity of a business plays an important role in how attractive or susceptible it is for ML/TF. For example, a large organisation is less likely to know a customer personally who thereby can be more anonymous than a customer of a small organisation. Organisations providing provides international services might be more attractive to a money

launderer than a domestic ones. Upon identifying the risks, the entity needs to adequately assess the ML/TF risk exposure, which would enable it to evaluate the likelihood of adverse effects arising from that risk and the potential impact of that risk on the realization of business objectives. The risk identification and analysis needs to be conducted for all existing and new products, activities and processes. An effective process of ML/TF risk identification and analysis serves as a basis for establishing an adequate system of risk management and control, and, consequently, for reaching the ultimate goal, thus minimizing possible adverse effects arising from that risk. The purpose of a risk assessment is to apply control measures proportionate to the identified risk. This allows entities to focus on the customers, countries, products, services, transactions and delivery channels that constitute the greatest potential risk. The process of an ML/TF risk assessment has four stages:

ii. Identifying the areas of the business operations susceptible to ML/TF;
iii. Conducting an analysis in order to assess the likelihood and impact of ML/TF;
iv. Managing the risks; and
v. Monitoring and reviewing the risks.

2.7 Special attention to terrorist financing

1.8 In view of the fact that the nature of terrorism financing differs from that of money laundering, the risk assessment must include also an analysis of the vulnerabilities of terrorism financing. Since the funds used for terrorism financing may stem from legal sources, the nature of sources may vary. When the sources of terrorism financing originate from criminal activities, the risk assessment related to money laundering is also applicable to terrorism financing.

2.9 The first step in assessing ML/TF risks is to identify certain risk categories, i.e., customers, countries or geographical locations, products, services, transactions and delivery channels specific for the entity. Depending on the specificity of operations of an entity, other categories could be considered to identify all segments in which ML/TF risk may emerge. The significance of different risk categories may vary from entity to entity, i.e., an entity may decide that some risk categories are more important to it than others are. For the analysis, the entity should make an estimate of the likelihood that these types or categories of customers will misuse the entity for money laundering or terrorism financing. This likelihood is for instance high if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but not impossible. In assessing the impact, the entity can for instance look at the financial damages from the crime itself or from regulatory sanctions; the reputational damage to

the entity or the sector. The impact can vary from minor if there are only short term or low cost consequences to major when there are very costly and long term consequences that affect the proper functioning of the entity. The tables below show a three-point scale. An entity can also decide on a more detailed scale.

Rating	Likelihood
High	Probably occurs several times in a year
Medium	Probably occurs once in a year
Low	Unlikely to occur but not impossible

Rating	Impact
Major	Long term, high cost consequences affecting functioning
Moderate	Medium term consequences with some costs
Minor	Short term or low cost consequences

2.10 Country or geographical risk may arise because of the location of a customer, the origin of destination of transactions of the customer, but also because of the business activities of the entity itself, its location and the location of its organisational units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to money laundering and terrorism financing. There is no general definition based on which particular countries or geographical areas can be categorised as low or high risk. The factors, which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing, may include different criteria. Factors that may indicate a higher risk are:

i. Countries or geographic areas subject to sanctions, embargoes or comparable restrictive measures issued, for instance, by the United Nations, the European Union or the United States.
ii. Countries or geographic areas identified by credible sources (e.g., the FATF, the IMF or the World Bank) as lacking an appropriate system of preventing money laundering and/or terrorism financing. Reference is made to the 'ICRG process' (International Co-operation Review Group) of the FATF. After each of its meetings (held in February, June and October) the FATF publishes lists of countries which in its opinion lack an adequate system of combating money laundering and terrorism financing.
iii. Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
iv. Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity.

2.11 For the purpose of the ML/TF risk assessment, the entity should define if a type of customer carries an increased ML/TF risk. Based on its own criteria, an entity can then determine whether a customer poses a higher risk. Categories of customers that may indicate a higher risk are:

i. Customers who conduct their business relationships or transactions (or who have these conducted) under unusual circumstances, such as an unexplained geographic distance between the entity and the location of the customer;
ii. Customers where the structure or characteristics of the entity or relationship make it difficult to identify the true owner or controlling interests, or customer that use nominees, trusts, family members or third parties, etc;
iii. Cash intensive businesses including (informal) money transfer agencies, foreign exchange bureaus, etc;
iv. Charities and other 'not-for-profit' organizations (especially those operating on a 'cross border' basis) which are not subject to any form of monitoring or supervision;
v. Indirect relationships through intermediaries who are not (or not sufficiently) subject to AML/CFT measures or who are not supervised;
vi. Customers who are Politically Exposed Persons (PEPs); and
vii. Occasional customers that do transactions above a certain threshold.

2.12 The delivery channels play a role when assessing the customer risk. The extent to which the entity works with customers directly or through intermediaries or correspondent institutions, or establishes business relationships without customers being physically present are important factors to be considered in assessing the risk of a category of customers. The entity should describe all types or categories of customers that it provides business to and make an estimate of the likelihood that these types or categories of customers will misuse the entity for money laundering or terrorism financing, and the consequent impact if it occurs.

2.13 A comprehensive ML/TF risk assessment must take into account the potential risks arising from the transactions, products and services that the entity offers to its customers and the way these products and services are delivered to the customer. The entity should pay particular attention to ML/TF risk, which may arise from the application of new technologies. In identifying the risks of transactions, products, and services, the following factors can be considered:

i. Services identified by internationally recognised and credible sources as being a

higher-risk, such as international correspondent banking services and (international) private banking activities;

ii. Services that inherently promote anonymity or can readily cross international borders, such as online banking services, prepaid cards, private investment companies and trusts;
iii. New or innovative products or services that are not provided directly by the entity but are provided through channels of the entity;
iv. Products that involve large payment or receipt in cash;
v. Non face-to-face transactions or services;
vi. One-off transactions

2.14 For the risk assessment, the entity should describe all products and services that it provides and make an estimate of the likelihood that customers will misuse that product for money laundering or financing of terrorism, and the impact thereof.

2.15 The ML/TF risk of each entity is specific and requires an adequate risk management approach, corresponding to the level and structure of the risk, and to the size of the entity. The objectives and principles of ML/TF risk management should enable entities to establish a business strategy, risk appetite, adequate policies and procedures, promote high ethical and professional standards and prevent entities from being misused, intentionally or unintentionally, for criminal activities.

2.16 ML/TF risk management requires attention and participation of several business units with different competences and responsibilities. It is important for each business unit to precisely know its role, level of authority and responsibility within the entity's organisational structure and within the structure of ML/TF risk management.

2.17 It is desirable for managers of different lines of business, responsible for risk management at the level of their organisational unit, to develop ML/TF risk management procedures, corresponding to the specific tasks of the organisational unit in question. This must be harmonised with the objectives and principles of ML/TF risk at the level of the entity as a whole.

2.18 Management gives direction to its business activities by setting the risk appetite, formulating objectives and making strategic choices from which subsequently policies and procedures are derived. Management should be able to determine the ML/TF risks of the business and take into account in the entity's ultimate goals and strategies. Documentation and communication of strategy, policies and procedures are important for their actual implementation.

2.19 Management should be actively involved in analysing and recognizing ML/TF risks and take adequate control measures (e.g., by allocating sufficient resources to setting up an adequate monitoring system or training). Management will thereby receive support from functions (compliance, security, risk management, commercial functions, etc.) that possess relevant knowledge and experience. Management should also determine the risk tolerance while guarding against the entity accepting customers or providing products and services on whom or which the entity has no knowledge or experience. It should ensure that sufficient account is taken of ML/TF risks in the development and pre-introduction phase of new products and services. It is important in this respect that members of the management team involved in the decision-making process have sufficient authority and powers to take and implement the necessary decisions.

2.20 Management's leadership abilities and commitment to the prevention of money laundering and terrorism financing are important aspects of implementing the risk-based approach. Management must encourage regulatory compliance and ensure that employees abide by internal procedures, policies, practices and processes aimed at risk mitigation and control. Management should also promote an ethical business culture and ethical behaviour.

2.21 Once the identification and risk analysis processes are completed, the strategy of ML/TF risk management is applied to enable the entity to implement adequate policies and procedures for reducing the risks and bringing it down to an acceptable level. This is geared towards avoiding reputational risks, operational risks, risks of sanctions imposed by a regulatory body and other forms of risk.

2.22 The policies and procedures should be approved by management and be applicable to all business units, branches and subsidiaries. They should allow for sharing of information between business units, branches and subsidiaries, with adequate safeguards on confidentiality and use of information exchanged. By assessing the risks and developing policies and procedures, the entity ensures the continuity of ML/TF risk management controls despite any changes in the management or staff composition or structure.

2.23 The policies and procedures should enable the entity to effectively manage and mitigate the identified risks and focus its efforts on areas in its business, which are more vulnerable to ML/TF misuse. The higher the risk, the more control measures have to be applied. An entity can implement adequate ML/TF risk controls for higher

risk products by setting transaction limits and/or a management approval escalation process. In addition, the development and application of risk categories for customers together with customer due diligence and transaction monitoring measures based on those risk categories is one of the strategies for managing potential ML/TF risks posed by customers. Specific policies and procedures will therefore need to be developed with respect to customer due diligence, transaction monitoring, recordkeeping and reporting to the FIU.

2.24 Management should be able to adequately manage ML/TF risks, to verify the level of implementation and functioning of the ML/TF risk controls, and to ascertain that the risk management measures correspond to the entity's risk analysis. The entity should therefore establish an appropriate and continuing process for ML/TF risk monitoring and review. This process will be done by the business control function to ensure on a regular basis that all processes are implemented; the compliance function to periodically monitor if the policies are adhered to and systems are in place; and the audit function to assess if the policies and process conform to the law and are performed in an adequate way.

2.25 Monitoring of ML/TF risks should include regular reports to management, which should contain the following:

i. The results of the monitoring process,
ii. Findings of internal controls,
iii. Reports of organisational units in charge of compliance and risk management,
iv. Reports of internal auditing, reports of the person authorised for detecting,
v. Monitoring and reporting any suspicious transactions to the FIU,
vi. As well as the findings contained in the supervisor's inspection reports on AML/CFT.

2.26 Management should be furnished with all relevant information, which will enable it to verify the level AML/CFT controls, as well as possible consequences for the entity's business if controls are not functioning properly.

2.27 The risk reports should indicate if appropriate control measures are established, adequate, and fully implemented for the entity to protect itself from possible ML/TF misuse. The monitoring and review process should include the appraisal of ML/TF risk exposure for all customers, products and activities, and ensure the implementation of proper control systems, with a view to identifying and indicating problems before any negative consequences for the entity's business occur. This process may also alert the

entity to any potential failures, for instance failure to include mandatory legislative components in the policies and procedures, insufficient or inappropriate customer due diligence, or level of risk awareness not aligned with potential exposure to ML/TF risks.

2.28 The entity must keep the ML/TF risk assessment up to date by setting up and describing the process of periodically reviewing the risk assessment. The entity must therefore also stay up-to-date with ML/TF methods and trends, international developments in the area of AML/CFT, and domestic legislation. Such a review can also include an assessment of the risk management resources such as funding and staff allocation and may identify any future needs relevant to the nature, size and complexity of the entity's business. A review should also be conducted when the business strategy or risk appetite of an entity changes or when deficiencies in the effectiveness are detected. When the entity is to introduce a new product or activity, an ML/TF risk analysis of that product is to be conducted before offering that new product or activity to customers.

