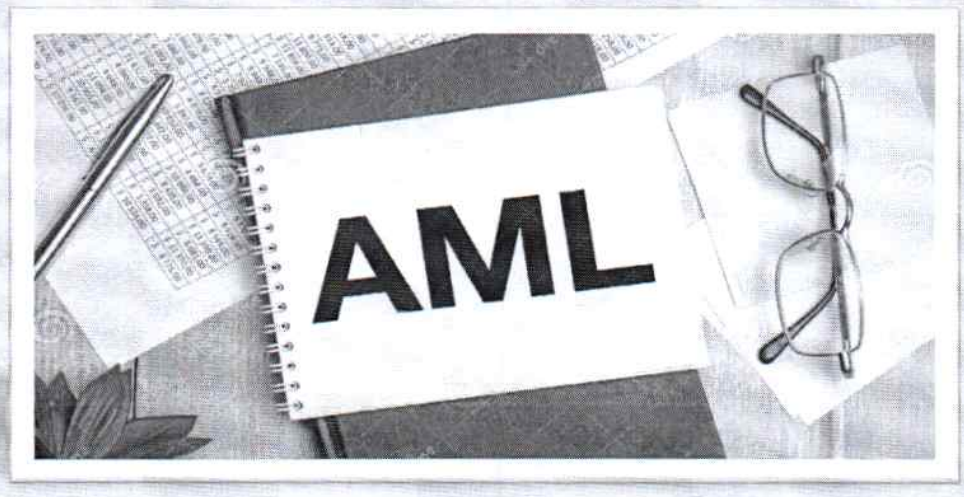
Modhumoti Bank PLC.
Your Access to Success

MMBPLC Policy on Prevention of Money Laundering & Combatting Terrorist Financing

Version 2025

AML & CFT Division
Modhumoti Bank PLC
Head Office



Editorial Committee

Chairman	:	Mr. Arab Fazlur Rahman, DMD & CAMLCO
Reviewed by		Central Compliance Committee (CCC)
Recommended by	:	Management Committee (ManCom)
Team Members	:	Mr. Md. Almas Uddin Miah, Head of AML&CFTD & Deputy CAMLCO
		Mr. Md. Mahabubur Rahman Chowdhury, FAVP, AML&CFTD
		Mr. Zahid Ahmed, Senior Executive Officer, AML&CFTD

Version Control:

MMBPLC Policy on Prevention of ML&CFT	:	August 2020 (1st Version)
MMBPLC Policy on Prevention of ML&CFT	:	December 2023 (2nd Version)
MMBPLC Policy on Prevention of ML&CFT	:	**December 2025** (Present Version)
Next Date of MMBPLC Policy on Prevention of ML&CFT	:	November 2026

MMBPLC POLICY on PREVENTION OF MONEY LAUNDERING & COMBATING TERRORIST FINANCING (V-2025)

TABLE OF CONTENTS

Combating Financing of Terrorism Guidelines

TABLE OF CONTENTS

ANNEXURES:

Preamble

In response to the growing global concern regarding Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF), the international community has taken extensive initiatives to safeguard the integrity and stability of the financial system. The United Nations (UN) was the first international body to adopt significant conventions and resolutions to combat money laundering. Building on these efforts, the Financial Action Task Force (FATF) was established in 1989 by the G-7 nations as the premier intergovernmental body to develop and promote international AML/CFT standards. FATF issued its first Forty Recommendations in 1990, and in the aftermath of the events of 2001, expanded its mandate to address terrorist financing through the creation of Eight (later Nine) Special Recommendations. In 2012, FATF consolidated these into the globally recognized Forty Recommendations, which now include measures addressing Proliferation Financing. Over 180 countries have endorsed these standards.

Recently Bangladesh Bank, SPCD Circular No. 2 dated 23 October, 2025 'Implementation of Risk Based Supervision (RBS): Supervisory Expectations and Banks' preparedness' circulated wherein it was instructed in serial no. 6 for *Documentation Update- 'Update all the risk management policies, manuals, standard operating procedures, and internal control frameworks to align with RBS framework by December 2025'*. Upon getting this concrete, practical and convenient guideline, the Bank, on its firm commitment for compliance, has formed a committee to review and update 'MMBPLC Policy on "Prevention of Money Laundering & Combating Terrorist Financing (Version-2025) with the determination of adopting the policy in the Bank within provided time frame to establish appropriate measures and techniques to combat ML/TF & PF.

The revised policy reflects the Bank's commitment to uphold global standards in Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT). It aligns with the recommendations of the Financial Action Task Force (FATF) and national regulatory requirements. The preamble emphasizes:

- **Purpose**: To establish robust internal controls that prevent misuse of banking channels for illicit financial activities.
- **Scope**: Applies to all departments and personnel, ensuring consistent compliance across the organization.
- **Responsibility**: Assigns clear accountability for implementing AML/CFT measures, including customer due diligence, transaction monitoring, and reporting suspicious activities.
- **Commitment**: Reinforces the bank's dedication to ethical practices and protecting the integrity of the financial system.

MMBPLC instructs all officials of the Branches/Divisions/Departments/Agent Banking to follow the guideline in order to mitigate Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) risks. The purpose of this guidance is to build the legal and regulatory framework for this purpose and thus the documents interpret the requirements of the relevant laws and regulations and how they might be implemented in practice. It indicates good industry practices in AML& CFT procedures through proper guidance, assists the banks to design & implement the systems and controls necessary to mitigate the risks of the banks being used in connection with Money Laundering, Terrorist Financing and Proliferation Financing.

Chapter # 1

Introduction

Chapter # 1
Introduction

1. Introduction

1.1 Money Laundering is being employed by launderers worldwide to conceal the proceeds earned from criminal activity. It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins. And the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit "dirty" money in one country and then have it transferred to any other country for use.

1.2 Money laundering has a major impact on a country's economy as a whole, impeding the social, economic, political, and cultural development of societies worldwide. Both money laundering and terrorist financing can weaken individual financial institution, and they are also a threat to a country's overall financial sector reputation. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound and stable financial sector.

