



FINANCIAL INTELLIGENCE UNIT OF THE GAMBIA

ANTI-MONEY LAUNDERING AND COMBATING TERRORIST FINANCING GUIDELINES FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPs)

AML/CTF guidelines of DNFBPs 2016
FIU The Gambia



AFRICAN DEVELOPMENT BANK GROUP
GROUPE DE LA BANQUE AFRICAINE
DE DEVELOPPEMENT

Table of Contents

ABBREVIATIONS	3
GENERAL INTRODUCTION	4
1.1 FIGHT AGAINST CRIMES	4
1.2 SCOPE	5
1.3 APPLICATION	5
1.4 MONEY LAUNDERING DEFINITION	6
1.5 STAGES OF MONEY LAUNDERING	6
1.6 IMPORTANCE OF COMBATING MONEY LAUNDERING	8
1.7 INTERNATIONAL EFFORTS TO COMBAT MONEY LAUNDERING	8
1.8 OFFENCE OF MONEY LAUNDERING	9
1.9 TERRORISM FINANCING	10
1.10 OFFENCE OF TERRORISM FINANCING	10
1.11 REVENUE GENERATING ACTIVITIES	11
1.12 LAUNDERING OF TERRORIST-RELATED FUNDS	11
1.13 STAGES OF TERRORISM FINANCING	12
1.14 IMPORTANCE OF COMBATING TERRORIST FINANCING	12
1.15 INTERNATIONAL EFFORTS TO COMBAT TERRORIST FINANCING	12
1.16 IMPLEMENTING ROBUST AML/CFT REGIME	12
1.16.5 FINANCIAL INTELLIGENCE UNIT OF THE GAMBIA	14
1.17 OBJECTS OF THE FIU	14
1.18 THE ROLE OF THE FIU	15
1.19 REPORTING ENTITIES	16
2.0 MONEY LAUNDERING AND TERRORISM FINANCING (ML/TF) RISK ASSESSMENT AND ADOPTING RISK-BASED APPROACH	17
2.1 WHO IS REQUIRED TO ASSESS MONEY LAUNDERING AND TERRORISM FINANCING RISKS	17

3.0 CUSTOMER DUE DILIGENCE (CDD)	18
3.5.1: CLIENT IDENTIFICATION (NATURAL PERSON-GAMBIAN RESIDENT):	20
3.5.2: CLIENT IDENTIFICATION (NATURAL PERSON GAMBIAN RESIDENT ABROAD):	20
3.5.3: CLIENT IDENTIFICATION (NATURAL PERSON-FOREIGN RESIDENT)	21
3.5.4: CLIENT IDENTIFICATION (NATURAL PERSON-FOREIGN NON-RESIDENT):	21
3.5.5: CLIENT IDENTIFICATION (LEGAL ENTITIES)	22
3.6: VERIFICATION OF CLIENT IDENTITY (NATURAL PERSONS AND LEGAL ENTITIES)	22
4.0: AML/CTF COMPLIANCE REQUIREMENTS	24
4.1.0: RECORD KEEPING REQUIREMENTS	24
4.2.0: REPORTING REQUIREMENTS	25
4.3.0: TRAINING REQUIREMENTS	27
4.4.0: INTERNAL CONTROLS	28
4.5.0: APPOINTMENT OF A COMPLIANCE OFFICER	29
5.0: ENHANCED DUE DILIGENCE (EDD)	30
6.0: TIPPING OFF	31
7.0: PENALTIES FOR NON-COMPLIANCE	32
8.0: RISK ASSESSMENT	33
9.0: SUSPICIOUS TRANSACTION REPORTING	42
9.12.1: RED FLAGS POINTING TO FINANCING OF TERRORISM	46
9.12.2: RED FLAGS POINTING TO MONEY LAUNDERING	47
10.0 HOW TO COMPLETE THE STR/SAR FORM	51
10.1 GENERAL GUIDELINES	51
10.2 SPECIFIC GUIDELINES	52
PART 1 – INFORMATION ON REPORTING INSTITUTION/PERSON	52
PART 2 – IDENTIFICATION OF PARTY OR PARTIES TO THE TRANSACTION	53
PART 3 – TRANSACTION DETAILS & SUSPICION	54
PART 4 – NAME OF ALL OFFICERS, EMPLOYERS OR AGENTS DEALING WITH THE TRANSACTION	56
PART 5 – DESCRIPTION OF SUSPICIOUS ACTIVITY	56
PART 6 – DESCRIPTION OF ACTION TAKEN	57
PART 7 – ADDITIONAL INFORMATION RELATING TO STR/SAR SUBMITTED TO THE FIU	57

ABBREVIATIONS

AML	Anti-Money Laundering
AML/CTF	Anti-Money Laundering and Combating Terrorist Financing
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CTF	Combating of Terrorism Financing
CTR	Cash Transaction Reports
DNFBPs	Designated Non-Financial Business Professions
FATF	Financial Action Task Force
FI	Financial Institutions
FIU	Financial Intelligence Unit
FT	Financing of Terrorism
EDD	Enhanced Due Diligence
KYC	Know Your Customer
ML	Money Laundering
PEP	Politically Exposed Person
RE	Reporting Entities
SDD	Simplified Due Diligence
STR	Suspicious Transaction Reports
TF	Terrorism Financing

GENERAL INTRODUCTION

1.1 Fight against crimes

1.1.2 The fight against crimes especially money laundering, terrorism financing and other transnational crimes is no longer the business of the law enforcement agencies only. The private sector especially financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) are obliged to combat these crimes by designing and implementing adequate policies and internal operational procedures. 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 DNFBPs 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.

1.1.3 Money launderers, terrorist financiers and other types of criminals find it attractive to use the DNFBPs to perpetrate their criminal ventures undetected.

1.1.4 Towards this end, international response has been to enhance the capacity of the DNFBPs 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.