2.29 Adopting Risk-Based Approach (RBA)

2.30 The FIs may adopt RBA and direct more resources to high risk areas and use simplified AML/CFT measures in areas where the ML/TF risks are generally low. However, the FIs enhanced due diligence measures should be taken where there is suspicion of money laundering and terrorist financing.

3.0 GUIDELINE III: AML/CFT COMPLIANCE PROGRAMME

3.1 What is AML/CFT Compliance programme

3.2 The AML/CFT Compliance programme is a legislative is a legislative requirement and a good business practice for all categories of reporting entities to implement. A well-designed, applied and monitored programme will provide a solid foundation for compliance with the AML/CFT Act and other relevant laws in The Gambia which have impact on AML/CTF. Verily, the financial institutions have different structures and provide varying types products and services and serving many types of customers; therefore, the compliance programmes of the financial institutions should be tailor made to reflect these realities.

3.3 The AML/CF Compliance Programme of financial institutions include the following:

i. Conducting a ML/TF risk assessment
ii. Approval and oversight by boards and senior management
iii. Appointing an AML/CTF compliance officer
iv. Regular independent review of the compliance programme
v. Employee due diligence program
vi. AML/CTF risk awareness training program
vii. Feedback mechanism
viii. Reporting obligations
ix. Ongoing customer due diligence

3.4 Conduct a ML/TF risk assessment

3.5 Money Laundering and Terrorist Financing Risk Assessment entails identifying money laundering and terrorist financing risks and developing policies and procedures to minimise and manage that risk. This requires the development of a framework to identify, prioritise, treat (deal with), control and monitor risk exposures. The risk management process involves assessing risks against the likelihood (or chance) of them occurring and the severity or amount of loss or damage (or impact) which may result if they do occur.

3.6 ML/TF risk is the risk that the financial institution or its products, services or delivery channels may be exploited by criminals to facilitate money laundering or terrorism financing. Financial institutions should therefore always guard against being used by criminals to advance their illegal activities. To achieve this, the financial institution should assessing the risks pose by the following:

i. Customer types-this is the ML/TF risks which customers may pose to the financial institution, including any customers who are politically exposed persons (PEPs) and their associates
ii. Product/Service types-this is the ML/TF risk which may emanate from financial services provided by the financial institution to its customers
iii. Geographic area-some areas where the financial institutions are located may pose ML/TF risks
iv. Delivery channel risks-this is the risk that the mode delivery of services may be used by criminals to launder funds or finance terrorism;

3.7 The financial institutions are required to measure ML/TF risk for each category (i.e. i, ii, iii & iv) and must measure the level of risk (for example high, medium or me). The financial institutions should implement internal controls and procedures to mitigate the ML/TF risk and adopt appropriate measures to manage the residual risk based on their risk appetite.

3.8 Approval and oversight by board and senior management

3.9 The Anti-Money Laundering and Counter Terrorism Financing Programme must be approved by the governing board of the financial institution and fully implemented. The board and senior management must make sure that they design, develop and implement a robust AML/CFT programme in their institution.

3.10 The board of directors is ultimately responsible for the effectiveness of the financial institution's AML/CFT framework. The board's oversight role is intended to

ensure, amongst other things, that there is compliance with all the relevant laws and regulations and international standards and that the institutions strive to achieve international best practices standards. They should ensure that such compliance framework assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

3.11 Directors and senior management should be aware that the use of a group-wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the financial institution and is compliant with the laws, regulations and guidelines of Republic of The Gambia.

3.12 Directors and senior management should also ensure that the laws and regulations are also adhered to by their subsidiaries and branches in and outside of the Republic of The Gambia. They should also understand that where some of a financial institution's operational functions are outsourced, the financial institution retains full responsibility for compliance with local laws, regulations and guidelines.

3.13 Directors and senior management are required to have knowledge and thorough understanding of their duties, their staffs' responsibilities and the obligations and responsibilities placed on the entities they represent. They should supervise and approve the development of AML/CFT policies and procedures that are appropriate to the risks faced by their institutions. The senior management should adequately inform board of directors about the adequacy of and effectiveness of the AML/CFT risk management systems.

i. 3.14 This oversight function by board and senior management should include:
ii. Ongoing reporting to the board on the performance and effectiveness of the AML/CTF procedures, including the results of an independent review, instances of non-compliance with the AML/CTF Act and any feedback received after an assessment by the Financial Intelligence Unit of the AML/CFT program
iii. Periodic review of the ML/TF risk faced by the financial institution to ensure the financial institution's risk-based procedures and controls are appropriate and proportionate to the ML/TF risk it faces
iv. The Board should take concrete actions to hold staff responsible for any infractions in the implementation of the AML//CFT Programme.

3.15 Appointing an AML/CTF compliance officer

3.16 Each financial institution must appoint a compliance officer in accordance with

Section 39 of the AML/CTF Act 2012. The compliance officer must be appointed at senior management level who should report direct to the board. The compliance officer should have the authority and resources to perform his or her responsibilities, including access to all relevant areas of the financial institution's operations and all relevant staff members (at any level) and the power to address problems relating to AML/CTF compliance and reporting obligations.

3.17 Duties of an AML/CTF compliance officer

i. 3.18 The compliance officer under Section 39 of the AML/CTF Act 2012 must be appointed at senior management level with the following functions:

ii. implement the customer identification and verification requirements
iii. implement record keeping and retention requirements
iv. implement the reporting requirements
v. make its officers and employees aware of the laws relating to money laundering and financing of terrorism;
vi. make its officers and employees aware of the procedures, policies and audit systems adopted by it to deter money laundering and financing of terrorism; or
vii. screen persons before hiring them as employees or assigning them duties
viii. train its officers, employees and agents to identify suspicious transactions, trends in money laundering and financing of terrorism activities and money laundering and financing of terrorism risks within reporting entities' products, services and operations;
ix. perform independent audits to test the compliance of its anti-money laundering and financing of terrorism procedures and systems
x. conduct AML/CFT risk assessment and implement measures to manage risk
xi. implement policies and procedures to prevent the misuse of technological developments including those related to electronic means of storing and transferring funds or value
xii. ensure continued compliance with the requirements of the AML/CTF Act 2012 and AML/CFT Guidelines
xiii. report non-compliance of the AML/CTF Act 2012 and AML/CFT Guidelines to the board and senior management
xiv. address any FIU feedback about the reporting entity's risk management performance or AML/CTF programme
xv. act as the FIU contact officer for matters such as reporting suspicious matters, international funds transfer instructions and threshold transactions, urgent reporting, compliance audits, or requests for information or documents

xvi. contribute to designing, implementing and maintaining internal AML/CTF compliance manuals, policies, procedures and systems
xvii. ensure full implementation of AML/CFT programme

3.19 Independent review of the AML/CFT programme

3.20 The financial institutions should conduct independent review of the AML/CTF policy/program every two years from the date it was approved by the board of directors of the financial institutions. The review must done by an independent person. Such an independent reviewer may be an internal or external person; for example an employee of the reporting entity such as the internal audit or legal department staff or external auditors or other compliance specialists. The review should assess the effectiveness of the AML/CFT Programme, compliance with the AML/CFT programme and the AML/CTF Act 2012 and best practices.

3.21 Employee due diligence programme

3.22 An employee due diligence program refers to the documented procedures for screening staff members to minimise any exposure to ML/TF risks. An employee due diligence programe should cover;

i. screening of prospective employees who, if employed, may be in a position to facilitate the commission of a money laundering or financing of terrorism offence
ii. rescreening existing employee, where the employee is transferred or promoted and may be in a position to facilitate the commission of a money laundering or financing of terrorism offence

3.23 A reporting entity should establish procedures to identify and verify the identity of prospective or existing employees, confirm their employment history (for example, through references or referee reports) and determine if they are suitable to be employed in a particular position in the business. The procedures should take into account the role of the employee and the nature, size and complexity of the business, and the type of risk it might reasonably face.

3.24 A reporting entity may determine that certain positions pose a higher risk than others because they may be, for example, vulnerable to collusion with, or coercion by, third parties. In such cases, the AML/CTF programme may set out more rigorous screening processes for higher risk positions.

3.25 Where an employee is engaged in a role that poses a high risk, the reporting

entity should require the applicant to provide Certificate of Character issued by the Gambia Police Force.

3.26 An employee due diligence programme must also outline a system to manage an employee who fails, without reasonable excuse, to comply with any system, control or procedure under the AML/CFT programme. A financial institution may consider establishing policies outlining the consequences of employee non-compliance with AML/CTF requirements; for example, disciplinary action ranging from issuing formal warnings through to dismissal, depending on the scale and seriousness of the breach refer staff to mandatory refresher training.

3.27 AML/CTF training programme

3.28 The AML/CTF programme must include an AML/CFT trainings for all categories of employees. The financial institution should extend AML/CFT training to boards of directors.

3.29 AML/CFT trainings are central to a financial institution's effort to protecting its business from being used to facilitate money laundering or terrorism financing. The training should ensure that employees are aware of the ML/TF risks related to the institution’s business and their role in mitigating the risk by contributing to the financial institution's overall compliance with relevant laws, regulations and guidelines.

3.30 The reporting entity should ensure that employees are aware of the sources of ML/TF risk to the reporting entity, the reporting entity's commitment to AML/CTF compliance, the reporting entity's AML/CTF policies and procedures, the reporting entity's obligations under the AML/CTF Act, regulation and guidelines and the consequences of non-compliance.

3.31 The training programme may specify who needs to be trained (for example, existing employees, new employees, employees transferring to different positions, senior managers, and new directors. It should also specify training courses for all categories of staff. The training programme may also describe how the training will be conducted; for example, through on-the-job training, especially for training relevant to a specific role, induction training, incorporating AML/CFT awareness for new employees and employees transferring into new positions, instructor-led training, whether through in-house training units or external training providers, online e-learning courses, ongoing communication of changes and updates to systems, controls

and procedures.

3.32 The training programme should apply at a minimum, to all employees who are in a position which has been assessed as posing a high ML/TF risk, have contact with customers, authorise and approve customer transactions, handle cash or funds, facilitate transaction reporting to the FIU, oversee or implement the AML/CFT programme. A financial institution's training programme should be reviewed and maintained to accommodate changes to the ML/TF risk faced by the reporting entity and the operating environment.

3.33 Feedback mechanism

3.34 A financial institution's AML/CFT programme must include appropriate procedures to facilitate feedback to the FIU on the financial institution's performance in managing ML/TF risk. This includes procedures for addressing recommendations contained in any reports FIU prepares on the financial institution's compliance with the AML/CTF Act, regulations or guidelines issued by the FIU or the supervisory authority. The FIU may also, from time to time, provide industry specific compliance feedback and guidance that reporting entities should use to maintain their AML/CFT programme and keep it up to date.

3.35 Reporting obligations

3.36 The AML/CFT Programme must include details about the reporting entity's AML/CFT reporting obligations; and appropriate systems and controls designed to ensure compliance with the reporting obligations.

3.37 A reporting entity's reporting obligations include the reporting of Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs) and any other reports the FIU may require financial institutions to file.