1.3 The process of money laundering and terrorist financing is very dynamic and ever evolving. The money launderers and terrorist financers are inventing more and more complicated and sophisticated procedures and using new technology for money laundering and terrorist financing. To address these emerging challenges, the global community has taken various initiatives against ML/TF. In accordance with international initiatives, Bangladesh has also acted on many fronts.

1.4 A Focus Group was formed to prepare a Guidance Notes on Prevention of Money Laundering with the representatives from Bangladesh Bank, Nationalized Commercial Banks, Private Commercial Banks and Foreign Banks operating in Bangladesh. The Focus Group has prepared a Guidelines and Bangladesh Bank has circulated that among all the Banks and Financial Institutions. All the Banks and Financial Institutions have been advised to formulate their own operation policies for effective prevention of Money Laundering.

1.5 Keeping the above mandatory requirement in view, Modhumoti Bank Limited has prepared this handbook giving the title "Anti-Money Laundering Policy (Revised)". This Book contains the fundamentals of the Guidance Notes of Focus Group as well as the recent changes and its implication procedures; we have to follow for compliance of the vital task.

1.6 Mainly, we have considered two things in preparing this revised AML Policy. Firstly, the contents of the Money Laundering Prevention Act, 2012 and Secondly, the Bangladesh Bank's Anti Money Laundering regulations, the related circulars issued form BFIU time to time and some important recent developments in AML/CFT regime.

1.7 It is expected that each and every employee of Modhumoti Bank Limited must exercise the anti-money laundering activities with due care and diligence for the sake of his / her carrier and for the interest of the institution itself.

2. What is Money Laundering

- Money laundering can be defined in a number of ways. But the fundamental concept of money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Most countries subscribe to the following definition which was adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):
- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

- The concealing or disguising the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.
- The Financial Action Task Force on Money Laundering (FATF)[1], which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term "money laundering" succinctly as "the processing of...criminal proceeds to disguise their illegal origin" in order to "legitimize" the ill-gotten gains of crime.

'Money Laundering' is defined in Section 2 (v) of the ML Prevention Act 2012 as follows:

"Money Laundering" means –

(i) Knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:-

1. concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
2. assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;

(ii) Smuggling money or property earned through legal or illegal means to a foreign country;

(iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or

(iv) Concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;

(v) Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;

(vi) Acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;

(vii) Performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;

(viii) Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

3. Why Money Laundering is done

Criminals engage in money laundering for **three** main reasons:

3.1 First, money represents the lifeblood of the organization/person that engages in criminal conduct for financial gain because it covers operating expenses and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

3.2 Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

3.3 Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

4. Why we must combat Money Laundering

4.1 Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a process vital to making crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and

[1] The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 34 countries and territories and two regional organizations.

expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences that result. Crime has become increasingly international in scope, and the financial aspects of crime have become more complex due to rapid advances in technology and the globalization of the financial services industry.

4.2 Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate. We also pay more taxes for public works expenditures inflated by corruption. And those of us who pay taxes pay more because of those who evade taxes. So we all experience higher costs of living than we would if financial crime—including money laundering—were prevented.

4.3 Money laundering distorts asset and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability and even systemic crisis. The loss of credibility and investor confidence, that such crisis can bring, has the potential of destabilizing financial systems, particularly in smaller economies.

4.4 One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, which co-mingle the proceeds of illicit activity with legitimate funds, to hide the ill-gotten gains. These front companies have access to substantial illicit funds, allowing them to subsidize front company products and services at levels well below market rates. This makes it difficult, if not impossible, for legitimate business to compete against front companies with subsidized funding, a situation that can result in the crowding out of private sector business by criminal organizations.

4.5 No one knows exactly how much "dirty" money flows through the world's financial system every year, but the amounts involved are undoubtedly huge. The International Money Fund has estimated that the magnitude of money laundering is between 2 and 5 percent of world gross domestic product, or at least USD 800 billion to USD1.5 trillion. In some countries, these illicit proceeds dwarf government budgets, resulting in a loss of control of economic policy by governments. Indeed, in some cases, the sheer magnitude of the accumulated asset base of laundered proceeds can be used to corner markets -- or even small economies.

4.6 Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government, and citizens to criminals. Furthermore, the sheer magnitude of the economic power that accrues to criminals from money laundering has a corrupting effect on all elements of society

4.7 The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing of government officials undermines the moral fabric in society, and, by weakening collective ethical standards, corrupts our democratic institutions. When money laundering goes unchecked, it encourages the underlying criminal activity from which such money is generated.

4.8 A nation cannot afford to have its reputation and financial institutions tarnished by involvement with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions and the underlying criminal activity -- fraud, counterfeiting, narcotics trafficking, and corruption -- weaken the reputation and standing of any financial institution. Actions by FIs to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A financial institution tainted by money laundering accusations from regulators, law enforcement agencies, may loss their good market reputation and damage the reputation of the country. It is very difficult and requires significant resources to rectify a problem that could be prevented with proper program.

4.9 Besides its effect on macro level, ML/TF also affects individual financial institution. If a money launderer uses a financial institution for making his/her money legitimate, the business of that financial institution may hamper. If the money launderer withdraws his/her deposited money from an FI before maturity, the FI will face liquidity crisis if the amount is big enough. Moreover, if it was found that an FI is used for ML/TF activities, and it did not take proper action against that ML/TF, as

per the laws of the country, the FI will have to face legal risk. Finally, the reputation of an FI can also be heavily affected through its involvement with ML/TF activities.

4.10 It is generally recognized that effective efforts to combat money laundering cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies.
Accordingly, in order to address the concerns and obligations of these three parties, these Guidance Notes were drawn up.

5. Stages of Money Laundering:

5.1 It is generally recognized that effective efforts to combat money laundering cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies. Accordingly, in order to address the concerns and obligations of these three parties, these Guidance Notes were drawn up.