1.1.5 Being mindful of international standards and best practices, The Gambia Financial Intelligence Unit is issuing these guidelines to serve as a guide to all DNFBPs in the Gambia. The guidelines are aimed at providing DNFBPs with requisite knowledge, deeper interpretation and understanding of the requirements and DNFBPs' obligations under the Anti-Money Laundering and Combating of the Financing of Terrorism Act, 2012 (AML/CFT Act, 2012). While this is aimed at ensuring compliance to the AML/CFT Act, 2012 and its attendant legislations, it also enhances the AML/CFT regime of The Gambia in fulfilling the 40 Recommendations of Financial Action Task Force (FATF). It also serves as a standard reference document to DNFBPs in building the AML/CFT capacity of their compliance officer and the general staff of the institutions.

1.2 SCOPE

1.2.1 The Guideline lays down the expectations of the Financial Intelligence Unit of The Gambia and should be regarded as the minimum standards expected of all DNFBPs in The Gambia in developing their risk management strategies and a key component of the criteria of the DNFBPs evaluation of AML/CFT compliance.

1.2.1 This Guideline is drawn mainly from the revised Financial Action Task Force (FATF)¹ Forty Recommendations on Combating Money Laundering and Financing of Terrorism and Proliferation and best practice papers issued by the FATF and other international organizations including the World Bank and the International Monetary Fund (IMF).

¹ FATF is an Inter-governmental body which sets standards, develops and promotes policies to combat money laundering and terrorist financing.

Guidance was also obtained from the Basel Committee on Banking Supervision and inputs from the supervisory authorities of the Central Bank of the Gambia.

1.3 APPLICATION

1.3.1 All the different sets of DNFBPs operating in The Gambia are obligated to comply with this Guideline, 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 “shall”. DNFBPs should allocate adequate resources to mitigate money laundering, terrorism financing and other related financial crimes risks in their institutions. DNFBPs should also ensure that, at a minimum, the Guideline is implemented in their branches and subsidiaries abroad, where applicable. When implementation is outside 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 one in The Gambia. If the standards are on the other hand lower than the standards in The Gambia, DNFBPs should abide by the standards in The Gambia. Furthermore, they should inform FIU of The Gambia and their respective regulator if the local laws in the country of operation prohibit the implementation of this guideline as a whole or in part thereof.

1.4 Money Laundering Definition

1.4.1 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.

1.4.2 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.

1.5 Stages of Money Laundering

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:

- i. **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, DNFBPs or law enforcement agencies. 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 cheque from a cancelled 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.
- ii. **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 or involving one or more DNFBP.
- iii. **Integration:** This is the third stage of the Money Laundering process. It is where the illicit funds are reinvested in the legitimate 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 of integration schemes include the purchase and resale of real estate, investment securities, or other assets.

1.6 Importance of combating money laundering

1.6.1 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 from engaging in illegal activities, criminals use money laundering techniques to protect their illegally obtained wealth.

1.6.2 In the Gambia, though the quantum of laundered funds is not precisely known, it is believed that 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 civilized society.

1.6.3 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 committed 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.

1.7 International efforts to combat money laundering

1.7.1 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 has taken giant steps to help countries to fight against money laundering. One of the most important institutions 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.

1.7.2 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.

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

1.7.4 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 of 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 United Nations Conventions have come into 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.

1.8 Offence of money laundering

- 1.81 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.

1.9 Terrorism Financing

1.9.1 Terrorist financing is the provision of funds to facilitate terrorist activities. 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 major sources of funding. Other sources of terrorist funding include smuggling, fraud, theft, robbery, identity theft, use of diamonds and precious metals in conflict zones, 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.

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

1.9.3 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.

1.10 Offence of Terrorism Financing

- 1.10.1 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-

- a) an individual, including a director, employee or agent of a reporting entity, to imprisonment for a term of not less than ten years; or
- b) a body corporate to a fine of not less than Ten Million Dalasi.

1.11 Revenue generating activities

1.11.1 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.

1.11.2 Financing of 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.

1.12 Laundering of terrorist-related funds

1.12.1 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.

1.13 Stages of terrorism financing

1.13.1 The stages of terrorist 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 or any other activity that facilitates their operations.

1.14 Importance of combating terrorist financing

1.14.1 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 and terrorism financing.

1.14.2 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, combating terrorism financing will protect the financial system from abuse, but also maintain and improve the reputational and operational capacities of the DNFBPs, and promote vibrant institutions free from being used as conduits to commit crimes.

1.15 International efforts to combat terrorist financing

1.15.1 The FATF Recommendations 2015 are key in the fight against terrorism financing. The UN International Convention for the Suppression of International Financing of Terrorism, UN Security Council Resolutions 1267, 1373 and others, have laid down the global action to fight terrorism and terrorist financing. Regional bodies have also taken actions to curb these menaces.

1.16 Implementing robust AML/CFT Regime

1.16.1 The Gambia has enacted series of laws to strengthen its Anti-Money Laundering and Counter Terrorism Financing 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.

1.16.2 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 crime 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.

1.16.2 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 dealing with their customers/clients and other persons

1.16.3 The legal regime is intended to meet the following;

- i. Deter money laundering, terrorism financing and other economic and financial crimes
- ii. Detect illicit proceeds of crimes and freeze, seize and confiscate such proceeds
- iii. Impose obligations on third parties whose services may be used by launderers and terrorists financiers and other criminals
- iv. Protect the integrity of the financial and economic systems against abuse by criminals.

1.16.4 Relevant domestic laws to combat 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

1.16.5 Financial Intelligence Unit of The Gambia

1.16.5.1 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; tasked 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.

1.17 Objects of the FIU**1.17.1 The objects of the FIU are divided into three categories 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.

1.18 The role of the FIU

1.18.1 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;

- i. 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;
- ii. 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;
- iii. request information from reporting entities, any supervisory agency, self-regulatory organization and any law enforcement agency for purposes of this Act;
- iv. 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 this 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 this Act;
- 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 this Act;
- 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.

1.19 Reporting entities

1.19.1 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.