4.0 GUIDELINE IV: CUSTOMER DUE DILIGENCE (KNOW YOUR CUSTOMER)

4.1 The financial institutions are obliged to incorporate comprehensive Customer Due Diligence (CDD) processes and procedures which shall include the identification and verification of identities of customers and beneficial owners, whether natural or legal before establishing business relationship or in the course of an already established relationship as stipulated in the AML/CTF Act, 2012. The obligation of customer identification and verification of identity extends to occasional customers and one off transactions. The main aim of the customer due diligence is for the financial institutions to know their customers and the people they deal with so as to prevent their products, services and systems from being exploited by criminals.

4.2 The CDD helps to prevent the financial system from being used by criminals in the commission of money laundering, terrorist financing, criminal conducts and related financial crimes. This requirement is the basic banking principle of Know Your Customer (KYC), i.e. it entails obtaining full particulars of the identity of a customer and having adequate knowledge of the purpose for which the customer desires to establish a business relationship with a financial institution. Evidence of identity is considered satisfactory if it establishes that the applicant is the person who he claims to be. As a result evidence shall be in such a form as to be able to provide undoubted identification should an investigation be undertaken at any future time. The best source would be a valid identity card, passport or other document bearing a photograph and other personal information of the applicant.

4.3 The financial institutions shall identify the customer (whether resident or non-resident, occasional, natural or legal persons, or legal arrangements) and verify the customer's identity using reliable, independent source documents, data or information.

4.4 For legal persons and arrangements this shall include institutions taking reasonable measures to understand the ownership and control structure of the customer.

4.5 All information obtain during verification should singularly or cumulatively be able to demonstrate that the individual so verified exists at the address given and that the he/she/it is the person whom the financial institution had established a relationship with and is the same as the documentation provided at the point of establishing relationship. Financial institutions should be able to ensure that their customers are not subject to sanctions by the United Nations or similar prohibition from any other official body or government.

4.6 The financial institution should always guard against forged copies of identification documents, as such they should sight and examine the original documents, copy and sign them as sighted with date. Where home visitation is conducted, financial institutions should record what was found with clear description of the building and its locations using landmarks where possible.

4.7 The identification and verification of identity should be done within a reasonable time or before entering into a business relationship with a customer using any official or other identifying document and verify the identity of the customer using reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer when an FI

a) enters into a continuing business relationship or conducts any transaction,
b) carries out an electronic funds transfer,
c) is suspicious that a money laundering or the financing of terrorism is involved or
d) has doubts about the veracity or adequacy of the customer identification and verification documentation or information it had previously obtained.

What constitutes an acceptable time span must be determined in the light of all the circumstances including the nature of the business and whether it is practical to obtain the evidence before commitments are entered into or money is exchanged. As a golden rule financial institutions are to obtain the evidence of identity prior to entering into commitments with the applicant for business.

4.8 In the case of casual customer the financial institution shall identify the customer and verify the identity of the customer for any transaction involving a sum greater than two hundred thousand Dalasi, and where the transaction is carried out in more than one transaction which seem to be connected and the amount is unknown at the start of the transaction, as soon as the amount is greater than two hundred thousand Dalasi.

4.9 Where a natural person conducts a transaction through a financial institution and the reporting entity has reasonable grounds to believe that the person is undertaking the transaction on behalf of a third party, then, such third party shall be identified and the identity verified. Where there are underlying principal(s), the true nature of the relationship between the principals and the account signatories must also be established and appropriate enquiries carried out on the former, especially if the signatories are acting on the instructions of the principal(s). In this context "principals" shall be taken to include beneficial owners, settlors, controlling shareholders, directors, major beneficiaries, etc., but the standard of due diligence will depend on the exact nature of the relationship and risks.

4.10 Where a financial institution is unable to obtain satisfactory evidence of the identity of a customer, the reporting entity shall not establish an account for or maintain a business relationship with the customer, and make a report of the attempted transaction to the Financial Intelligence Unit.

4.11 If during the establishment of business relationship, or when carrying out occasional transactions, an FI suspects that transactions relate to ML or TF, the financial institution is required to;

a. Seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.

b. File STR to the FIU if it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF.

4.12 When performing customer due diligence (CDD) in relation to legal persons or arrangements, FIs shall;

a. Verify that any person purporting to act on behalf of the customer is so authorized, and identify that person,

b. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation or similar evidence of establishment or existence and obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement,

c. Identify the beneficial owners, including forming an understanding of the ownership and control structure, and take reasonable measures to verify the identity of such persons. Measures needed for satisfactory performance of this function shall require identifying the natural persons with a controlling interest and identifying the natural persons who are the main players of the legal person or arrangement,

d. For trusts, identify the settlor, the trustee or person exercising effective control over the trust and beneficiaries.

4.13 Financial institutions are required to obtain information on the purpose and intended nature of the business relationship of the applicant and conduct ongoing due diligence on the business relationship. This shall include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business risk profile, and where relevant, the source of funds.

4.14 Financial institutions are prohibited from opening or maintaining anonymous accounts and accounts in fictitious names or numbered accounts.

4.15 CUSTOMER IDENTIFICATION AND VERIFICATION

4.16 Identification of Natural Person (Gambian Resident)

4.17 For the purpose of identifying a Gambian Resident in The Gambia the financial institutions shall collect the following from the customer or from any available source(s):

1. Valid identification document such as passport, national identity card, driver's license or voter's card with clear photo
2. Tax identification certificate
3. Names

4. Residential address
5. Nationality
6. Official Personal Identification Number or other Unique Identifier as in National Identity Card, Passport, Tax Identification Certificate
7. Date and place of birth
8. Gender
9. Occupation or position held where applicable
10. Name of employer where applicable
11. Telephone, fax numbers, and e-mail address
12. Source of income, if a PEP, the source of wealth
13. Expected use of the account: amount, type, purpose and frequency of the transactions expected
14. Financial products or services requested by the customer
15. Destination of funds passing through the account
16. Specimen signature
17. Any other relevant information

4.18 Verification of Identity of Natural Person (Gambian Resident)

4.19 The financial institutions are required to verify the identity of the customer through information collected in paragraph 4.17by using reliable, independent sourced documents, data or information. The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should enable the financial institution to satisfy itself that it knows who the customer is.

4.20 The financial institution shall use combination of the following to verify the identity of customers:

i. Confirm the identity of the customer or the beneficial owner from a valid official document such as Passport, National Identification Card, Driver's License or voter's card or other official identification document that may be approved by Minister Responsible for Finance and Economic Affairs that bears a photograph of the customer

ii. Confirm the date and place of birth from an official document

iii. Confirm the validity of official documentation provided through certification by an authorized person where there is suspicion 3 of the validity and veracity of

the document obtained

iv. Confirm the residential address through customer visitation where applicable

v. Contact the customer by telephone or email

vi. Collect reference on the customer

vii. Search on Credit Reference Bureau database where applicable

viii. Any other means of identity verification

4.21 Where a person purporting to act on behalf of the customer, the financial institution shall identify and verify identify of the person so authorized using the same identification and verification requirements required for Gambian Resident in The Gambia. The financial institution shall verify the authorization to act on behalf of the customer by use of signed authority, official judgment or equivalent documents.

4.22 Identification of Natural Person (Gambian Non-Resident)

4.23 In addition to the identification documents mentioned in paragraph 4.17 the financial institution shall collect any five of the following:

i. Country of residence
ii. Resident Permit or any reliable document issued by the foreign country where applicable
iii. Residential address abroad
iv. Other Nationality
v. untry
vi. Telephone numbers
vii. Utility Bills (if applicable)

4.24 Verification of identity of Natural Persons (Gambian Non-Resident)

4.25 In addition to verification requirements specified in paragraph 4.18, the financial institution shall;

i. Confirm the residential address in the foreign country

ii. Obtain notorisation (by authorized person) of the official document such as Passport, National Identification Card, Driver's Licence or Residential Permit or any other official document

iii. Any additional means of verification

4.26 Identification of Natural Person (Foreign National Resident in The Gambia)

4.27 In addition to identification requirements in paragraph 4.17the financial institutions shall use the following to identify foreign nationals resident in The Gambia:

i. Official foreign identification document such as passport, national identity card or driver's license

ii. Alien Permit or identity card

4.28 Verification of identity of natural persons (Foreign National Resident in The Gambia)

4.29 In addition to verification requirements in paragraph 4.18 the financial institutions are required to conduct the following:

i. Obtain the Security Clearance for foreign nationals from high risk countries

ii. Confirm if the person is not in any sanction lists

iii. Any additional means of verification

4.30 Identification of natural person (Foreign National Non-Resident in The Gambia)

4.31 In addition to the identification requirements in paragraph 4.17, the financial institutions are required to identify such customers by obtaining the following:

i. Obtain notorised copies of the identification document

ii. Notorisation shall be done by authorized person/entity in The Gambia

4.32 Verification of identity of natural person (Foreign National Non-Resident in The Gambia)

4.33 In addition to verification requirements in paragraph 4.27 the financial institutions shall carry out the following for the purpose of verification of identity:

i. Obtain reference from a Gambian resident or non-resident

ii. Verify the identity of Gambian providing the reference

4.34 Identification requirements for enterprises/sole proprietorship businesses

4.35 For the purpose of identification of identities of enterprises or sole proprietorships, the financial institutions are required to obtain the following:

i. Identify the natural person(s) operating the business as required in paragraph 4.17

ii. Identify the ultimate beneficiaries where applicable

iii. Business/Owner's tax identification certificate

iv. Obtain the business registration certificate

v. Obtain the audited financial statements where applicable

vi. Business lines and business turnover

4.36 Verification of identity for enterprises and sole proprietorships

4.37 In addition to verification requirements in paragraph 4.18 the financial institutions shall carry out the following:

i. Confirm the place of business through customer visitation

ii. In case of doubts as to authenticity or veracity of the identification documents, obtain verification from the issuing authority

iii. Confirm business address, telephone number and email, where applicable etc.

iv. Obtain evidence of payment of Municipal or Area Council fees or duties

v. Verify annual business registration certificate

vi. Verify annual business certificate for new business

vii.

4.38 Identification requirements for corporations or limited liability entities

4.39 The financial institutions are required to adequately identify the identities of corporations, companies and limited liability companies by obtaining the following:

i. Name of the corporation, company, entity
ii. Memorandum and Articles of Association
iii. Business Registration Certificate
iv. Permanent address of the principal place of business and other locations
v. Types of business
vi. Tax identification certificate
vii. Contact phone numbers, e-mails, fax, website, where applicable
viii. Audited financial statements where applicable
ix. Expected account activity, turnover, deposits
x. Products and services required
xi. Source of funds Board Resolution to open and operate account
xii. Power of attorney (where applicable)
xiii. Identify signatories to the account as provided in paragraph 4.18
xiv. Identify identities of shareholders holding 10% of shares and above
xv. Identify identities of beneficial owners (i.e. beneficial owners, people or entities holding beneficial interests) behind a corporate body before a business relationship is established) if they exist

4.40Verification of identities of corporations, companies or limited liability entities

4.41 The financial institutions are required to verify the identity of such customers by obtaining the following:

i. Verify authenticity of memorandum and articles of associations from issuing authority
ii. Verify the authenticity of business registration from issuing authority
iii. Obtain reference
iv. Sight the audited financial statements where applicable
v. Verify business address by customer visitation
vi. In case of subsidiaries, obtain the business registration certificate and certified copies of memorandum and articles of associations by authorized person resident in The Gambia
vii. Conduct open source searches
viii. Verify identities of signatories, shareholders holding 10% shares and above and ultimate beneficiaries
ix. Undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated
x. Obtaining prior bank references
xi. Contact the corporate entity by telephone, mail or e-mail.
xii. Obtain the by-laws where applicable and/or any other relevant corporate documents filed with the Companies' Registry
xiii. Obtain annual reports where applicable
xiv. Verify whether the power of attorney is valid by contacting other persons related to the company
xv. Any other means of verification

4.42 Where signatories of a corporate entity are not directors, mangers or employees of the corporate entity, financial institution should exercise caution and ensure that the identity of the signatories are verified in compliance with these guidelines. The financial institutions should closely monitor the ongoing business relationship with the corporate body.