5.2 Bankers should have clear idea about the various stages of laundering of money. Detection mechanism can only be successful only if the employees concerned possess the knowledge of whole visible and invisible phases money laundering takes place.

5.3 There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewellery) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). There are a number of crimes where the initial proceeds usually take the form of cash that needs to enter the financial system by some means. Bribery, extortion, robbery and street level purchases of drugs are almost always made with cash. This has a need to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated.

Despite the variety of methods employed, money laundering is not a single act but a process accomplished in 03 (three) basic stages which are as follows:

Placement	The physical disposal of the initial proceeds derived from illegal activity.
Layering	Separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
Integration	The provision of apparent legitimacy to wealth derived criminally. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

5.4 The three basic steps may occur as separate and distinct phases. These steps may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations.

5.5 The three basic steps may occur as separate and distinct phases. These steps may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations.

The table below provides some typical examples.

Placement stage	Layering stage	Integration stage
i) Cash paid into bank (sometimes with staff complicity Or mixed with proceeds of Legitimate business). ii) Cash deported. iii) Cash used to buy high value goods, property or business assets. iv) Cash purchase of single premium life insurance or other investment	i) Sale or switch to other forms of Investment. ii) Money transferred to assets of Legitimate financial institutions. iii) Telegraphic transfers (often Using fictitious names or funds disguised as proceeds of legitimate business). iv) Cash deposited in outstation branches and even overseas banking system. v) Resale of goods/assets.	i) Redemption of contract or switch to other forms of investment. ii) False loan repayments or forged invoices used as cover for laundered money. iii) Complex web of transfers (both domestic and international) makes tracing original source of funds virtually impossible.

6. Vulnerability of the Financial System to Money Laundering

6.1 Money laundering is often thought to be associated solely with banks and moneychangers. All financial institutions, both banks and non-banks, are susceptible to money laundering activities. Whilst the traditional banking processes of deposit taking, money transfer systems and lending do offer a vital laundering mechanism, particularly in the initial conversion from cash, it should be recognised that products and services offered by other types of financial and non-financial sector businesses are also attractive to the launderer. The sophisticated launderer often involves many other unwitting accomplices such as currency exchange houses, stock brokerage houses, gold dealers, real estate dealers, insurance companies, trading companies and others selling high value commodities and luxury goods.

6.2 Certain points of vulnerability have been identified in the laundering process, which the money launderer finds difficult to avoid, and where his activities are therefore more susceptible to being recognized. These are:

- entry of cash into the financial system;
- cross-border flows of cash; and
- Transfers within and from the financial system.

6.3 Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their procedures with due regard to that risk.

6.4 Although it may not appear obvious that the products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that weaknesses cannot be exploited.

6.5 Banks and other Financial Institutions conducting relevant financial business in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. The liquidity of some products may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

6.6 All banks and non-banking financial institutions, as providers of a wide range of money transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.

6.7 All banks and non-banking financial institutions, as providers of a wide range of money transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.

6.8 Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

6.9 However, in addition, banks and non-banking financial institutions, as providers of a wide range of services, are vulnerable to being used in the layering and integration stages. Other loan accounts may be used as part of this process to create complex layers of transactions.

6.10 Some banks and non-banking financial institutions may additionally be susceptible to the attention of the more sophisticated criminal organizations and their "professional money launderers". Such organizations, possibly under the disguise of front companies and nominees, may create large scale but false international trading activities in order to move their illicit monies from one country to another. They may create the illusion of international trade using false/inflated invoices to generate apparently legitimate international wire transfers, and may use falsified/bogus letters of credit to confuse the trail further. Many of the front companies may even approach their bankers for credit to fund the business activity. Banks and non-banking financial institutions offering international trade services should be on their guard for laundering by these means.

6.11 Investment and merchant banking businesses are less likely than banks and money changers to be at risk during the initial placement stage.

6.12 Investment and merchant banking businesses are more likely to find them being used at the layering and integration stages of money laundering. The liquidity of many investment products particularly attracts sophisticated money laundering since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

6.13 Although it may not appear obvious that insurance and retail investment products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that non-traditional banking products and services are not exploited.

6.14 Intermediaries and product providers who deal directly with the public may be used at the initial placement stage of money laundering, particularly if they receive cash. Premiums on insurance policies may be paid in cash, with the policy subsequently being cancelled in order to obtain a return of premium (e.g. by cheque), or an insured event may occur resulting in a claim being paid out. Retail investment products are, however, more likely to be used at the layering and integration stages. The liquidity of a mutual funds may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

6.15 Lump sum investments in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. Payment in cash should merit further investigation, particularly where it cannot be supported by evidence of a cash-based business as the source of funds.

6.16 Insurance and investment product providers and intermediaries should therefore keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

6.17 Corporate vehicles trust structures and nominees are firm favorites with money launderers as a method of layering their proceeds. Providers of these services can find themselves much in demand from criminals.

6.18 The facility with which currency exchanges can be affected through a bureau is of particular attraction especially when such changes are affected in favor of a cheque or gold bullion.

7. How MMBPLC Can Combat Money Laundering

It is now not only our moral obligation to prevent money laundering; but we are legally obligated to take effective measures to prevent it. Laundering of money is as much devastating for the society as to the economy of the country as a whole. Any or all money laundering activities, somehow routes through banking channel. So that the employees of MMBPLC family must know the channels concerned for combating money launder.

7.1 One of the best methods of preventing deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. "**Know Your Customer**" is the key-policy to know what our customers do, how much their transactions are legitimate, how much not. Thus, a prudent Banker can identify the transactions relating to money launder and can take the necessary measures to prevent it.

7.2 Money launders activities are susceptible to recognition and have therefore to a large extent concentrated on the deposit taking procedures of Banks i. e. the placement stage. Therefore, if a Banker analysis the withdrawal pattern of an Account holder, he/she can understand whether the concerned transactions are money laundering related or not.