1.19.2 The reporting entities are provided in for Schedule I, PART II of the Anti-Money Laundering 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 MONEY LAUNDERING AND TERRORISM FINANCING (ML/TF) RISK ASSESSMENT AND ADOPTING RISK-BASED APPROACH

2.1 Who is required to assess money laundering and terrorism financing risks

All reporting entities including the DNFBPs are required to conduct counter money laundering and combating of terrorism financing risk assessment on annual basis and report result of their assessment to the Financial Intelligence Unit of The Gambia and their regulators. They are required to develop risk identification, prioritization, treatment, control and monitoring framework. The risk assessment should establish the likelihood (or chance) of the risk occurring and the severity or amount of loss or damage (or impact) which may result if they do occur.

2.2 The DNFBPs are required to develop and implement AML/CFT policies and internal controls and appropriate procedures taking into consideration the money laundering and terrorists financing risks.

2.3 The money laundering and terrorism financing risks are the probability that a reporting entity or its products and services could be exploited by criminals to perpetrate money laundering, terrorism financing and related financial crimes. In assessing money laundering and terrorism financing risks, the reporting entity should assess ML or TF risks for the following:

- i. Customer risks-this should include ML/TF risks in all categories of customers, including politically exposed persons (PEPs) and their associates
- ii. Product or service risks-the ML/TF risks in all types of products and services offered to customers and clients.
- iii. Delivery channel risks- this should include ML/TF risks when using various channels and methods in providing products and services to the customer and clients, for example, over-the-counter or online, wire transfers, etc.
- iv. Geographical location risk-this is the ML/TF risk arising from doing business in a geographic area; it should include both domestic and foreign jurisdictions where the reporting entity conducts business.

2.4 The ML/TF risk assessment must measure the level of risk (for example high, medium or low risk) for each of the risk categories (i.e. i, ii, iii & iv) stated above. This risk level determines the risk-based approach the DNFBP needs to adopt to establish robust AML/CFT programme.

2.5 The DNFBP's risk assessment framework must be flexible because the entity's risk profile may change. The reporting entity must also be able to identify and monitor significant changes in its ML/TF risks and amend its procedures accordingly.

2.6 The ML/TF risk assessment should also include ML/TF risks posed by the following:

- i. New products and services, before the entity introduces them to the market
- ii. New methods of delivering new products and services, before the entity adopts them
- iii. New or developing technologies used to provide products and services, before adopting them and
- iv. Changes in the nature of the business relationship, control structure or beneficial ownership of its customers.

2.7 A DNFBP's ML/TF risk assessment should be in writing and presented to senior management and the board of directors and should be updated and reviewed annually.

3.0 CUSTOMER DUE DILIGENCE (CDD)

3.1: Customer due diligence is the leading criteria in the efforts to preventing DNFBPs from being used by criminals in the commission of financial crimes including Money Laundering and Terrorism Financing. The DNFBPs' knowledge of their clients would enable them to apply such knowledge to transactions initiated by their client(s) and take adequate measures if there is a divergence between what the client claims to be and their actual activities.

3.2: In establishing relationships, maintaining existing relationships and in some instances in the case of one-off transactions above a designated threshold, all DNFBPs in delivering services to their clients are required to carry out the following;

- a. Identify and verify the identity of their clients. The responsibility lies on the DNFBP to know to a reasonable extent the types of client(s) they are dealing with and to satisfy itself to a reasonable degree that the client is what he/she/it claims to be;
- b. Identify beneficial owners by taking necessary steps to ensure that if a client is acting on behalf of another person (natural or legal) where the latter provides the funds or investments is to be held in the name of someone else, DNFBPs have the obligation to verify the identity of both the client and the agent/trustee unless the client is itself a self regulatory or regulated institution within The Gambia;
- c. Obtain additional information in an attempt to understand the client's business and circumstances. It is highly recommended to perform CDD at the point of entering a business relationship;
- d. Take special care in dealing with introduced businesses. The required and appropriate CDD measures must be taken in dealing with such customers;
- e. Conduct Enhanced Due Diligence (EDD) when there is suspicion of Money Laundering or Terrorism Financing, when a Politically Exposed Person (PEP) is involved or when there is high risk involved.

3.3: DNFBPs should not carry out or agree to carry out any business or provide advice to person (s) (legal or natural), unless it is certain to a reasonable extent about the identity of their clients.

3.4: Certain DNFBPs (3.4.1 and 3.4.2) below are required to take adequate Customer Due Diligence/ Know Your Customer (CDD/KYC) measures for transactions on or above a specified threshold. The appropriate CDD/KYC measures should be taken once a client engages in a financial transaction(s) or related transactions equal to or above the designated thresholds. Furthermore, extra care is required in dealing with clients who carry out series of transactions below the designated thresholds with the intention of avoiding a report being filed to the FIU.

3.4.1: The designated threshold for dealers in precious metals and stones is USD15, 000 (Fifteen Thousand US Dollars or its Dalasi equivalent at the prevailing market exchange rate).

3.4.2: The threshold for casinos (including internet casinos, if applicable) is USD3, 000 (Three Thousand United States Dollar or its Dalasi equivalent at the prevailing market exchange rate).

3.5: Below is a list of know your customer (KYC) requirements necessary to carry out CDD for various client categories;

3.5.1: CLIENT IDENTIFICATION (NATURAL PERSON-GAMBIAN RESIDENT):

For the purpose of identifying a client who is a Gambian and resident in The Gambia, DNFBPs shall consider the following as means of identifying a customer/client:

- a. a valid photo bearing national identity card, drivers' licence, passport, voter's card with clear photo or other official identification document;
- b. Tax Identification Number (TIN)
- c. the person's name, address and occupation, including utility bills if applicable;
- d. Telephone, fax numbers, and e-mail address;
- e. Date and place of birth;

3.5.2: CLIENT IDENTIFICATION (NATURAL PERSON GAMBIAN RESIDENT ABROAD):

This in addition to the requirements listed in section 3.5.1 (a-d) may include all or some of the following:

- a. Country and address of residence abroad;
- b. Telephone numbers abroad;
- c. Utility Bills if applicable;
- d. Place of work and position held;
- e. And any other proof of identity

3.5.3: CLIENT IDENTIFICATION (NATURAL PERSON-FOREIGN RESIDENT)

DNFBPs shall use some of the following to identify this category of client/customer.