4.43 Corporate bodies may sometimes be part of a complex organization, as such trusts and foundations. Financial institutions are required to show particular care when verifying the legal existence of such entities and to ensure that any person purporting to act on behalf of the corporate entity is authorized to do so. The principal requirement is to look behind the corporate veil of the entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. For such entities, financial institutions are required to confirm that such entities exist for legitimate reasons and as such may visit the

business/company to ensure that there is an actual physical presence.

4.44 Where a financial institution suspects a change in the corporate structure of an entity or suspects a change in the nature of business of an entity, the financial institution should carry out a further check on the entity.

4.45 Financial institutions should ensure that identities of new signatories of a corporate entity are verified whenever they change. They may also need to confirm if there were also changes in the directors or shareholders or the nature of the business. It should be noted that such changes could be an indicator for the need to conduct a fresh risk assessment of the company as they may have potential money laundering and terrorist financing tendencies.

4.46 Identification requirements for Government Entities (corporations, agencies, commissions, parastatals, ministries, departments and others

4.47 The financial institutions shall obtain the following:

i. Name of the entity
ii. Evidence of establishment of entity such as Act of Parliament, Regulation, where applicable
iii. Tax Identification Certificate
iv. In case of public private partnership obtain identities of the private party or parties, beneficial owners and obtain the agreement or documentation of the arrangement
v. Approval from National Treasury, relevant line ministry and/or Ministry of Finance and Economic affairs to open an account
vi. Permanent address and other locations
vii. Functions, types of activities
viii. Contact phone numbers, e-mails, fax, website, where applicable
ix. Audited financial statements where applicable
x. Expected account activity, turnover, deposits
xi. Products and services required
xii. Source of funds and wealth
xiii. Board Resolution to open and operate account
xiv. Power of attorney where applicable
xv. Identify signatories to the account as provided in paragraph ******
xvi. Identify identities of shareholders holding 10% or more of shares where applicable

4.48 Verification requirements for Government Entities (corporations, agencies, commissions, parastatals, ministries, departments and others

i. Verify whether the entity is established by law
ii. Verify whether the board is constituted or not
iii. Verify the business address by customer visitation
iv. Contact relevant ministries to ascertain entity's existence
v. In case of public/private partnership verify identities of the private entity or entities, the beneficial owners or the ultimate beneficiaries and verify the agreement from competent authority Conduct open source searches
vi. Obtaining prior bank references where applicable
vii. Contact the corporate entity by telephone, mail or e-mail
viii. Obtain the by-laws where applicable and/or any other relevant corporate documents filed with the Companies' Registry
ix. Obtain annual reports where applicable
x. Verify whether the power of attorney is valid by contacting other persons related to the company (where aplicaple)

4.49 Identification requirements for partnership business

4.50 The financial institution shall obtain the following:

i. Name of partnership or unincorporated business
ii. Principal business address
iii. Telephone contact details and emails where appropriate
iv. Tax Identification Certificate
v. Partnership deed or agreement
vi. Description and nature of the business
vii. Business registration certificate
viii. Bussiness annual Return
ix. Date of commencement of business
x. Products or services offered or line of business
xi. The reason for establishing the business relationship with the financial institution
xii. Annual financial statement, where appropriate
xiii. Partner Resolution to open bank account
xiv. Identification of partners as well as beneficiaries
xv. Such documentary or other evidence as is reasonably capable of establishing the identity of the partners or beneficial owners

4.51 Verification of identity of partnership business

4.52 The financial institution shall verify the identity of the partnership business by requesting the following:

i. Verification of identity of partnership and unincorporated business
ii. Obtain identities of all partners, beneficiaries shall be same for natural persons
iii.
iv. Verify business address by customer visitation
v. Contact the business by telephone, fax, e-mail where possible
vi. Confirm existence of the partnership from the relevant government institution where there is doubt as to the authenticity or veracity of the documents provided
vii. Audited financial statement where appropriate
viii. Verify from an independent source where possible

4.53 Other Legal Structures and Fiduciary Arrangements

4.54 Financial institutions should verify the identity of the provider of funds for a trust or settlor and all those who have the power to remove the trustees and advisors of a foundation, a nominee and fiduciary accounts or any other legal structure. This is important as Legal structures such as these can be used by criminals who wish to mask the origin of funds derived from crime if the trustee or fiduciary does not carry out adequate procedures.

4.55 Trust Clients

4.56 When an account is open on behalf of a person or a transaction conducted on behalf of person, financial institution should take reasonable measures to obtain information about the true identity of those persons on whose behalf an account is opened or a transaction is conducted.

4.57 At a minimum, the financial institution should obtain the following, whether the financial institution is a named trustee or is providing services to a trust:

i. Name of trust
ii. Nature/type of trust
iii. Country of establishment
iv. Identity of the ultimate natural person providing the funds, if not the ultimate

settlor

4.58 The financial institution should conduct the following in addition to obtaining identification evidence for the trustee(s) and any other person who is signatory on the account, or has any decision making powers that affects the business relationship so established with the financial institutions;

a. Make suitable enquiries for the purpose of obtaining information about the legal structure and the source of funds of the client or customer;
b. Financial institutions are required to obtain the identification and evidence of the settlor, protector(s) or and/controller(s) and for any person or persons that wields an effective control over the trust which includes an individual who has the power whether alone or jointly or with the consent of another person to do the following;

i. Dispose of, advance, lend, invest, pay or apply the trust property;
ii. Vary the trust;
iii. Add or remove a person as a beneficiary or to or from a class of beneficiaries;
iv. Appoint or remove trustees;
v. Or direct the conduct of (i) to (iv) above or withhold consent to exercise or veto the exercise of powers such as mentioned in (i) to (iv) above.

4.59 For nominee relationships, financial institutions should obtain identification evidence for the beneficial owner(s).

4.60 Financial institutions should ensure that ongoing due diligence is maintain in circumstances where changes happens in any of the parties to a trust, revision of the trust, addition of funds to the trust, investment of trust funds or distribution of trust assets or provision of benefits out of trust assets.

4.61 Where a settlor dies, written proof should be obtained for the source of funds in the form of a will creating the trust or Grant of Probate,in line with the applicable laws.

4.62 Financial institutions are required to certify any of the documents so obtain as certified true copies in addition to cross-checking any bank account on which the trustees have drawn funds from are in their names and any additional signatories are verified.

4.63 Any application to open an account or undertake a transaction on behalf of another without the applicant identifying a trust or nominee capacity should be regarded as suspicious and should trigger further enquiries.

4.64 A financial institution should undertake a verification of the identity of any beneficiary of a legal structure. Though it can be difficult to identify the beneficiaries of trusts precisely at the outset as some beneficiaries may be unborn children or only become vested when certain circumstances occur. In any circumstance, financial institution must conduct verification of beneficiaries before the first distribution of assets. Further, verification of protectors/controllers should also be undertaken the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice.

4.65 A trust is a mechanism where a settlor seeks to benefit a beneficiary, typically, not in return for any consideration as such financial institutions must maintain vigilance where there is no apparent connection or relationship of the settlor to the beneficiaries of a trust. A financial institution should try to understand the reason why the settlor wants to benefit a beneficiary with whom he seemingly has no connection.

4.66 Where an apparent relationship between the settlor and the trustee is absent, a financial institution should demonstrate that it understands the commercial rationale for the arrangement and has verified the identity of the various counterparties.

4.67 Financial institutions should obtain a copy of the trust creating instrument and other supporting documentation or instruments as a means of satisfying itself of the verification of the identity of trust.

4.67 Where applicable laws and regulations in the jurisdiction where trust are established prohibits the implementation of one or any of these guidelines, financial institutions are required to inform the Central Bank of the Gambia and the FIU of such prohibitions.

4.68 Identification requirements of Non-Profit Organisations

4.69 For the purpose of identification of Non-Profit Organisations and charities the financial institutions are required to obtain the following:

i. The foundation's charter and any official document which shows proof of establishment

ii. Business registration
iii. In the case of NGOs, approval from competent authority must be obtained
iv. Permanent location and branches
v. Contact details such as telephone, mailing address, e-mail or fax where applicable
vi. Identities of all natural persons
vii. Intervention areas
viii. List donors and their identities
ix. Tax Identification Certificate

4.70 Verification of identities for Non-Profit Organisations and charities

i. In the case of NGO, verify its existence from the NGOs affairs agency
ii. Confirm address by customer visitation
iii. Ascertain the source of funds of the NGOs
iv. Contact beneficiaries of the NPOs
v. Visit project sites where applicable
vi. Obtain audited financial statements where applicable
vii. Verify whether the NPO has no link to designated persons or sanctioned persons
viii. Conduct verification requirements for all natural persons

4.71 Executorships Accounts

4.72 Financial institutions should verify the identity of an executor of an estate where the business relationship was entered into for the purpose of winding up the estate. This verification should be conducted in line with this guidance, depending on the nature of the executor (whether personal, corporate, or a firm of attorneys). However, financial institutions need not verify the identity of the executor or administrator when payment from an established bank account in the deceased's name is being made to the executor or administrator in accordance with the Grant of Probate or Letters of Administration solely for the purpose of winding up the estate.

4.73 Identification and verification of identity of refugees and asylum seekers

4.74 A refugee or asylum seeker who applies to open a bank account without being able to provide the usual evidence of identity, reliance shall be placed on relevant document issued by competent authority in The Gambia. The identities of refugees or asylum seekers should be verified. As is required for such exceptional circumstances, accounts of this type shall be closely monitored to prevent their possible misuse given that such refugees could be PEPs.

4.75 Identification and verification of identity for minors

4.76 Financial institutions shall identify and verify the identity of the parent or guardian. The identification details of the minor shall be confirmed from the birth certificate.

4.77 Opening of accounts in joint names

4.78 The identification and verification of identities for natural persons shall be extended to all persons for the joint name.

4.79 Account opening for intermediaries

4.80 Intermediaries hold funds on behalf of their customers in clients' accounts. Such accounts may be general accounts holding the funds of many clients or may be specific accounts opened for a single client. In each case it is the intermediary who is the institution's customer and these situations should be distinguished from those where the intermediary introduces a client who himself becomes a customer of the institution.