7.3 Bank and Financial Institutions must keep transaction records that are comprehensive enough to establish an Audit trail. Modhumoti Bank Limited maintains it. So that analyzing the transaction records, we can ascertain primarily about the people and organizations involved in laundering schemes.

7.4 In complying with the requirements of the Act and in following those Guidance Notes, we should at all-time pay particular attention to the fundamental principle of '**good business practice'**- know your customer'. If Bankers have sound knowledge of their customers business and pattern of financial transactions and commitments, they will easily understand which transaction is the outcome of money laundering.

This aspect is referred to in Chapter-VIII of these Guidance Notes- Recognitions and Reporting of suspicious Transactions. It will also be dealt with in staff training programs which are a fundamental part of the procedures designed to recognize and combat money launder and which are referred to Chapter-IX – Training and Awareness

Chapter # 2

International and National Anti-Money Laundering Initiatives

CHAPTER # 2

International and National Anti-Money Laundering Initiatives

1. Introduction:

In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts. This part of this Guidance Notes discusses the various international organizations that are viewed as the international standard setters. It further describes the documents and instrumentalities that have been developed for anti-money laundering (AML) and combating the financing of terrorism (CFT) purposes.

2. The United Nations:

The United Nations (UN) was the first international organization to undertake significant action to fight money laundering on a truly world-wide basis. The role of UN is important for several reasons which are -

First, it is the international organization with the broadest range of membership. The UN, founded in 1945, has 191 members from all across the world.

Second, the UN actively operates a program to fight money laundering; the Global Program against Money Laundering, which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).

Third, and perhaps most importantly, the UN has the ability to adopt international treaties or conventions that obligate the ratifying countries to reflect those treaties or conventions in their local laws.

In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other action on the part of an individual country.

2.1 The Vienna Convention

Due to growing concern about increased international drug trafficking and the tremendous amounts of related money entering into financial system, the UN, adopted the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) known as Vienna Convention, named after the city in which it was signed. The Vienna Convention deals primarily with provisions to fight the illicit drug trade and related law enforcement issues. At present, nearly 169 countries including Bangladesh are party to the convention. The convention came into force on November 11, 1990.

2.2 The Palermo Convention

In order to fight against internationally organized crimes, the UN adopted the International Convention against Transnational Organized Crime (2000), named after the city in which it was signed as Palermo Convention. The Palermo Convention specifically obligates each ratifying country to:

- Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;
- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
- Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information;
- Promote international cooperation.

This convention has come into force from 29th September 2003, having been signed by 147 countries and ratified by 82 countries.

2.3 Global Program against Money Laundering

The UN Global Program against Money Laundering (GPML) is within the UN Office of Drugs and Crime (UNODC). The GPML is a research and assistance project with the goal of increasing the effectiveness of international action against money laundering by offering technical expertise, training and advice to member countries upon request.

3. The Financial Action Task Force

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, FATF has 38 Members, 2 Regional Bodies, 2 Observer Countries and number of Associate Members.

3.1 FATF 40+9 Recommendations

FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. Although not binding as law upon a country, the Forty Recommendations was widely endorsed by the international community including World Bank and IMF and relevant organizations as the international standard for AML. The Forty Recommendations were initially issued in 1990 and revised in 1996 and 2003 to take account of new developments in money laundering and to reflect developing best practices internationally. To accomplish its expanded mission of combating financing of terrorism FATF adopted nine Special Recommendations in 2001.

3.2 FATF New Standards

FATF Plenary has again revised its recommendations in February 2012. The previous 40+9 Recommendations has been accumulated into 40 (forty) recommendations called the FATF Standards. Proliferation financing has been included in the new standards. There is no special recommendation to address the financing of terrorism. All special recommendations have been merged with the 40 recommendations. FATF is now working on the assessment process under the new standards. The following table shows the summery of new standards.

Table 1: Summery of new FATF 40 Standards:

Group	Topic	Recommendations
1	Policies and Coordination	1-2
2	Money Laundering and Confiscation	3-4
3	Preventive Measures	9-23
4	Transparency and Beneficial Ownership of Legal Persons and Arrangements	24-25
5	Power and Responsibilities of Competent Authorities and Other Institutional Measures	26-35
6	International Co-operation	36-40

3.3 Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of 40+9 recommendations is facilitated by a two-stage process: self-assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of 40+9 recommendations. In the mutual evaluation stage, each member is examined and assessed by experts from other member countries in every five years. The first Mutual Evaluation (ME) of Bangladesh was conducted by a joint team of World Bank and International Monetary Fund in October, 2002 and the report thereof was -

adopted by the APG in September, 2003. The 2nd Mutual Evaluation of Bangladesh was conducted by an APG team in August, 2008.

3.4 The NCCT List

FATF adopted a process of identifying those jurisdictions that serve as obstacles to international cooperation in implementing its recommendations. The process used 25 criteria, which was consistent with 40+9 recommendations, to identify such non-cooperative countries and territories (NCCT's) and place them on a publicly available list. NCCT was a process of black listing of non-compliant country. Considering its massive impact on respective country, the FATF introduced new implementation mechanism known as International Cooperation and Review Group (ICRG).

3.5 ICRG (International Co-operation review group)

The FATF has set up the International Co-operation Review Group (ICRG) as a new process that is designed to notably engage those jurisdictions which are 'unwilling' and pose a real risk to the international financial system. The ICRG process is designed to bind members of FATF and FATF Style Regional Body (FSRB) that show effective commitment to the standards against those that evade their international obligations. The time and money that one jurisdiction spend on creating an effective system in that country is wasted if a neighbor remains a safe haven for criminals. The ICRG process is focused on specific threats and specific risk in specific countries. If needed, these jurisdictions may be publicly identified by the FATF Plenary.

The second role of the ICRG is to work with those jurisdictions to convalesce the shortcomings underpinning the judgment of the FATF Plenary. This means there could be a focused follow up process between the ICRG and a specific jurisdiction. If all evaluation reviews and regular follow ups are conducted properly, there should be no duplication or conflict within the FATF family and between the follow up processes.