- a. Valid Foreign Passport
- b. Valid Foreign National Identification Card
- c. Residence Permit/Alien Identification Card
- d. Valid Driver's license issued by competent agency
- e. Official Tax identification number or tax clearance certificate
- f. Birth Certificate or sworn declaration of age
- g. Documentary evidence of address
- h. Recent utility bills (if applicable)
- i. Bank Statement or passbook containing current address

- j. Tenancy agreement
- k. Place of work, and any other proof of identity.

3.5.4: CLIENT IDENTIFICATION (NATURAL PERSON-FOREIGN NON-RESIDENT):

The proof of identity of a client of foreign nationality and resident abroad should in addition to {3.5.3 (a-k)} above should include;

- a. Certified national documents and proof of residence by his/her embassy or consulate should in case the original is not sighted by the competent official of the DNFBPs.

3.5.5: CLIENT IDENTIFICATION (LEGAL ENTITIES)

DNFBPs are required to collect evidence of the existence of the legal entities (these include; corporate bodies, partnerships, trust companies, etc.), the identities of management, and the identities of shareholders and the beneficial owners.

The following documents may substantiate identity of legal persons:

- a. Registered corporate name and any trading names
- b. Original or certified copy of the certificate of incorporation and memorandum and articles of associations and
- c. Registration or incorporation number
- d. Principal place of business operations
- e. Mailing address
- f. Contact telephone and fax number numbers
- g. Names of Directors
- h. Partnership deed,
- i. Trust, nominees and fiduciary agreements and;
- j. Evidence of identity of any other legal arrangements thereafter.

Enhanced due care should be taken in dealing with non-resident legal entities. The proof of evidence of identity of the management, shareholders, beneficial owners and any such person(s) controlling interests in the legal entity should be provided as in sections 3.5.1, 3.5.2, 3.5.3 and 3.5.4.

3.6: VERIFICATION OF CLIENT IDENTITY (NATURAL PERSONS AND LEGAL ENTITIES)

3.6.1: The identification documents obtained in section 3.5.1, 3.5.2, 3.5.3, 3.5.4 and 3.5.5 should be verified by the DNFBPs from independent sources for authentication.

3.6.2: All copies of the identify documents should be stamped, dated and signed by the Compliance Officer and other competent persons in the DNFBPs and marked “original sighted” or in any suitable wordings acknowledging sighting the original. In the case of a natural person the identity document as may apply should have the photographic evidence of the client/customer.

3.6.3: DNFBPs shall take adequate measures in verifying the identities of all clients especially when dealing with non-face-to-face customers who supply information by post, telephone, or electronically. Such documents must be authenticated by competent authorities. All copies of identity documents sent by post or electronically must be certified by a lawyer, notary public/court of competent jurisdiction, foreign consulate, banker, accountant, senior public servant, or other person of comparable seniority in the private sector. The person doing the certification must be known and capable of being contacted, if necessary.

3.6.4: Where the reporting entity is unable to obtain satisfactory evidence of identity of a customer, the DNFBPs should not establish a business relationship with the customer/client. However, appropriate time should be given to obtain the appropriate identification documents. If the customer/client fails to provide relevant identification in a reasonable span of time, then the DNFBP should discontinue the transaction or the relationship.

3.6.5: DNFBPs are required to verify the identity of legal person’s existence. In doing so, the DNFBPs should use independent sources to verify the legality of the existence of the business. This may include verifying with the Registrar of Companies in The Gambia and abroad in the case of a foreign legal entity and from other official documents or sources.

The identities of the shareholders, the beneficial owners, and any such person(s) having interest in the legal persons should be verified.

3.6.6: DNFBPs should also verify the authenticity of the legal authority of the natural persons running the day to day management of the legal persons. The Power of Attorney and Third Party Mandates should be adequately verified.

3.6.7: In the case of trust, nominees and fiduciaries, the DNFBPs are required to identify and verify the identity of the trustee(s), the settlor(s), i.e. the provider of the funds, the controllers (who have the power to remove the trustees) beneficiaries, and signatories. All monies received or payments made on behalf of trusts should be checked to identify the source of the funds and the nature of the transactions and to ensure that adequate due diligence has been observed by the remitting bank on the underlying client and the origin of the funds.

3.6.8: DNFBPs should see the constitutions of clubs, associations or the societies and satisfy themselves with their legitimate purpose and existence before establishing the relationship. The natural persons charged with the responsibility of discharging the affairs of the clubs, associations or societies should be established and verified as appropriate. In the case of a suspicion of the clubs, associations or the societies of being involved, aiding and/or about to assist third party in a money laundering and terrorism financing schemes or any other criminal conduct, then the veil should be lifted to identify the contributing members of the associations and/or any affiliates.

3.6.9: When an existing customer enters into a new agreement to purchase products or services, there is no need to verify the identity or address for such a customer unless the name or the address provided differs from the information in the designated institution’s records. However, care must be taken to guard against impersonation fraud.

3.6.10: Customer/client identification and verification specified in sections 3.5.1, 3.5.2, 3.5.3, 3.5.4 and 3.5.5 applies to casual customers when the sum of the transaction is greater than GMD 200,000 (Two hundred thousand dalasi) or its equivalent in any foreign currency.

In certain circumstances, DNFBPs should take measures to verify the identity of the officials purporting to act on behalf of the government and/or government agency.

4.0: AML/CTF COMPLIANCE REQUIREMENTS

The AML/CFT requirements detailed in subsection 4.1.0 to 4.5.0 below shall be implemented by DNFBPs.

4.1.0: RECORD KEEPING REQUIREMENTS

DNFBPs should establish and maintain records of;

- a. A Person’s identity;
- b. Transactions carried out by DNFBPs for clients and correspondence relating to the transactions as is necessary to be readily reconstructed at any time by the FIU or competent authority,
- c. Reports made to the FIU – STRs and other reports;
- d. Enquiries relating to money laundering and financing of terrorism made by it to the FIU.