4.81 Where an applicant for business is not acting as a principal, institutions are to obtain full identification of both the applicant and any person on whose behalf the applicant is acting. Applicant must be duly authorized in writing by the principal. Where the above identification cannot be done, in principle, the transaction shall not be carried out but it shall be considered suspicious and subsequently reported.

4.82 There are instances where the applicant for business is an advocate, notary, certified public accountant and auditor or nominee company established and practicing in The Gambia who is not acting on his own behalf. In such cases institutions shall obtain from these persons a signed declaration to the effect that they have the authority to act on behalf of the principal and ensure that:

i. Applicant is acting in his professional capacity
ii. Applicant has maintained a professional relationship with the principal for the immediate preceding three months
iii. If such relationship is not held, applicant must present satisfactory references from at least two persons who held such relationship
iv. Applicant is aware of business activities of principal and has no suspicion of present or possible future criminal activity

v. Applicant has obtained satisfactory evidence of identity of principal and
vi. Applicant will inform institution concerned upon revocation of powers

4.83 In the case where an applicant for business is a corporate body whose share capital is partly or totally held under nominee, FIs are not to undertake or carry out any business with such applicant unless they obtain disclosure of the full details of the ultimate beneficiary or beneficiaries.

4.84 Certification of Identification Documents

4.85 Due caution should be exercised by financial institutions when considering certified documents, this is especially so when such documents are said to emanate from jurisdictions that are perceived to be high risks or from unregulated entities. When a financial institution accepts such documents, it has the responsibility to satisfy itself that the certifying authority is appropriate. They should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

4.86 Customer identification and verification (Enhanced Due Diligence)

4.87 Non-face-to-face customer

4.88 Where financial institutions are requested to open accounts or form business relationships with persons who are not available for a personal interview, such as non-resident customers they shall pay special attention to any ML/TF risks that may arise from new or developing technologies that might favour anonymity, and take measures to prevent their services being used for ML/TF schemes.

4.89 In particular financial institutions shall have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.

4.90 Examples of non-face to face operations include:

i. Business relationships concluded over the internet or by other means such as through the post;
ii. Services and transactions over the internet including trading in securities by retail investors over the internet or other interactive computer services;
iii. Use of ATM machines;

iv. Telephone banking;
v. E-Transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

4.91 In accepting business from non-face-to-face customers, financial institutions shall apply equally effective customer identification and verification procedures and ongoing monitoring standards to non-face-to-face customers as for those available for interview.

4.92 Even though face-to-face and non-face-to-face customers can provide the same documents, it is more difficult to match the customer with the documentation in the case of non-face-to-face customers. Therefore, there must be specific and adequate measures to mitigate the risk.

4.93 The measures to mitigate risk shall include: -

i. Certification of documents presented
ii. Requesting for additional documents to complement those which are required for face-to-face customers
iii. Develop independent contact with the customer
iv. Independent verification of documents by contacting third party and third party introduction in line with these Guidelines and
v. Requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

4.94 Politically Exposed Persons (PEPs) and other high risk persons

4.95 The AML/CFT ACT, 2012 defines PEPs as individuals in The Gambia or in a foreign country entrusted with public functions, their family members or close associates. These functions include Heads of State or of government, senior politicians, senior government, judicial or senior military officials, senior executives of state owned corporations, important political party officials including immediate family members or close associates of the politically exposed person.

4.96 The financial institutions shall;

i. Develop clear procedures within their processes and procedures that would help in determining if a an already existing customer/client or policy holder has subsequently become a PEP, this may entail use of electronic databases or other commercial databases for politically Exposed Persons

ii. Take reasonable measures in establishing the source of funds or wealth of PEPs

iii. Exercise greater scrutiny on PEP accounts and/or transactions and conduct enhanced on-going monitoring of accounts/transactions such that changes in transaction patterns that suggest abuse of office or other corrupt practice or misuse of government property can be detected early

iv. Obtain senior management approval to establish business relationship or continue the relationship where a customer is found to be or subsequently becomes a PEP

v. Assess the money laundering and terrorist financing risks the PEP may pose and adopt measures to effectively manage the risks

vi. Keep close scrutiny of any complex structures (for example, legal structures such as corporate entities, trusts, foundations and multiple jurisdictions)

vii. Develop profile of expected activity from the business relationship between the financial institution and the PEP, this is to provide a basis for future monitoring of the relationship. The profiles should be review regularly and updated

viii. Keep close scrutiny of any unusual features, such as very large transactions, the use of government accounts, particularly where demands for secrecy, the use of cash or bearer bonds or bearer insurance policies or other instruments are involved, or any such products or service that can be used to break audit trail

ix. File timely reports to the FIU where proposed or existing business relationships with PEPs is suspicious

4.97 Products and services requiring special consideration

4.98 Special consideration should be given to the following products and services, which may pose an additional risk to a financial institution:

i. Provision of safe custody, safety deposit boxes, store cash products and insurance products; Where a financial institution offer and provide facilities to hold boxes, parcels and sealed envelopes in safe custody, it is expected that a financial institution should follow the identification procedures set out in these

Guidelines

ii. Life insurance and non-life insurance contracts such as
    a. Unit-linked with profit single premium contracts
iii. Single premium life insurance policies that store cash
iv. Fixed and variable annuities
v. Endowment Policies

4.99 Technological developments

4.100 Financial institutions should have policies and measures in place to prevent the misuse of technological products or platforms in money laundering or terrorist financing schemes. A financial institution that offers an internet-based or telephone products and services should ensure that it has reliable and secure methods to verify the identity of customers. Appropriate risks level of verification should be used commensurate with the risk level so identified as being associated with the customer, product or service either singularly or compositely. Financial institutions are required to implement multi-factor verification measures, layered security or other controls reasonably calculated to mitigate the risks so identified.

4.101 Reliance on third parties to conduct KYC

4.102 Any individual or entity that is not a direct party to a contract or agreement or transaction but is affected by it or has an interest in it will be regarded as a third party within these guidelines.

4.102 Circumstances occur where it becomes necessary for financial institutions to rely on a third party for the purpose of conducting KYC procedures. Under such circumstances, financial institutions can only do so when such entities are themselves financial institutions. Such circumstances could be any of the following:

4.103 When the financial institution cannot determine whether or not an occasional transaction involves cash because a customer deposited funds into an account that is held for and on behalf of the financial institution by another financial institution; or

4.104 Where a financial institution being an account holder of another financial institution, conducts a transaction on behalf of a customer, using the facilities of a financial institution, the financial institution may rely upon the written confirmation of that financial institution that it has verified the identity of the customer concerned.

4.105 This exemption applies only to occasional transactions conducted by financial institutions that are facility holders of a financial institution. However, appropriate due diligence most be carried out including obtaining necessary evidence of identity where a person is being introduced to the financial institution for the purpose of forming a business relationship with the financial institution.

4.106 Intermediaries

4.107 A financial institution is required to not only verify the identity of an intermediary but also to look beyond the intermediary to identify the client behind the intermediary. Measures must be taken by a financial institution to verify the identity of the underlying clients. In this regard, the financial institution should consider the nature of the intermediary, the domestic regulatory regime in which the intermediary operates, the intermediary's geographical base and to the type of business being conducted by the intermediary.

4.108 Exemptions and concessions

4.109 Financial Institutions

4.110 In the case where the FIU or Central Bank of The Gambia certifies either financial institutions or some other agency or body as an eligible introducer, a financial institution should satisfy itself that the financial institution does actually exist and is also subject to being regulated and subject to equivalent or higher AML/CFT standards of regulation.

4.111 In all cases the financial institution must be satisfied that it can rely on the eligible introducer. The financial institution may request from an eligible introducer such evidence as it reasonably required to satisfy itself as to the identity of the introducer and the adequacy and robustness of its KYC policies and procedures.

4.112 Occasional Transactions

4.113 An occasional transaction is one that is conducted by a person without an account or any relationship with the financial institution, a one-off transaction carried out by a person not through an established relationship in respect of which that person is a customer/account or holder. Occasional transactions may include:

i. Cheque cashing drawn on the financial institution

ii. Exchange of coins for notes or notes for coins
iii. Purchase of foreign currency for holiday travel
iv. Transactions via money transfer services business
v. Transfers to individuals by walk in customers to non-customers of financial institutions

4.114 It is important for a financial institution to determine whether an account holder is undertaking an occasional transaction, or whether the transaction is the initial step in an ongoing business relationship, as this can affect the verification requirements. The same transaction may be viewed differently by a financial institution and by an introducing intermediary, depending on their respective relationships with the account holder. Therefore, where a transaction involves an intermediary, both the financial institution and the intermediary must separately consider their positions and ensure that their respective obligations regarding verification of identity and associated record keeping are met. For occasional transactions exceeding D200,000.00 or its equivalent, financial institutions should conduct due diligence measures which should include identifying and verifying customers. This covers where the transactions are conducted as a single transaction or in multiple transactions that appear to be linked;

4.115 The degree of suspicion or materiality of such suspicion should determine the extent to which the identification and verification exercise that a financial institution should conduct on occasional transactions that exceeds the above mentioned thresholds.

4.116 Minimally, a financial institution should identify and verify the persons conducting occasional transactions below the above thresholds, maintain an effective system to monitor for abuse of occasional transactions; and establish clear instructions for the timely reporting of unusual and suspicious occasional transactions.

4.117 A financial institution needs to be vigilant such that it aggregates the series of linked transactions which exceeds the prescribed limit of D200,000 and they should verify the identity of the customer in such cases. These can be in cases where two or more occasional transactions appears at the outset or at a later stage, that the transactions are linked and that the aggregate amounts of the transactions exceed or are likely to exceed the prescribed D200,000 or its equivalent.

4.118 Though, there is some difficulty in defining an absolute time scale that linked transactions may fall within. International best practice dictates that identification of linked transactions that exceeds the prescribed thresholds can be identified over a

period of three months. Therefore the relevant procedures for linking will ultimately depend on the characteristics of the product rather than an arbitrary time limit.

4.119 Failure to satisfactorily complete CDD

4.120 Where a financial institution is unable to comply with CDD measures outlined in these Guidelines, the financial institution shall not open the account, commence business relations or perform the transaction and should consider making a suspicious transaction report.

4.121 Shell Banks

4.122 Shell banks are defined as financial institutions that do not have physical presence in any country. FIs shall not enter into, or continue a correspondent banking relationship with shell banks. FIs shall protect against establishing relations with respondent foreign FIs that allow their accounts to be used by shell banks.

4.123 Correspondent banking

4.124 Correspondent Banking/Insurance

4.125 Correspondent banking is the provision of banking service by one bank (correspondent) to another bank (respondent), this can be between local banks (commercial banks and Micro-finance banks) or they can be between banks in different jurisdictions usually with the (respondent) bank domiciled overseas. Such correspondent bank faces additional ML/TF risks; this is because it has no relationship with the customers of the respondent bank.

4.126 The decision to engage in a correspondent/respondent relationship between two institutions should be based on each institutions ML/TF risk assessment of the other. Particularly, as it relates to the measures each institutions has put in place for the prevention, detection, control systems and the quality of the other's AML/CFT regulatory and supervisory regime.

4.127 Financial institutions should not enter into any such relationships or continue with any such respondent or correspondent relationship with shell financial institutions.

4.128 Senior management approval should be obtained before going into any new

correspondent relationships. Such relationships should be entered only after a careful assessment and review of the other institution based on a risk-based assessment and after making provisions for such the risks identified and a conduct of a complete due diligence on the other financial institution.