4. The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of Ten countries. Individual countries are represented by their central banks, or by the relevant authorities with formal responsibility for prudential supervision of banking where that authority is not the central bank. The committee has no formal international supervisory authority or force of law. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank/financial institution supervisory issues. These standards and guidelines are adopted with the expectation that the appropriate authorities within each country will take all necessary steps to implement them through detailed measures, statutory, regulatory or otherwise, that best suit that country's national system. Three of the Basel Committee's supervisory standards and guidelines concern money laundering issues.

4.1 Statement of Principles on Money Laundering

In 1988, the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention). The Statement on Prevention outlines basic policies and procedures that managements of banks/FIs should undertake to assist in suppressing money laundering. There are essentially four principles contained in the Statement on Prevention:

- Proper customer identification;
- High ethical standards and compliance with laws;
- Cooperation with law enforcement authorities; and
- Policies and procedures to adhere to the statement.

4.2 Basel Core Principles for Banking

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provides a comprehensive blueprint for an effective bank supervisory system and

covers a wide range of topics. Core Principle 15, one of the 25 Core Principles, deals with money laundering; it provides:

Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know your customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank from being used; intentionally or unintentionally, by criminal elements.

These "know your customer" or "KYC" policies and procedures are a crucial part of an effective institutional framework for every country.

In addition, the Basel Committee issued a "Core Principles Methodology" in 1999, which contains 11 specific criteria and five additional criteria to help assess the adequacy of KYC policies and procedures. These, additional criteria include specific reference to compliance with The Forty Recommendations.

4.3 Customer Due Diligence

In October, 2001, the Basel Committee issued an extensive paper on KYC principles, entitled Customer due diligence for banks/FIs (Customer Due Diligence). This paper was issued in response to noted deficiencies in KYC procedures on a world-wide basis. These KYC standards build upon and provide more specific information on the Statement on Prevention and Core Principle 15.

5. The Egmont Group of Financial Intelligence Units

In 1995, a number of governmental units known today as Financial Intelligence Units (FIUs) began working together and formed the Egmont Group of FIUs (Egmont Group), named after the location of its first meeting at the Egmont-Arenberg Palace in Brussels. The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML programs and to coordinate AML initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs worldwide.

The mission of the Egmont Group has been expanded in 2004 to include specifically financial intelligence on terrorist financing. To be a member of the Egmont Group, a country's FIU must first meet the Egmont FIU definition, which is "a central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national regulation, in order to counter money laundering and terrorist financing." Bangladesh FIU applied for membership in the Egmont Group.

6. Asia Pacific Group On Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 41 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD, United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units.

APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations of the Financial Action Task Force on Money Laundering and Terrorist Financing.

The APG has five key roles:

- To assess compliance by APG members with the global standards through a robust mutual evaluation program;
- To coordinate bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region in order to improve compliance by APG members with the global standards;

- To participate in, and co-operate with, the international anti-money laundering network - primarily with the FATF and with other regional anti-money laundering groups;
- To conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities; and
- To contribute to the global policy development of anti-money laundering and counter terrorism financing standards by active Associate Membership status in the FATF.

The APG also assists its members to establish coordinated domestic systems for reporting and investigating suspicious transaction reports and to develop effective capacities to investigate and prosecute money laundering and the financing of terrorism offences.

Money laundering has become a global problem as a result of the confluence of several remarkable changes in world markets (i.e., the globalization of markets). The growth in international trade, the expansion of the global financial system, the lowering of barriers to international travel, and the surge in the internationalization of organized crime have combined to provide the source, opportunity, and means for converting illegal proceeds into what appears to be legitimate funds.

7. National Initiatives: Issues and initiatives of CAMLCO Conference 2023, 2024 & 2025 & BFIU's Annual Report

In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and terrorist financing, considering their severe effects on the country. Some important initiatives are shown below:

a) Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40+9 recommendations. Subsequently, Bangladesh, as the first South Asian country, promulgated Money Laundering Prevention Act (MLPA), 2002 which came into force on 30 April, 2002. For exercising the power and shouldering the responsibilities, as stated in the MLPA, a separate department named Anti Money Laundering Department (AML&CFTD) was established at Bangladesh Bank.

b) To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009.

c) To combat terrorism and terrorist financing Bangladesh also enacted Anti-Terrorism Act (ATA), 2009. To address the gap identified in the MER, some provisions of ATA 2009 have been amended through enactment of Anti-Terrorism (Amendment) Act 2012.

d) Bangladesh has enacted Mutual Assistance in Criminal Matters Act, 2012 to enhance international cooperation on ML/TF and other related offences.

e) In the process of responding to international concern, Bangladesh Government formed a central and several regional taskforces on 27 January, 2002 to combat money laundering and illegal Hundi activities in Bangladesh.

f) On May 16, 2007 financial intelligence unit (FIU) was established in BB for receiving, analyzing and disseminating Suspicious Transaction Reports (STR) related to ML/TF and Cash Transaction Reports (CTR). As per the provision of MLPA, 2012 AML&CFTD is now working as separate unit in BB as Bangladesh Financial Intelligence Unit (BFIU).

g) Bangladesh Bank (BB) has already issued Guidance Notes under 'core risk' management titled 'Guidance Notes on Prevention of Money Laundering' for banks. BB has also issued guidance notes on for insurance companies, Financial Institutions and money changers.

h) A rigorous Customer Due Diligence (CDD) procedure has been introduced to protect identity theft by customer through issuance of Uniform Account Opening Form for all banks. It includes standardized Know Your Customer (KYC), Transaction Profile (TP) and Risk Grading of Customer.

i) To facilitate exchange of information and intelligence among FIUs, Bangladesh FIU has already signed 36 (thirty-six) MoUs with other FIUs.

j) To provide guidance for effective implementation of regime, a National Coordination Committee headed by the Honorable Finance Minister and a Working Committee headed by the secretary of Bank and Financial Institutions Division of Finance Ministry were formed consisting representatives from all regulatory authorities.