4.1.1: The records mentioned above (4.1.0) shall be kept for a minimum period of five (5) years from the date;

- a. The evidence of a person’s identity was obtained;
- b. Of any transaction or correspondence;
- c. The account is closed or business relationship ceases, whichever is the later.

4.1.2: If the identification and verification of identity was done electronically, evidence(s) shall be kept electronically or the printed copies certified and kept for a period of not less than five years from the date of termination of the relationship. In the case of transaction(s) conducted electronically, such evidences shall be kept for a period of five years from the date of termination of the relationship.

4.1.3: In the case of a reliance on third party verification(s) (if permitted), all such records shall be kept for at least five years. Where such is permitted, DNFBPs have the ultimate responsibility for client(s)/ customer(s) identification and verification and in such circumstances; the records must be kept for a period of at least five years.

4.2.0: REPORTING REQUIREMENTS

4.2.1: If a DNFBP suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to money laundering or terrorist financing, it is required to report promptly to the Financial Intelligence Unit (FIU) as per section 33, subsection (1a) and (1b) of the Anti-Money Laundering and Combating Terrorism Financing 2012. The DNFBPs must have the requisite technology or means to detect suspicious transactions.

4.2.2: DNFBPs should also file a report if it receives information that may be relevant to;

- a. An act preparatory to an offence of terrorism financing OR;
- b. An investigation or prosecution of any person or for criminal conduct, a money laundering or terrorism financing offence.

4.2.3: Such report of suspicions shall be made and delivered to the Financial Intelligence Unit (FIU) as per section 33, subsection (2a, b, c & d) of the AML/CTF Act 2012 in a prescribed form (see appendix). In addition to reporting suspicious transactions,

- a. Casinos are required to report to the FIU if they enter into transactions or related transactions with their clients which is equal to USD 3, 000 or above or its equivalent in any currency. In addition, all casinos are required to operate under proper licencing by a supervisory authority.
- b. Dealers in precious metals and precious stones are required to report to the FIU if they enter into business transactions or related transactions with their customers involving amount of USD 15, 000 or its equivalent in any currency.
- c. Real estate agents are required to report suspicious transaction(s) to the FIU, after forming a reasonable suspicion of the customer activities which may be related to money laundering and/or terrorism financing activities or any criminal conduct.
- d. Accountants, lawyers, notary publics or other independent legal professionals are required to report suspicious transactions to the FIU in relations to their client(s) after having made reasonable grounds of suspicion of money laundering and terrorism financing activity or any criminal conduct. Accountants, lawyers, notary publics or other independent legal professionals relates to;
 - i. buying and selling of real estate,
 - ii. managing client money,
 - iii. managing bank savings or securities accounts,
 - iv. the organisation of contributions for the creation, operation or management of companies or the buying and selling of business entities,
 - v. acting as or arranging for another person to act as a director or secretary of a company, a partner in a partnership or in a similar position in relation to other legal persons,

- vi. providing a registered business office address or accommodation, or a correspondence or administrative address for a legal person, or
 - vii. Acting as or arranging for another person to act as a Trustee of an express trust or nominee shareholder for another person.
- e. Trust or Company Service Providers are also required to report suspicious transactions to the FIU after having made reasonable grounds of suspicion of money laundering and terrorism financing activity or any criminal conduct in relation to their clients. Trust or Company Service Providers relates to;
- i. acting as a formation agent of legal persons,
 - ii. acting as a director or secretary of a company, partner in a partnership or a similar position in relation to other legal persons,
 - iii. providing a registered office, business address or accommodation, or correspondence or administrative address for a company partnership or any other legal person or arrangement,
 - iv. acting or arranging for another person to act as a trustee of an express trust, or
 - v. acting or arranging for another to act as a nominee shareholder for another person.

4.2.4: Professional secrecy of some professions are given due consideration as in the case of the lawyers as specified in section 33 (6a, b, c & d) of the AML/CTF Act 2012. However, as in section 33 (7) of the same Act where the information consists wholly or partly of, or relates wholly or partly to receipts, payments, income, expenditure, or financial transactions of a specified person (whether a lawyer, his or her client, or any other person), it shall not be a privileged communication if it is contained in or comprises the whole or part of, any book, account, statement or other record prepared or kept by the lawyer in connection with a trust account of the lawyer.

4.3.0: TRAINING REQUIREMENTS

4.3.1: According to section 39 of the AML/CTF Act 2012, Reporting Entities shall;

- a. Make its officers and employees aware of the laws relating to money laundering and financing of terrorism;
- b. Make its officers and employees aware of the procedures, policies and audit systems adopted by it to deter money laundering and financing of terrorism;
- c. 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.

4.3.2: DNFBPs should at a minimum, maintain the following information so as to show proof of compliance with the training requirements,

- 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 DNFBPs own training plan.

4.3.3: AML/CFT Training can be categorized for different staff levels such as New Hire Orientation, front line officers, supervisors and compliance staff. Training for the entire staff can also be conducted.

4.4.0: INTERNAL CONTROLS

4.4.1 DNFBPs shall have an effective internal control framework consisting of policies, procedures and processes. The internal controls of DNFBPs shall take into consideration the risk of Money Laundering and Terrorism Financing to the operations of their organisations.

4.4.2: The policies, procedures and processes should be able to mitigate risk especially high risk areas such as high risk customers, products and services and transactions with customers from high risk jurisdictions.

4.4.3: DNFBPs shall have an internal audit department tasked with the function of carrying out assessments to test and evaluate how effective compliance policies are being implemented and whether they are effective against the risks identified associated with clients, products and services;

4.4.4: Assessments should also be taken to identify and note weaknesses in policies and procedures and proffer corrective measures while ensuring a timely follow-up of actions;

4.4.5: The frequency of such assessments should be carried out taking into consideration the DNFBP's size and risk profile;

4.4.6: Senior Management of DNFBPs shall be committed to the development and implementation of Internal Controls and ensuring compliance to the internal control measures. A compliance culture driven from the top is vital in improving the management and mitigation of both business and regulatory risks.