4.129 Correspondent institutions are required to ensure that all CDD measures are conducted by the respondent institutions when the services of "payable through" accounts are involved, and that the respondent institutions can avail the correspondent any information relating to any of its customer that uses the payable through account when required by the correspondent.

4.130 Respondent institutions should provide the following to the correspondent institution should they request for them when the need arises;

i. Information on the ownership, board and senior management;

ii. Assessment of the risk profile of the respondent institution. Financial institutions should consider the location and nature of business, major business activities of the respondent and determine from and determine from publicly available information the reputation of the respondent;

iii. Correspondent institutions are required to satisfy themselves with the adequacy of the respondent's AML/CFT program;

iv. Confirmation that the respondent does not maintain business relations with shell banks;

v. Assessment of the quality and level of the supervision and regulatory conduct in the respondent's country, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; and

vi. Evidence of senior management's approval before establishing the relationship.

vii. Financial institutions should monitor transactions conducted through correspondent relationships according to the risk they perceive of the other party. Where the respondent bank or counterparty is not regulated by a country with equivalent or higher AML/CFT standards of regulations, additional due diligence should be carried out.

viii. Financial institutions should undertake a more detail CDD and understanding of the counterparty when the risk level of engaging with the counter-party is perceived to be high.

ix. FIs shall obtain approval from senior management before establishing new correspondent relationship.

5.0 GUIDELINE V-WIRE TRANSFERS

5.1 The purpose of guideline VI is to ensure that the financial institutions and money transfer organisations are not exploited as conduit for transfer of funds to facilitate the financing of terrorist acts, terrorist orgnisations and individual terrorists, even if the funds are not used for a specific terrorist act(s). Thus the FIs are required to collect adequate information on all parties to the wire transfers. The wire transfers are refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person or not. The wire transfers include

both cross border and domestic transfers.

5.2 All FIs are required to record on all wire transfer instructions, regardless of the amount involved, the name of the originator, the name of the beneficiary, the account number for each, or a unique transaction reference number.

5.3 Information required for wire transfers

5.4 The FIs should ensure that all wire transfers (i.e. domestic and cross-border) include the following information:

i. Name of the originator
ii. Originator account number where such an account is used to process the transaction
iii. Originator's address, or national identity number, or customer identification number, or date and place of birth
iv. Name of the beneficiary
v. Beneficiary account number where such an account is used to process the transaction
vi. Purpose of the transfers
vii. Banks/financial institutions involve in the transactions
viii. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

5.5 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraphs 5.4 in respect of originator information, provided that they include the originator's account number or unique transaction reference and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

5.6 Ordering financial institution

5.7 The ordering financial institution should ensure that all wire transfers contain required and accurate originator information, and required beneficiary information. The ordering financial institution should maintain all originator and beneficiary information collected. The ordering financial institution should not execute the wire transfer if it does not comply with the requirements specified in paragraph 5.4.

5.8 Intermediary financial institution

5.9 For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

5.10 An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information and consider filing STRs should it is unable to get the required information or in case of suspicion raise from the circumstances of the wire transfers.

5.11 An intermediary financial institution should have effective risk-based policies and procedures for determining:

i. when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

ii. the appropriate follow-up action, which include filing STR to FIU

5.12 Beneficiary financial institution

5.13 A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

5.14 For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified. A beneficiary financial institution should also have effective risk-based policies and procedures for determining:

i. when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
ii. the appropriate follow-up action, which include filing STR to FIU

5.15 Obligation on money or value transfer service operators

5.16 Money or value transfer service (MVTS) providers are required to comply with all of the relevant requirements in paragraphs 5.9 to 5.14 In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider should take into account all the information from both the ordering and beneficiary sides.

5.17 Exemptions on wire transfers

5.18 The requirements under this guideline do not extent in the following transactions:

i. Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, the requirements applies to a credit or debit or prepaid card transaction used as a payment system to effect a person-to-person wire transfer.

ii. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

5.19 Implementation of UN Security Council Resolutions and wire transfers

5.20 All financial institutions are prohibited from conducting transactions for or on behalf of individuals and entities designed by the UN Security Council Resolutions on terrorism, terrorist financing, proliferation of weapons of mass destruction and other subsequent resolutions or other sanction regimes of the UN. All cross-border wire transfers should be checked against the UN Designated Persons List and where there is a match, the FI should immediately freeze the transaction(s) and/or fund(s) and immediately file STR to the FIU. The freezing of the funds and filing of the STR should be done not more than 24 hours from the point of discovering the match.

5.21 The FIs are required tocheck all wire transfers against terrorist designations of other countries and file STR to the FIU where a match is found.

6.0 GUIDELINE VI: REPORTING OF SUSPICIOUS TRANSACTIONS TO THE FINANCIAL INTELLIGENCE UNIT

6.1 obligation to file STR and other reports

6.2 The financial institutions are required to file Suspicious Transaction Reports (STRs), Cash Transaction Reports, Foreign Wire Transfer Reports and other reports to the FIU. These reports are necessary in the fight against money laundering, terrorist financing and other related crimes in The Gambia.

6.3 Filing STRs to the FIU

6.4 In reporting STR to the FIU the financial institutions are obliged to comply with the guidance notes indicated below.

6.5 PART I

6.6 Introduction

6.7 This Guidance Note is intended to provide assistance to Financial Institutions and Designated Non-Financial Businesses and Professions (DNFPBs) known as Reporting Entities in meeting their obligations to make a Suspicious Transaction (STR) to the Financial Intelligence Unit (the FIU). These obligations are imposed under section 33 of Anti-Money Laundering and Combating Terrorist Financing (AML/CTF) 2012. This Guidance Note includes information on who must file, when to file, how to complete the STR form set out in the Appendix and the procedure for submission to the FIU.

6.8 STRs play a crucial role in the fight against money laundering and terrorism financing and the FIU is committed to ensuring that Reporting Entities in The Gambia file STRs of the highest quality. The Guidance Note should be read together with the AML/CTF Act 2012 and National Regulations on Terrorist Financing.

6.9 PART II

6.10 Reporting entities' obligations under the AML/CTF Act 2012

6.11 Who is required to report a Money Laundering or Financing of Terrorism transaction or activity? Section 33 of the AML/CTF Act 2012 requires that Reporting Entities send Suspicious Transaction Report (STR) to the FIU when they have:

a. Reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of a criminal conduct, money laundering or financing of terrorism;

b. Information that may be relevant to:
   (i) An act preparatory to an offence of the financing of terrorism, or

   (ii) An investigation or prosecution of any person or for a criminal

conduct, a money laundering or financing of terrorism offence; or may otherwise be assistance in the enforcement of the AML/CTF Act 2012

6.12 Reporting entities include the following:

(a) Financial Institutions:

a. Banks licensed by the Central Bank of The Gambia

b. Micro-Financial Institutions licensed by the Central Bank of The Gambia

c. Insurance Companies licensed by the Central Bank of The Gambia

d. Foreign Exchange Bureaus licensed by the Central Bank of The Gambia and Money Transfer Operation

e. Designated Non-Financial Businesses and Professions which include:

i. Casinos (including internet casinos);
ii. Lawyers Notaries and other independent legal professionals;
iii. Accountants when they prepare for or carry out transactions for their clients concerning:
(a) The buying and selling of real estates,
(b) The managing of client money, securities or other assets,
(c) The managing of bank, savings or securities accounts,
(d) The organization of contributions for the creation of, operation or management of companies, or
(e) The creation, operation or management of legal persons or arrangement and buying and selling of business entities;
iv. Real estate agents;
v. Dealers in precious metals;
vi. Dealers in precious stones; and
vii. Trust and company service providers.

6.13 PART III

6.14 Time to submit a STRto the FIU

6.15 A Suspicious Transaction Report must be sent to the FIU as soon as practicable but no later than three working days on which the Reporting Entity's personnel (the Compliance Officer) knew or formed the suspicion that:

a. A transaction or attempted transaction may be related to the commission of a criminal conduct, money laundering or financing of terrorism;
b. An Information may be relevant to:

i. An act preparatory to an offence of the financing of terrorism, or

ii. An investigation or prosecution of any person or for a criminal conduct, a money laundering or financing of terrorism offence; or may otherwise be assistance in the enforcement of the AML/CTF Act 2012

6.16 Reporting entities should ensure that their internal systems support the timely filing of STRs and avoid unnecessary delay.

6.17 PART IV

6.18 Whatis a suspicious transaction/activity

6.19 Suspicion of money laundering, terrorism financing or criminal conduct requires a degree of satisfaction that may not amount to belief, but should extend beyond mere speculation and be based on some foundation that money laundering terrorist financing or criminal conduct has occurred or is about to occur.

6.20 Suspicion involves a personal and subjective assessment. Reporting Entities have to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence a financing of terrorism offence or offence of criminal conduct.

6.21 In this regard, Reporting entities are required to pay special attention to:

i. Business transactions with individuals, corporate persons and financial institutions in or from other countries, which do not or insufficiently comply with the recommendations of the Financial Action Task Force;

ii. A transaction which is complex, unusual or large, whether completed or not;

iii. Unusual patterns of transactions; and

iv. Insignificant but periodic transactions which have no apparent or visible lawful purpose.

6.22 A transaction includes:

i. The receiving or making of a gift. The sum of money involved in the transaction is irrelevant. There is no monetary threshold for making a report of a suspicious transaction;

ii. A one-off transaction. This means any transaction other than one carried out in the course of an existing business relationship;

iii. Two or more one-off transactions which appear to be linked;

iv. A transaction which is attempted i.e. which is not completed.

v. Reporting Entities may become suspicious because the customer activity deviates from the normal activity for that customer, business or sector. Reporting Entities must therefore understand what the normal activity is for each customer and how this transaction differs from that.

vi. When considering making a suspicious transaction report, the Reporting Entities should consider all the circumstances of the transaction. Relevant factors include your knowledge of the customer's business, financial history, background and behavior. As a general principle, any transaction that causes a reporting entity to have a feeling of apprehension or mistrust about the transaction should be closely examined and the entity should consider filing a STR.

vii. Finally, Reporting Entities should bring together all the relevant factors. Some factors may seem individually insignificant, but taken together may raise the suspicion of money laundering, the financing of terrorism or a criminal conduct.

6.23 Distinction between knowledge and suspicion

6.24 Having knowledge means actually knowing something to be true and can be

inferred from surrounding circumstances. Suspicion of money laundering, terrorist financing and other criminal conducts on the other hand, requires a degree of satisfaction that may not amount to belief, but should extend beyond mere speculation and be based on some foundation that money laundering terrorist financing and other criminal conduct has occurred or is about to occur.

6.25 In the case of either knowledge or suspicion, a STR shall be filed with the FIU.

6.26 PART V

6.27 How to identify a suspicious transaction or suspicious activity

6.28 The Red Flags below are some general indicators, which may be helpful in identifying a suspicious transaction/activity. The presence of one or more of these indicators does not necessarily mean that a Money Laundering Terrorist Financing or criminal conduct is in fact taking place. The Reporting Entity, upon the examination of the Transaction, must build its conclusions on an objective basis and consider carefully all related conditions and evidence.