k) Bangladesh Government has developed the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism. The strategy consists of following strategic objectives:
   1. Strengthening the legal framework
   2. Enhancing effectiveness of the FIU
   3. Enforcing compliance of all reporting agencies
   4. Structural improvement and capacity building in tracing out methods, techniques and channels of money laundering and terrorist financing
   5. Improving transparency in financial reporting on issues
   6. Ensuring transparency in the ownership of legal entities
   7. Enhancing financial inclusion
   8. Maintaining a comprehensive database
   9. Boosting national coordination both at policy and operational levels
   10. Developing and maintaining international and regional cooperation on
   11. Heightening public awareness
   12. Stemming the illicit outflows and inflows of fund

l) BFIU in cooperation with Anti-Corruption Commission has assessed ML/TF risk and vulnerabilities in Bangladesh and drafted the National ML/TF Risk and Vulnerability Assessment Report.

m) Bangladesh has continued it pursuance to get membership of the Egmont Group, the global forum for cooperation. In this regard, the off-site evaluation has already been conducted by Malaysia and Thailand as sponsor and cosponsor respectively.

n) The Bank and Financial Institutions Division, Ministry of Finance has issued a circular instructing all the related agencies to share relevant information with Bangladesh Bank.

o) BFIU has continued its effort to develop its IT infrastructure which is necessary for efficient and effective functioning of the unit. In this regard, it has finalized the procurement process of 'goAML' software for online reporting and software-based analysis of CTR and STR.

p) BFIU has established MIS to preserve and update all the information and to generate necessary reports using the MIS.

q) BFIU has arranged a number of training programs, workshops, seminars and road-shows to create awareness among the staff of reporting organizations, regulatory authorities about related issues.

Chapter # 3

The Offences of ML & TF and Punishments as per Law

Chapter # 3

The Offences of ML & TF and Punishments as per Law

3.1 Offences under the Money Laundering Prevention Act, 2012 & Punishments:

All offences under the MLP Act, 2012 are cognizable, non-compoundable and non-bailable and the penalties for the commission of the offences all have prison terms and / or fines as prescribed in the Act as follows:

Section No	Nature of Offense	Punishment
4.2	Attempt, assist and make conspiracy for Money Laundering by **any person**.	Minimum 4 years and maximum 12 years of imprisonment with seizure of double the property acquired through ML or Tk.10 (ten) lac which one is higher. Additionally, Court can order to forfeit the property acquired through ML or Predicate Offences of that person.
4.4	Attempt, assist and make conspiracy by **any entity.**	Penalty of double the value of property acquired or Tk. 20 (Twenty) lac which one is higher with cancellation of registration/approval.
5	Violation of an order for freezing or Attachment	Imprisonment for a term not exceeding 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or with both
6.3	Disclosure of information	Imprisonment up to 2 years or penalty of maximum Tk. 50,000/= or both.
7.2	Obstructing or non-cooperation in Enquiry.	Imprisonment up to 01 year or penalty of maximum Tk.25, 000/= or both.
8.2	Providing false information	Imprisonment up to 03 year or penalty of maximum Tk. 50,000/=or both.
23 Power of Bangladesh Bank on Reporting Organization like us & if we fail:		
23.3	Failing to submit required information within stipulated time	Penalty of Tk. 10,000/= per day up to maximum Tk. 5.00 lac, If such penalty is imposed more than 3 times in a financial year, license will be cancelled.
23.4	Furnishing false statements	Penalty of minimum Tk. 20,000/= and maximum Tk. 5.00 lac, If such penalty is imposed more than 3 times in a financial year, license will be cancelled.
23.5	Failing to comply with any instruction.	Penalty of Tk.10,000/= per day up to maximum Tk.5.00 lac for particular non-compliance issue, If such penalty is imposed more than 3 times in a financial year, license will be cancelled.
23.6	Failing to comply with the instruction of section 23(1)(Ga) regarding Account Freezing or Suspend Order by Bangladesh Bank	Minimum Penalty of that Account Balance which will not more than double of balance as per instruction circulation date
23.7	Failing to pay the penalty as per section 23 & 25 of MLPA, 2012	Realize the amount by debiting self-named account of related person /entity/reporting agency with any Bank/Financial Institution /Bangladesh Bank and if any amount remains unpaid, suit will be filed for recovery of the same by the order of Court.
23.8	Penalty have been imposed to Owner, Director and employees under payroll or contract service of any reporting agency for non-compliance of AML & CTF instruction	Individual penalty of minimum Tk. 10,000/= and maximum Tk. 5.00 lac along with administrative disciplinary action.
25.2	Any reporting organization failed to discharge their responsibility as per Article 25 (1) of the MLP Act, 2012 like preserving customers proper and full information, record keeping for Closed. A/C for minimum 5 (five) years, failure of submission return/ sending STR to Bangladesh Bank.	Penalty of minimum Tk. 50,000/= and maximum Tk. 25.00 lac. Additionally, license will be cancelled of that organization or Branch, service center, booth of that organization.

Penalties of Terrorist Financing

Offence	Reference	Penalties
Committing the offence of financing terrorism	Sec. 7(1) & 7(3) AT Act 2009	Min 4 yrs. to 20 yrs. of rigorous imprisonment with fine of two times of the value of the property involved with the offence or Tk. 10 Lac whichever is higher
Entity committed the offence of financing terrorism	Sec. 7(1) & 7(4) AT Act 2009	The entity can be banned by the Government with fine of three times of the amount involved with the offence or Tk. 50 lac whichever is greater
Non-compliance	**Reference**	**Penalties**
Failure to comply with th directions issued by BB or knowingly provide any wrong information	Sec. 15(8) of AT Act 2009	Maximum fine of Tk25 lac and may suspend the registration or license
Failure to take necessary measures, with appropriate caution and responsibility, to prevent and identify terrorist financing and to spontaneously report suspicious transaction if any.	Sec 16(1) & 16 (3)AT Act 2009	Maximum fine Tk25 lac and suspend the registration or license.