4.5.0: APPOINTMENT OF A COMPLIANCE OFFICER

4.5.1: DNFBPs are required to appoint a compliance officer at senior management level with relevant qualification and experience who shall be responsible for ensuring that the reporting entity complies with the requirements of the Act. Due to resource constraints and size of some DNFBPs, compliance officer's job may be handled by a competent staff at senior management level with comparable knowledge and experience. The functions of the compliance officer include but not limited to the following:

- a. Development and establishment of the AML/CFT compliance program and manual of compliance procedures;
- b. Receiving and vetting suspicious transactions reports from staff;
- c. Filing suspicious transactions reports with the Financial Intelligence Unit (FIU);
- d. Ensuring that the compliance program is implemented;

- e. Coordinating the training of staff in AML/CFT awareness, detection, methods and reporting requirements;
- f. Serving both as a liaison to relevant regulatory authorities and a point-of-contact for all employees on issues relating to money laundering and terrorist financing;
- g. Review compliance policies and procedures to reflect changes in legislations or international developments;
- h. Participate in the approval process for high-risk business lines and new products, including those involving new technologies;
- i. Monitor the business relationships for whom an STR has been made earlier.

5.0: ENHANCED DUE DILIGENCE (EDD)

5.1: DNFBPs are required to apply enhanced due diligence (EDD) on clients assessed as presenting a higher risk for ML/TF on a risk sensitive basis. As such DNFBPs may conclude that the standard evidence of identity required under the identification procedures in this guideline is insufficient and as such may seek to obtain additional information about a particular client.

5.2: Circumstances may result to a DNFBP determining that a client is high risk. Such may include but not limited to the following;

- a. Product type
- b. Client type/profession
- c. The volume of client business activity;
- d. Ownership and legal structure;
- e. Source of funds/Source of Wealth
- f. Nationality taking into consideration clients from high risk countries;
- g. Residence status

5.3: The extent of additional information sought by a DNFBP and of any monitoring carried out in respect of any particular client will depend on the ML/TF risk that the client is assessed to pose to the DNFBP.

5.4: DNFBPs should therefore adopt a risk based approach (RBA) in risk ranking existing clients into different risk classes (low, medium and high) or by adopting a numbering system of 1 to 5 with 1 being the lowest risk and 5 being the highest risk. The risk rankings of clients shall be documented and shall be conducted for all existing customers.

5.5: DNFBPs should pay particular attention to the following business relations and transactions;

- i. Where a customer has not been physically present for identification purposes;
- ii. Business relationships and transactions with persons from or in countries and jurisdictions known to have inadequate AML/CFT measures (high risk countries);

iii. Business relationships or occasional transactions with Politically Exposed Persons.

5.6: A Politically Exposed Person (PEP) is a person who is or has been entrusted with a prominent public function domestically or in a foreign country, such as a Head of State or of government, a senior political party official, a senior Government official, judicial or military officer, a person who is or has been an executive in a foreign country of a state-owned company, or a person who is or has been a senior political party official in a foreign country, or any immediate family member or close associates.

5.7: A DNFBP should satisfy itself as to the source(s) of wealth of the PEPs.

5.8: Senior management approval and oversight must be sought in establishing a client or business relationship with PEPs.

5.9: In relation to prospective clients, DNFBPs are required to conduct an assessment of the potential risk inherent in each new client relationship. This assessment shall be conducted prior to the establishment of the business relationship taking into consideration the products or services to be of interest to the client, whether the client may expose the DNFBP and if so to what extent. This assessment will enable the DNFBP to determine whether or not to establish the business relationship.

6.0: TIPPING OFF

6.1: Sections 34 and 35 of the AML/CTF Act 2012 prohibits reporting entities, its Directors, officers, employees or agents or any other person to disclose the fact that a suspicious transaction report has been filed with the FIU.

6.2: A person shall not disclose

- a. That a report has been or may be made or further information has been provided to the FIU;
- b. That the reporting entity has formed a suspicion in relation to a transaction; OR
- c. Any information from which the person to whom the information is disclosed could reasonably be expected to infer that a suspicion has been formed or that a report has been made.

7.0: PENALTIES FOR NON-COMPLIANCE

Failure to comply with the requirements of the AML/CTF Act 2012 can result to penalties and/or criminal charges to reporting entities and individuals. Some of the following penalties for non-compliance include;

7.1: Unauthorised disclosure of suspicious transaction reports (Tipping Off) - A person who discloses information in relation to a filed STR contrary to sub-section 1 and 4 of section 34 AML/CTF Act 2012 commits an offence and is liable on conviction to a fine not exceeding GMD 10,000 (Ten thousand dalasi) or imprisonment not exceeding two years or both the fine and imprisonment.

7.2: Accounts in fictitious, false or incorrect name - A person who opens, operates or authorises the opening of an account in fictitious names is liable to a fine not exceeding GMD 10,000 or imprisonment not exceeding two years or both fine and imprisonment – s.32 of the AML/CFT Act 2012.

7.3: Offence of Money Laundering – An individual, including a director, employee or agent of a reporting entity is liable to imprisonment for a term of not less than 10(ten) years if convicted for Money Laundering;

In the case of a body corporate the penalty is a fine of not less than GMD 10,000,000 (Ten million dalasi) or an order for the revocation of the licence of the body corporate or both may be applicable.

7.4: Offence of Terrorism Financing - An individual, including a director, employee or agent of a reporting entity is liable to imprisonment for a term of not less than 10 (ten) years if convicted for Money Laundering;

In the case of a body corporate the penalty of a fine of not less than GMD 10,000,000 (Ten million dalasi) or an order for the revocation of the license of the corporate body or both may be applicable.

NB: A person who directly or indirectly commits the offence of financing of terrorism if he/she

- a. 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;
- b. Organises or directs others to commit, attempts to commit or conspires to commit an offence of terrorism financing.