6.29 Red Flags, which point to a transaction being related to the Financing of Terrorism, are similar to those relating to money laundering. In fact, it is possible that a transaction could be related to both. For example, funds to be used for terrorist activity could be the proceeds of criminal activity as well as from legitimate sources. 6.30 Red Flags pointing to Financing of Terrorism

6.31 Behavioral Indicators:

a. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations;
b. Use of false corporations, including shell-companies;
c. Inclusion of the individual or entity in the United Nations 1267 Sanctions list;
d. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities;
e. Beneficial owner of the account not properly identified.
f. Use of nominees, trusts, family members or third party accounts;
g. Use of false identification;

6.32 Indicators linked to the financial transactions:

a. The use of funds by the non-profit organization is not consistent with the purpose for which it was established;
b. The transaction is not economically justified considering the account holder's business or profession;
c. A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds;
d. Transactions which are inconsistent with the account's normal activity;
e. Deposits were structured below the reporting requirements to avoid detection;
f. Multiple cash deposits and withdrawals with suspicious references;
g. Frequent domestic and international ATM activity;
h. No business rationale or economic justification for the transaction;
i. Unusual cash activity in foreign bank accounts;
j. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country;
k. Use of multiple, foreign bank accounts.

6.33 Red Flags pointing to Money Laundering

a. The client cannot provide satisfactory evidence of identity;
b. Situations where it is very difficult to verify customer information;
c. Situations where the source of funds cannot be easily verified;
d. Transactions in countries in which the parties are non-residents and their only purpose is a capital investment (they are not interested in living at the property they are buying);
e. Frequent change of ownership of same property in unusually short periods with no apparent business, economic or other legitimate reason and between related persons.
f. Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
g. Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
h. The client sets up shell companies with nominee shareholders and/or directors.
i. Client repeatedly changes Attorneys within a short period without any reasonable explanation.
j. Client purchases property in names of other persons or uses different names on offers to purchase, closing documents and deposit receipts.
k. Client deposits a large amount of cash with you to make payments which are

outside of the client's profile.

l. Client negotiates a purchase but wants to record a lower value on documents, paying the difference "under the table", (inadequate consideration).
m. An intermediary who has no apparent reason to be involved provides client's documents such as identification, statement of income or employment details, (the intermediary may be the real client).
n. Client gives power of attorney to a non-relative to conduct large transactions (same as above).
o. Transaction involves legal entities and there is no relationship seen between the transaction and the business activity of the buying company, or the company has no business activity.
p. Client requests the firm to act as his agent in obtaining high sum bankers' drafts, cashiers' cheques and other cash equivalent or near cash monetary instruments or in making wire transfers to and from other banks or financial institutions, (anonymity).
q. Divergence from the type, volume or frequency of transactions expected in the course of the business relationship

6.34 Impact on the Business Relationship/Transaction after Forming a Suspicion

6.35 The law does not require a Reporting Entity who has filed a STR to end or terminate their financial relationships with the reported individual or entity except in the two (2) following circumstances:

a. Where satisfactory evidence of identity has not been obtained; or
b. Where a designated or listed entity attempts to enter into a transaction or continue the business relationship.

6.36 In all other cases, Reporting Entities should be aware that the decision to continue the business relationship after filing a STR, should be based on commercial or risk containment reasons. However, a decision to terminate the business relationship must also ensure that the customer is not alerted to the filing of the STR, which would constitute the offence of tipping off.

6.37 PART VI: How to make a suspicious transaction report

6.38 The prescribed STR form to be used by Reporting Entities is as provided in the ANNEX 1 of this guideline, which is the same as the one earlier sent to the Reporting Entities.

6.39 It is essential that Reporting Entities complete all relevant fields in the form with accurate information.

6.40 Contents of the STR

6.41 The value of an STR depends on the quality of information it contains. An STR should set out in a clear manner the basis for knowledge or suspicion of Money Laundering, Financing of Terrorism or any criminal conduct.

6.42 Reporting Entities should include as much relevant information about the customer, transaction or activity that it has available from its records.

6.43 In Part V of the STR form, on "Suspicious Activity Information/explanation/description", a detailed explanation as to why the Reporting Entity is filing a suspicious transaction report should be clearly given.

6.44 The information about the transaction and what led to your suspicion is important in completing the STR. Provide as many details as possible including anything that made you suspect that it might be related to Money Laundering, Financing of Terrorism, any criminal conduct, both or all. It is not critical for the Reporting Entity to determine whether the offence is one or the other, it is the information about your suspicion that is important not the distinction between the offences.

6.45 Supporting documents

6.46 You are required to enclose copies of all the necessary documents facilitating the transaction and identifying the party or parties to the transaction.

6.47 NOTE: THE STR IS TO BE COMPLETED BY THE COMPLIANCE OFFICER WITHOUT THE KNOWLEDGE OF THE CUSTOMER BEING REPORTED. IT MUST NOT BE COMPLETED IN THE PRESENCE OF THE CUSTOMER. THE CUSTOMER OR ANY OTHER STAFF OF THE REPORTING ENTITY WHO HAS NO INPUT IN THE STR MUST NOT BE TOLD THAT AN STR WOULD BE MADE OR HAS BEEN MADE TO THE FIU.

6.48 STR Submission to the FIU

6.48 STRs must be reported, by the following method until for now:

6.49 Hand delivered in a SEALED envelope and stamped "CONFIDENTIAL" and addressed to:

The Director
Financial Intelligence Unit
380 Senegambia Highway
Kerr Serign
West Coast Region
The Gambia

6.50 However, the FIU may with time and if the need arise specify additional methods to be used for submitting STRs by notification in writing to the Reporting Entities.

6.51 The Reporting Entity may, in limited circumstances, make a STR via telephone [(220) 4466839 or 4466840] where the Reporting Entity believes the immediate attention of the FIU is required i.e. urgent cases. Such urgency could arise:

a. Where a Reporting Entity's impression of a transaction has gone beyond suspicion and amounts to knowledge or belief that the transaction involves money laundering, financing of terrorism or criminal conduct;
b. Where there is belief of an imminent crime; or
c. To avoid flight of assets out of The Gambia which may be irrecoverable.

6.52 In each case that an oral report is made it should be followed as soon as practicable by a written report.

6.53 FIU Procedures upon the Receipt of an STR

6.54 Upon the receipt of a STR/SAR, the FIU will provide feedback in form of a written acknowledgement letter to the Reporting Entity's Compliance Officer within three(3) working days from the day received. The FIU may also require a Reporting Entity to produce specific information that the FIU may reasonably require to conduct its analysis. Reporting Entities should be cooperative in this regard.

6.55 The FIU will also provide further written feedback on the STR that:

a. An intelligence report was sent to the Law Enforcement Agency (LEA) for investigation;
b. The LEA has advised that the investigation has been closed;
c. The STR has been filed for intelligence purposes; or

d. The suspect has been charged/convicted of an offence.

6.56 PART VII: How to complete the STR form

6.57 This guidance is provided to assist Reporting Entities in preparing the STR reporting form.

6.58 General Guidelines

6.59 All fields on the STR form should be filled out. No field is to be left blank. Insert the letters "N/A" (not applicable) where information requested does not relate to your reporting.

6.61 The space marked "Report No." at the top right hand corner of the STR form is for the Reporting Entity's unique identifier given to each STR submitted to the FIU. All reports to the FIU should be sequentially numbered and that number written in this space.

6.62 Dates – Dates should be entered using the format "dd/mm/yy," where "dd" is the day, "mm" is the month and "yy" is the year. Zero (0) should precede any single digit number. If the month or day is not available or unknown, enter zeros in the space for "mm" and "dd." For example, 00/01/15 indicates an unknown day in January 2015.

6.63 Numbers – Monetary amounts should be entered using the format "$0,000,000". All amounts should be reported in currency in which the transaction was conducted in (GMD, USD, £, €, ¥, etc.).

6.64 PART 1- Information on reporting institution/person

6.65 Item 1- Which type of reporting person or entity best describes you – Tick against the most appropriate reporting entity or person that best describes your status.

6.66 Item 2- Name of the Reporting Institution or Person– You should clearly enter the full legal (Trade) name of the Reporting Institution or Person.

6.67 Item 3- Full Address of Reporting Institution or Person – Enter the full address of the Reporting Entity or Person.

6.68 Items 4 and 5- Telephone Number and email address – Enter the a phone number,

(either official or cell phone) on which the contact person can be reached. Also, enter a reliable email address of the contact person in the space provided in item 5.

6.69 Item 6- Supervised by (if applicable) – Specify the supervisory authority under whose supervision the reporting institution is operating.

6.70 Item 7- Full name of contact and telephone – Enter the name of the person who prepared the information and telephone number where the preparer can be easily reached. It would be extremely helpful if individual identified in this section has specific knowledge of the underlying facts.

6.71 Item 8-Name and Title of reporting officer – Enter the position in the reporting entity held by the preparer. In addition, the preparer must sign and enter date of signature in the space provided in 8.1 and 8.2 respectively.

6.72 PART 2 – Identification of party or parties to the transaction

6.73 Item 9, 10 and 11 – Name of individual or Entity;

a. If the suspicious activity involves an individual, enter his or her last name or surname in Item 9, first name in Item 10 and middle initial in Item 11. If there is no middle initial, enter "N/A" in Item 11.

b. If the suspicious activity involves an organization (entity), enter its name in Item 9 and enter "N/A" in Items 10 and 11.
c. If the reporting entity has knowledge o f a separate "trading as" name, in the Narrative, also enter the individual or organization's name, followed by the phrase "T/ A." and the name of the business in Item 9. For example, Kekuta Totala T/A as Alaa Indeh Enterprise.

6.74 Item 12- Individual's Identity (enclose copy or copies) Check appropriate box of identification provided by the suspect(s) and enclose copy or copies of the identification documents.

6.75 Item 13- Full Address- Enter permanent address of the person identified in items 9, 10, and 11. If the individual is from foreign country, enter both foreign country address as well as the local address.

6.76 Item 14- Nationality- Enter the nationality of the suspect in the space provided.

6.77 Item 15- Phone number(s)- Enter the correct phone number(s) of the suspect space provided. If it is a legal entity, enter the both the office phone and personal numbers.

6.78 Item 16- Date of Birth- If an individual is named in items 9 to 11, enter his/her date of birth using the method for entering dates described in part VII [dd/mm/yy].

6.79 Item 17- individual's occupation or type of business- Fully identify the occupation, profession or business of the person on whose behalf the transaction(s) was conducted. For example, secretary, carpenter, attorney, housewife, restaurant owner, textile store clerk, etc. Avoid using non-specific terms such as merchant, self-employed, businessman, etc.

6.80 Item 18 – Date of Incorporation- If an entity or organization is named in item 9 to 1,1enter the date of incorporation using for entering date described in part VII [dd/mm/yy].

6.81 Item 19- Business Registration Number- If an entity or organization is named in items 9 to11, enter the business registration number as provided in the business registration certificate from the Registrar of Companies.

6.82 Item 20- Relationship to the reporting institution – Enter the type of relationship existing between the suspect and the reporting institution. For example, customer, employee business partner, etc.

6.83 Items 21and 22- Is the relationship an insider relationship – Check against the appropriate option that identifies the suspects relationship with the reporting institution.