3.1.1 Offences committed by an entity.–

As per section 27 of MLPA-2012, if any offence under this Act is committed by an entity, every proprietor, director, manager, secretary or any other officer, staff or representative of the said entity who is directly involved in the offence shall be deemed to be guilty of the offence, unless he is able to prove that the offence has been committed without his knowledge or he tried his best to prevent it.

Explanation– In this section "director" includes any member of the partnership entity or any of the Board of Directors of the entity, by whatever name called.

3.1.2 Responsibility of Reporting Organizations to Prevent Money Laundering under the laws –

In Bangladesh, compliance requirements for Bank, as reporting organization, are based on Money Laundering Prevention Act 2012(amendment 2015), Anti-terrorism Act-2009 (amendment 2012 & 2013) and circulars or instructions issued by BFIU time to time. According to section 25 of MLPA-2012 (amendment 2015) Banks responsibilities to prevent money laundering are –

a) To maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;

b) To preserve previous records of transactions of any customer's account for at least 5(five) years from the date of closure;

c) To provide with the information maintained under clauses (a) and (b) to BFIU from time to time, on its demand;

d) If any suspicious transaction or attempt of such transaction as defined under clause (z)3 of section 2 is observed, to report the matter as suspicious transaction report' to the BFIU immediately on its own accord.

If any reporting organization violates the provisions of sub-section (1), BFIU may-

a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty-five) lac on the reporting organization; and

b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches, service centers, booths or agents, or as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

If any person or entity or reporting organization fails to pay any fine imposed by BFIU under sections 23 and 25 of this Act, BFIU may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank, and in this regard if any amount of the fine remains unrealized, BFIU may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

If any reporting organization is imposed fine under sub-sections 23 (3), (4), (5) and (6), BFIU may also impose a fine not less than Taka 10 (ten) thousand but not exceeding taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

3.2 Offences under the Anti-Terrorism Act-2009 (Amendment 2013): & Punishments:

Section # 7.3 –

If any person is found guilty of any of the offences mentioned in sub-sections (1), the person shall be punished with an imprisonment for a term not exceeding 20(twenty) years but not less than 4(four) years, and in addition to that, a fine may be imposed equal to twice the value of the property involved with the offence or taka 10 (ten) lac, whichever is greater.

Section # 7.4 –

a) If any entity is found guilty of any of the offences mentioned in the sub-sections(1)-(a) steps may be taken in accordance with section 18 and in addition to that a fine may be imposed equal to thrice the value of the property involved with the offence or taka 50 (fifty) lacs, whichever is greater;
b) The head of such entity, whether he is designated as Chairman, Managing Director, Chief Executive or any other name, shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than four years and in addition to that a fine may be imposed equal to twice of the value of the property involved with the offence or taka 20 (twenty) lac, whichever is greater, unless he is able to prove that the said offence was committed without his knowledge or he had tried utmost to prevent the commission of the said offence.

Section # 16 Duties of Banks–

1. Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through them which are connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to the Bangladesh Bank without any delay.

2. The Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting agency, have been complied with or not.

3. If any reporting agency fails to comply with the provision under sub-section (1) the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank

not exceeding taka 25 (twenty five) lac and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.

4. If the Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of any reporting organization fails to comply with the provision under sub-section (2) the chairman of the Board of Directors, or the Chief Executive Officer, as the case may be, shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding taka 25 (twenty five) lac and Bangladesh Bank may remove the said person from his position, as the case may be, shall inform the competent authority about the subject matter to take appropriate action against the person.

5. If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to subsection (3) or if the chairman of the Board of Directors, or the Chief Executive Officer, whatever they may be called, fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section (4), Bangladesh Bank may recover the amount from the reporting agency or from the account of the respective person by debiting any account maintained in any bank or financial institution or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

3.3. "Safe Harbor" Provision for Reporting under MLP Acts.

3.3.1 The Money Laundering Prevention Acts encourages reporting organizations to report all suspicious transactions by protecting reporting organizations and their employees from criminal and civil liability when reporting suspicious transactions in good faith to the competent authorities.

3.3.2 Section 28 of the Acts provides the "***Safe Harbor***" for such reporting, which is, although any person may be damaged or there remains possibility to be damaged, any criminal or civil or administrative or any other legal action cannot be administered against the reporting organization, or its Board of Directors, or any of its employees.

3.3.3 Despite the above safe harbor, if the reporting organizations fail to report STR/SAR, then they will be subject to punishment under Section 25(2) of the Acts.

3.4. Penalty As per Provisions of TAX related Laws:

3.4.1: Delayed submission/ Non-submission/Wrong submission:

As per clause No. 266(2)(Ga) of Income Tax Act-2023, Fails to file or furnish any information as required under section 200, in which case the Income-tax authority requiring the information under section 200 may impose a fine of Tk.50,000/- (Taka fifty thousand) on such person and, if the failure continues (for non-submission of information), an additional penalty for Tk.500/- (Taka Five hundred) may be imposed for every day during which the failure continues;

3.4.2: Penalty for failure in furnish/provide information and failure to perform/completion of some duties/tasks as per clause No 311 of Income TAX Act-2023:

If any person, without reasonable cause, fails to furnish the information or to perform the following acts, he shall be punished with rigorous imprisonment for a term which may extend up to 1 (one) year or with fine or with both,

3.5 Money Laundering Prevention Rules-2019

The purpose of MLP Rule is to build the legal and regulatory framework for Anti-Money Laundering and combating Financing of Terrorism (AML & CFT) and thus the documents interpret the requirements of the relevant laws and regulations, and how they might be implemented in practice. Here, the practical steps and formalities are illustrated on - how & who to escalate, conduct and execute an investigation under the MLPA law. The Bangladesh Government made Money Laundering Prevention Rules-2019 under the power conferred by Section-29 of the Money Laundering Prevention Act-2012 (Act No. V of 2012) which has been preserved in