8.0: RISK ASSESSMENT

8.1: Risk can be seen as a function of threat, vulnerability and consequence. An ML/TF risk assessment is a process based on a methodology, agreed by those parties involved, that attempts to identify analyse and understand ML/TF risks and serves as a first step in addressing them. Ideally, a risk assessment, involves making judgments about threats, vulnerabilities and consequences.

8.2: A 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.

8.3: 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 reporting 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.

8.4: 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.

8.5: FATF Recommendation 1 and its Interpretative Note require DNFBPs to conduct a business related risk assessment of its ML/TF risks. To execute this, DNFBPs 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. A reporting entity is 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:

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

8.6: Risk is a function of the likelihood of occurrence of risk events and the impact of risk events. The likelihood of occurrence is a combination of threat and vulnerability. Accordingly, the level of risk can be mitigated by reducing the size of the threats, vulnerabilities, or their impact.

8.7: 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 international services might be more attractive to a money launderer than 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:

8.4: 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.

8.5: FATF Recommendation 1 and its Interpretative Note require DNFBPs to conduct a business related risk assessment of its ML/TF risks. To execute this, DNFBPs 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. A reporting entity is 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. Identifying the areas of the business operations prone to ML/TF;
- ii. Conducting an analysis in order to assess the likelihood and impact of ML/TF;
- iii. Managing the risks; and
- iv. Monitoring and reviewing the risks.

8.6: Risk is a function of the likelihood of occurrence of risk events and the impact of risk events. The likelihood of occurrence is a combination of threat and vulnerability. Accordingly, the level of risk can be mitigated by reducing the size of the threats, vulnerabilities, or their impact.

8.7: 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 international services might be more attractive to a money launderer than 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:

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

In view of the fact that the nature of terrorism financing differs from that of money laundering, the risk assessment must also include 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.

8.8: 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 is 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

8.9: 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:

- 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.
- 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.
- Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
- Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activities.

8.10: 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:

- 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;
- 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, trustees, family members or third parties, etc;
- Cash intensive businesses including (informal) money transfer agencies, foreign exchange bureaus, etc;
- Charities and other non-profit organizations (especially those operating on a 'cross border' basis) which are not subject to any form of monitoring or supervision;
- Indirect relationships through intermediaries who are not (or not sufficiently) subject to AML/CFT measures or who are not supervised;
- Customers who are Politically Exposed Persons (PEPs); and
- Occasional customers that do transactions above a certain threshold.

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.

8.11: 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:

- Services identified by internationally recognised and credible sources as being a higher-risk, such as international correspondent banking services and (international) private banking activities;
- Services that inherently promote anonymity or can readily cross international borders, such as online banking services, prepaid cards, private investment companies and trusts;
- New or innovative products or services that are not provided directly by the entity but are provided through channels of the entity;
- Products that involve large payment or receipt in cash;
- Non face-to-face transactions or services;
- One-off transactions

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.

8.12: 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.

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.

It is desirable for managers of different lines of businesses, 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.

8.13: 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 strategies, policies and procedures are important for their actual implementation.

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 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 power to take and implement the necessary decisions.

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.

8.14: 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.

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.

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.

8.15: 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. The audit function is to assess if the policies and processes conform to the law and are performed in an adequate way.

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

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

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.

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.

8.17: 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.

9.0: SUSPICIOUS TRANSACTION REPORTING

9.1: Section 33 of the AML/CTF Act 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 of assistance in the enforcement of the AML/CTF Act 2012

Reporting entities are:

(a) Financial Institutions:

- i. Banks licensed by the Central Bank of The Gambia
- ii. Micro-Financial Institutions licensed by the Central Bank of The Gambia
- iii. Insurance Companies licensed by the Central Bank of The Gambia
- iv. Foreign Exchange Bureaus licensed by the Central Bank of The Gambia

(b) Designated Non-Financial Businesses and Professions

- 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:
 - The buying and selling of real estates,
 - The managing of client money, securities or other assets,
 - The managing of bank, savings or securities accounts,
 - The organization of contributions for the creation of, operation or management of companies, or
 - 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.

9.2: 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:
 - 1. An act preparatory to an offence of the financing of terrorism, or
 - 2. 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

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

9.3: 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.

9.4: 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 or financing of terrorism offence or criminal offence.

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

- a. Business transactions with individuals, corporate persons, financial institutions and DNFBPs in or from other countries, which do not sufficiently comply with the recommendations of the Financial Action Task Force;
- b. A transaction which is complex, unusual or large, whether completed or not;
- c. Unusual patterns of transactions; and
- d. Insignificant but periodic transactions which have no apparent or visible lawful purpose.

9.6: A transaction includes:

- a. 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;
- b. A one-off transaction. This means any transaction other than one carried out in the course of an existing business relationship;
- c. Two or more one-off transactions which appear to be linked;
- d. A transaction which is attempted but not completed.

9.7: 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.

9.8: 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 behaviour. 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.

9.9: 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.

9.10: 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.

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

9.11: 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.

9.12: 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.

9.12.1: Red Flags pointing to Financing of Terrorism**I. Behavioural 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, trustees, family members or third party accounts;
- (g) Use of false identification;
- (h) Abuse of non-profit organizations;

II. 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.

9.12.2: 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

9.13: 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.

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.

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

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

9.15: 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.

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

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.

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.

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

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.

9.17: STRs must be reported, by the following method:

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

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

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.

The Reporting Entity may, in limited circumstances, make a STR via telephone [(220) 4466841/4466840] 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.

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

9.18: Upon the receipt of a STR, the FIU will provide feedback in form of a written acknowledgement letter to the Reporting Entity's Compliance Officer within ten (10) 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.

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.

10.0 HOW TO COMPLETE THE STR/SAR FORM

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

10.1 General Guidelines

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 institution.

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.

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.

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

10.2 SPECIFIC GUIDELINES

PART 1 – INFORMATION ON REPORTING INSTITUTION/PERSON

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.

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

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

Items 4 and 5 – Telephone Number and email address – Enter 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.