6.84 Item 23- Date of Suspension / Termination / Resignation- Enter the date of either the suspension, termination or resignation of the suspect using the date description in part VII [dd/mm/yy].

6.85 PART 3- Transaction details & suspicion

6.86 Item 24- Date of Transaction- nter the first known date of suspicious transaction using the date description in part VII [dd/mm/yy]. If multiple or related activity is conducted by the suspect during the reporting period, the reporting institution or entity may report all activity on one STR form. Enter the date of the initial activity

and the last occurrence date in Part 6 of the form. The first known date is a mandatory field.

6.87 Item 25- Date posting if different from date of transaction- Enter the date of posting of the funds into suspect account if different from the date of the suspicious transaction using the date description in part VII [dd/mm/yy].

6.88 Item 26- Funds involved in the transaction- Check against the most appropriate option that identifies the type of funds involved in the suspicious transaction being reported.

6.89 Item 27-Amount involved in the transaction- Enter the total amount involved in the suspicious activity. An aggregated total of all transactions for multiple or related suspicious activities by the same individual or organization within the same reporting period may be shown in this field. The breakdown of this total may then be listed in Part 5.

6.90 Item 28- Type of Account- State clearly the type of account(s) the suspect is operating. For example personal current account, personal savings account, corporate current account, corporate savings account, etc.

6.91 Item 29- Bank Account Details- Enter the account number(s) that were affected by the suspicious activity. If more than one account is affected, provide the additional account numbers in Part 5. If no account is affected, enter "N/A.".

6.92 Item 30- Status of the account at the time the transaction was initiated (if applicable) – For each account listed in item, 29 indicate whether the account is still open or has been closed and the date of closure if closed.

6.93 Item 31- Reason for suspicion (complete part 5 as well)- State in brief the reason for suspicion in section and provide a detailed description in part 5.

6.94 Item 32 - Has the suspicious activity had a material impact on, or otherwise affected, the financial soundness of the institution or person – indicate by ticking against the appropriate option the impact of the suspicious activity or transaction on the reporting institution or any other person.

6.95 PART 4 – Name of all officers, employers or agents dealing with the transaction

6.96 Item 33 and 33.1- Contact for assistance- Enter the name of the person who can be contacted for additional information. It would be extremely helpful if the individual identified in this section has specific knowledge of the underlying facts.

6.97 Item 33.2 and 33.3- Enter the contact person's title or occupation in the reporting entity and a reliable phone number the contact person can be easily reached.

6.98 PART 5- Description of suspicious activity

6.99 Item 34- Description of suspicious activity- Describe clearly and completely the facts or unusual circumstances that led to the suspicion of money laundering, terrorist financing or any criminal conducts. The care with which this section is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood.

6.100 Provide a complete chronological account of what is unusual, irregular or suspicious about the transaction. You should also include materials or any other information that you believe is necessary to better enable the FIU to understand the transaction you are reporting. If necessary, continue the narrative on a copy of this page of the STR.

6.101 Remember that any supporting documentation such as spreadsheets, photocopies of cancelled checks or other documents, surveillance photos, etc., must be retained at the financial institution for a period of 5 years as indicated in Section 27 of the AML/CTF Act 2012.

6.102 PART 6- Description of action taken

6.103 Item 35- Description of action taken- Please describe what action was or will be taken by you as a result of the suspicious transaction(s). State also whether the suspect made any voluntary statement as to the origin or source of the proceeds. Kindly enclose copy of the statement, if any.

6.104 Part 7- Additional information relating to STR submitted to the FIU

6.105 Request for further information

6.106 The Director, in the exercise of his/her powers under AML/CTF Act 2012 may, having regard to the intricacy of a case make a request for additional information from

the Entity that filed the suspicious transaction report or from any other Reporting Entity in order to facilitate the analysis process

6.107 Tipping Off/ Confidentiality

6.108 Upon filing a suspicious transaction report to the FIU, a Reporting Entity is not allowed to inform anyone, including the client/customer, about the contents of a STR or even that you have made such a report. It is an offence under Sections 34 and 35 of the AML/CTF Act 2012. In addition, officials of the reporting entity should be wary of requesting any information that you would not normally request during a normal transaction which may alert your client that you are making a suspicious transaction report.

6.109 Immunity

6.110 A reporting entity, its directors, officers, partners or employees who submit reports or provide information in accordance with the AML/CTF Act and in good faith shall not be liable to criminal, civil, disciplinary or administrative proceedings for breach of any restriction on disclosure of information imposed by contract or any legislative, regulatory or administrative provision, regardless of the result of the report. This protection also extends to information provided voluntarily to FIU because of your suspicions of money laundering, terrorism financing or any criminal conducts.

6.111 For feedback on or clarification about this Guidance Note contact:

The Director
Financial Intelligence Unit
380 Senegambia Highway
Kerr Serign
West Coast Region
The GambiaTel: +220 4466839 or 4466840

7.0 GUIDELINE VII: RECORD KEEPING REQUIREMENT

7.1 Record-keeping

7.2 Financial institution should establish a document retention policy that provides for the maintenance of records, including those related to customer identification, business transactions, internal and external reporting and training, this will go a long way to

show its commitment to compliance with the AML/CFT ACT, 2012 and will further ease and facilitate investigations (for intelligence purpose only) undertaken by the FIU and law enforcement agents.

7.3 Transaction Records

7.4 Financial institution should retain all business transactions records for a minimum of five years. This should be done after the completion of the business transaction or in termination of the business relationship under whatever circumstance. However, financial institution may wish to retain records beyond the stipulated period until such a time it no longer needs it or when advised by the FIU or other competent authority. This can be done in the following circumstances;

i. There has been a report of a suspicious activity; or
ii. There is an on-going investigation relating to a transaction or client.

7.5 Financial institutions should at least establish a financial profile and audit trail of transactions and other information which should include the following;

i. The name, address, occupation of the beneficial owner of an account and, where appropriate, principal activity of each person conducting the transaction or on whose behalf the transaction is being conducted;

ii. The volume of funds passing through the account or business relationship in question;

iii. The nature of the business relationship or transaction;

iv. The transaction date for transactions or date of activity for actions deem to be suspicious;

v. Details of the transaction which should include; the amount involve in the transaction, the source and destination of the funds , type of instruments used, and type and denomination of currency used where applicable;

vi. The form of instruction and authority for instruction;

vii. Details of the parties to the transaction; and

viii. Where applicable, the product/service through which the transaction was conducted and any other products/services directly involved in the transaction.

7.6 Verification of Identity Records

7.7 Just as transaction records and other details of the business relationship are to be retained for a period of five years, verification of identity of customers must also be retail for the same period whether for individual or natural customers notwithstanding the nature of the business relationship. Furthermore, this should be from the date the person ceases to be a customer or after the verification was carried out, whichever is the later.

7.8 The date when a person ceases to be a customer by this Guidelines should be the date when:

i. One-off transaction occurred or where series of transactions occurs, the date of the last transaction on the series;

ii. A business relationship is severed; or

iii. Proceedings commence in a debt recovery process at insolvency.

iv. When formalities to severe business relationship has not happen and five years has elapsed from the date of the last transaction on the business relationship, then the retention period should take effect from date of the completion of the last transaction.

v. Where a financial institution is liquidated and finally dissolved, the relevant identification, verification and transaction records must be retained by the liquidator or the financial institution for the balance of the prescribed period remaining at the date of dissolution.

7.9 Credit/debit slips, cheques and other forms of instruments used in the transactions or any business relationship records should be retained in a format, whether hard copy, electronic, scanned or microfilm, or any format that should be admissible in court and which would facilitate reconstruction of individual transactions so as to provide, where necessary, evidence for investigations and prosecution of criminal activity and to enable quick access of information in response to requests from the FIU or other law enforcement agencies.

7.10 Financial institutions should prioritize records to be retained as some records can be retained for a long period of time and in some cases almost indefinitely. Records should be retained in a way that they can be retrieved without undue delay when requested.

7.11 When there is a merger or take-over between financial institutions or entities, financial institutions should ensure that all records described can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than a financial institution, the financial institution should endeavor to retrieve those records before the end of the contractual arrangement. The nature of records that should be retained is set out below.

7.12 Customer Records

7.13 In order to comply with Part V of the AML/CFT ACT, 2012, a financial institution should retain:

a. Copies or records of customer identification, including those obtained through the conduct of enhanced due diligence;
b. Account files, account statements and business correspondence; and
c. All business transaction records.
d. All records related to unusual and suspicious transaction reports should be maintain by financial institutions. These should include:

e. All reports made by staff to the Chief Compliance Officer;
f. The internal written findings of unusual transactions investigated. This applies irrespective of whether a suspicious report was made;
g. Consideration of those reports and of any action taken; and

h. All quarterly or annual reports made by the Chief Compliance Officer to senior management and the board of directors.

i. Training Records

7.14 Financial institution should at a minimum, maintain the following information so as to show proof of compliance with part VI, Section 43,:

a. Details and contents of training programs provided to staff members;

b. Names of staff receiving the training;

c. Dates that training sessions were held;

d. Test results carried out to measure staff understanding of money laundering and terrorist financing requirements; and

e. The financial institutions own training plan

8.0 GUIDELINE VIII: FILING OF OTHER REPORTS

8.1 Cash Transaction Reports (CTRs)

8.2 The financial institutions are required to file CTRs to the FIU as and when they occur. The CTRs shall be filed to the FIU on or before close of business of every Friday of the Week. Cash Transaction is any cash withdrawal(s) or deposit(s) amounting to a specific threshold. The threshold for individuals, enterprises, sole proprietorship or partnership business or any unincorporated business is

D450,000 (Four Hundred and Fifty Thousand Dalasi) or its equivalent in any other currency. The threshold for companies, corporations is D2,000,000 (Two Million Dalasi) or its equivalent in any other currency. Where the customer appear to structure transactions to avoid CTRs reporting requirements such transactions shall be reported as CTRs as soon as the structured transactions amounts to the threshold.

8.3 The CTRs shall be filed in prescribed CTR form provided in ANNEX II.

8.4 The failure to file CTR shall tract a penalty of D1,000 (one thousand Dalasi) per day per transaction from the date the transaction occur.

8.5 Foreign Wire Transfer Reports (FWTRs)

8.6 The financial institutions are required to file FWTRs to the FIU on or before close of business every Friday of every week. The foreign wire transfers are any transfer of funds outside the jurisdiction of The Gambia. The payments are made through funds transfers to beneficiaries outside The Gambia. The threshold for reporting FWTRs for individuals, enterprises, sole proprietorship, partnership and other unincorporated businesses is USD15,0000 (fifteen thousand United States Dollars) or its equivalence in any currency and for companies and corporations the threshold is USD50,000 (fifty thousand United States Dollars) or its equivalence in any currency.

8.7 Where the customer conducts transactions which seem to avoid FWTRs requirements, the financial institution is required to file a report as soon as the related transactions add up to the threshold.

8.8 The failure to file FWTR shall attract a penalty of D1,000 (one thousand Dalasi) per day for each transaction from the day transaction occur.

8.9 The FWTRs shall be filed in prescribed FWTRs form provided in ANNEX III

ANNEXES

Annex I	:	Suspicious transaction reports form
Annex I	:	Cash transaction reports form
Annex III	:	Foreign Wire Transfer Reports form