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

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.

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.

PART 2 – IDENTIFICATION OF PARTY OR PARTIES TO THE TRANSACTION

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

- 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.
- If the suspicious activity involves an organization (entity), enter its name in Item 9 and enter “N/A” in Items 10 and 11.
- If the reporting entity has knowledge of 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.

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.

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.

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

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

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].

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.*

Item 18 – Date of Incorporation – If an entity or organization is named in item 9 to 11, enter the date of incorporation using for entering date described in part VII [dd/mm/yy].

Item 19 – Business Registration Number – If an entity or organization is named in items 9 to 11, enter the business registration number as provided in the business registration certificate from the Registrar of Companies.

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.

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

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].

PART 3 – TRANSACTION DETAILS & SUSPICION

Item 24 – Date of Transaction – Enter 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.

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].

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.

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.

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.

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.”.

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.

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.

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.

PART 4 – NAME OF ALL OFFICERS, EMPLOYERS OR AGENTS DEALING WITH THE TRANSACTION

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.

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.

PART 5 – DESCRIPTION OF SUSPICIOUS ACTIVITY

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.

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

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

PART 6 – DESCRIPTION OF ACTION TAKEN

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). Also state whether the suspect made any voluntary statement as to the origin or source of the proceeds. Kindly enclose copy of the statement, if any.

Part 7 – ADDITIONAL INFORMATION RELATING TO STR/SAR SUBMITTED TO THE FIU

I. Request for further information


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

II. Tipping Off/ Confidentiality

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.

III. Immunity

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.

 FINANCIAL INTELLIGENCE UNIT OF THE GAMBIA Suspicious Transaction Report			
Send completed form by registered post or hand delivery to: Financial Intelligence Unit 380 Senegambia Highway Kerr Serign West Coast Region		Report No. _____ Date of report ____/____/____	
Use this form if you are a reporting person or entity and you have reasonable grounds to suspect that a transaction(s) is/are related to money laundering, terrorism financing and other criminal conducts. All fields of the report marked with an asterisk (*) must be completed. The ones that are also marked "if applicable" must be completed if they are applicable to you or the transaction being reported. For all other fields, you have to make reasonable efforts to get the information.			
PART 1 Information on Reporting Institution/Person			
1 Which of the following types of reporting persons or entities best describes you? *			
A. ___/Commercial Bank B. ___/Insurance company/agent C. ___/Foreign Exchange Bureau D. ___/Micro-Finance Company	E. ___/Real Estate Company/agent F. ___/Accountant G. ___/Lawyer (Private) H. ___/Independent legal professionals	I. ___/Notary J. ___/Dealer in precious metals K. ___/ Dealer in precious stones L. ___/Trust & Company Service Provider	
2 Full name of Reporting Institution or Person* _____ 3 Full address of Reporting Institution /Person* _____ _____ 4 Telephone No.* _____ 5. Email Address _____ 6 Supervised by (if applicable) ___/CBG ___/FIU ___/ Others (please specify) _____ 7 Full Name of Contact Person* and Telephone No.* _____			
This suspicious report should not be communicated directly or indirectly to any person involved in the suspicious transaction or to an unauthorised third party that this transaction has been reported (Section 34 of THE AML/CTF ACT 2012)			
Sign Here	8 Name and Title of reporting officer* _____ <input type="checkbox"/>	8.1 Signature of reporting officer* _____	8.2 Date of Signature* _____

PART 2 Identification of the party or parties to the transaction	
9. Surname* or Name of Entity* _____	10. Given Name* _____
	11. Other /Initial* _____
12. Individual's Identity* (enclose copy) ID Card ___/ ___/ ___/ Driver's License / ___/ ___/ Passport ___/ ___/ Other (description) _____	
13. Full address* _____ _____	
14. Nationality* _____	15. Phone number* _____
16. Individual's date of birth* _____/_____/_____ Day Month Year	17. Individual's Occupation* or Type of Business* _____ _____
18. Date of Incorporation (if applicable) _____/_____/_____ Day Month Year	
19. Business Registration Number: _____	
20. Relationship to the reporting institution* _____ _____ _____	21. Is the relationship an insider relationship?* A ___ Yes B ___ No 22. If YES please specify below* A ___ Still employed B ___ Suspended C ___ Terminated D ___ Resigned 23. Date of Suspension / Termination / Resignation* ____/____/_____ Day Month Year
PART 3 Transaction Details & Suspicion	
24. Date of Transaction* ____/____/_____ Day Month Year	25. Date posting if different from date of transaction* ____/____/_____ Day Month Year
26. Funds involved in the transaction* A. ___/ Cash D. ___/ Electronic Funds Transfer G. ___/ Insurance Policy J. ___/ Others B. ___/ Cheque E. ___/ Bank Draft H. ___/ Money Order _____ C. ___/ Currency Exchange F. ___/ Securities I. ___/ Real Estate (specify)	
27. Amount of Transaction* _____	28. Type of account* _____
29. Bank account details* _____	
30. Status of the account at the time the transaction was initiated (if applicable) _____	
31. Reason for suspicion* (complete part V as well) _____	
32. Has the suspicious activity had a material impact on, or otherwise affected, the financial soundness of the institution or person* ___/ Yes ___/ No	
PART 4 Name of all officers, employers or agents dealing with the transaction	
33. Contact for assistance*	
33.1 Full name* _____	33.2 Title / Occupation* _____
33.3 Telephone No* _____	

PART 5 Description of suspicious activity
34. This section of this report is Critical . Describe clearly and completely the facts or unusual circumstances that led to the suspicion of money laundering, terrorist financing or 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.* <i>If necessary, continue the narration on a duplicate of this page.</i>

PART 6 Description of action taken

35. 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.

If necessary, continue the narration on a duplicate of this page.

FIU

380 Senegambia Highway, Kerr Serign
West Coast Region, The Gambia
Tel: +220 4466839 / 4466840
Web: www.fiugambia.gov.gm
Email: info@fiugambia.gov.gm