MMBPLC Common Folder R:10.10.10.116\ANTI MONEY LAUNDERING\1. BFIU related Policy & Circular\2. National Level AML CFT Acts Rules > Money Laundering Prevention Rules-2019

3.6 **Anti-Terrorism Rules- 2013**

The purpose of the rules is to build the legal and regulatory framework for combating the Financing of Terrorism and thus the documents interpret the requirements of the relevant laws and regulations, and how they might be implemented in practice. Here, the practical steps & formalities are illustrated on how & who to escalate, conduct and execute an investigation under the ATA law. In exercise of the power conferred by section 43 of the Anti-Terrorism Act, 2009 (Act No. XVI of 2009) the Bangladesh Government made Anti-Terrorism Rules, 2013 that has been preserved in the Bank's Common Folder R:*10.10.10.116\ANTI MONEY LAUNDERING\1. BFIU related Policy & Circular\2. National Level AML CFT Acts Rules > Anti-Terrorism Rules-2013*

3.7 Bankers' Books Evidence Act-2021

Different investigation authorities may ask for bank account information under the provision of this law. The schedule 2(1)(DA) of this Act prescribed the authorized areas/ Persons/ organization and terms & conditions regarding disclosure of customer information. The law also states some offences, punishments and trail to prevent unauthorized use & leakage of any information. Bank Official should ensure the compliance of concerned provisions of this law (ACT is Annexure# 18) before disclosing customer information. As now, scope of Law Enforcement Agencies (LEA) has increased, staff must exercise caution and prudently cross check with Head-Office before disclosing any information.

Chapter # 4

Requirements of Anti-Money Laundering Policy

CHAPTER # 4
Requirements of Anti-Money Laundering Policy

4.1.1 AML & CTF Compliance Program

The compliance program of MMBPLC is documented and communicated to all levels of the organization after getting approval of the Management and by its Board of Directors. In developing an AML&CTF compliance program, attention has been paid to the size and range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by the bank. The program includes-

1. Senior management role including their commitment to prevent ML, TF & PF;
2. Internal policies, procedure and controls- it should include Bank's AML & CTF policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self-assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;
3. Compliance structure includes establishment of Central Compliance Committee (CCC), appointment of chief anti-money laundering compliance officer (CAMLCO), branch anti-money laundering compliance officer (BAMLCO);
4. Independent audit function- it includes the role and responsibilities of internal audit on AML & CTF compliance and external audit function;
5. Awareness building program includes training, workshop, seminar for banks employees, member of the board of directors, owners and above all for the customers on AML & CTF issues.

4.1.2 Senior Management Commitment

The most important element of a successful anti-money laundering program is the commitment of Senior Management. Senior Management of MMBPLC is highly committed to the development and enforcement of the Anti-Money Laundering, Anti-Terrorist Financing and Proliferation Financing objectives which can deter criminals from using their facilities for money laundering or financing of terrorism or proliferation financing, thus ensuring that they comply with their obligations under the laws and rules. For the purpose of this policy, Senior Management means the Managing Director & CEO and the Board of Directors of the Bank.

4.1.3. Role of Senior Management (Board of Directors):

As per section 1.2 of the BFIU Circular#26, MMBPLC has its own Policy Manual on AML & CTF –which is approved by the Board of Directors. Similarly as per the Anti-Terrorism Act (ATA), 2009, the Board of Directors, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15 of ATA, which are applicable to the reporting agency, have been complied with or not.

- Approve AML & CFT compliance program and ensure its implementation;
- Issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- Take reasonable measures through analyzing self-assessment report and independent testing report summary;
- Understand ML & TF risk of the Bank, take measures to mitigate those risk;
- CEO or/and MD shall issue statement of commitment to prevent ML, TF & PF in the Bank and if necessary shall also observe the overall status of the compliance issue;
- Ensure compliance of AML & CFT program;
- Allocate enough human and other logistics to effective implementation of AML & CFT compliance program.

4.1.4. Communication of Compliance Program

Senior Management must convey that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of the Bank's Anti Money Laundering Policy the Managing Director & CEO, on behalf of the Senior Management, is sending a statement to all employees every year that clearly sets forth the Bank's policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. The statement evidence indicates the strong commitment of the Bank and its senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing.

4.2.1 Statement of commitment of CEO or MD includes the followings:

- Banks policy or strategy to prevent ML, TF & PF;
- Emphasize on effective implementation of Bank's AML & CFT compliance program;
- Clear indication of balance between business and compliance, risk and mitigating measures;
- Compliance is the responsibility of each employee during their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance;
- Point of contact for clarification in case of any ambiguity arises;
- Consequences of non-compliance as per Human Resources (HR) Policy of the Bank.

4.2.2. Senior Management has accountability to ensure that the Bank's policy, process and procedures towards AML & CFT are appropriately designed and implemented, and are effectively operated to minimize the risk of the Bank being used in connection with ML & TF.

4.2.3 Senior Management must need to ensure the adequacy of the human and other resources devoted to AML & CFT. Moreover, they need to ensure the autonomy of the designated officials related to AML & CFT. Senior Management must take the report from the Anti-Money Laundering Division into consideration which will assess the operation and effectiveness of the Bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner.

4.2.4 Senior Management should adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the Bank.

4.2.5 Senior Management must be responsive of the level of money laundering and terrorist financing risk when the Bank is exposed to and take a view whether the Bank is equipped to mitigate that risk effectively; this implies that decisions on entering or maintaining high-risk business relationships must be escalated to senior management.

4.2.6 Written Anti Money Laundering Policy

- An AML policy must include the following 4 (four) key elements:
  - ➢ High level summary of key controls;
  - ➢ Objective of the policy (e.g. to protect the reputation of the institution);
  - ➢ Scope of the policy (A statement confirming that the AML/CFT policy applies to all areas of the business); and
  - ➢ Waivers and exceptions- procedures for obtaining exemptions from any aspects of the policy should be carefully controlled; and operational controls.

Chapter # 5

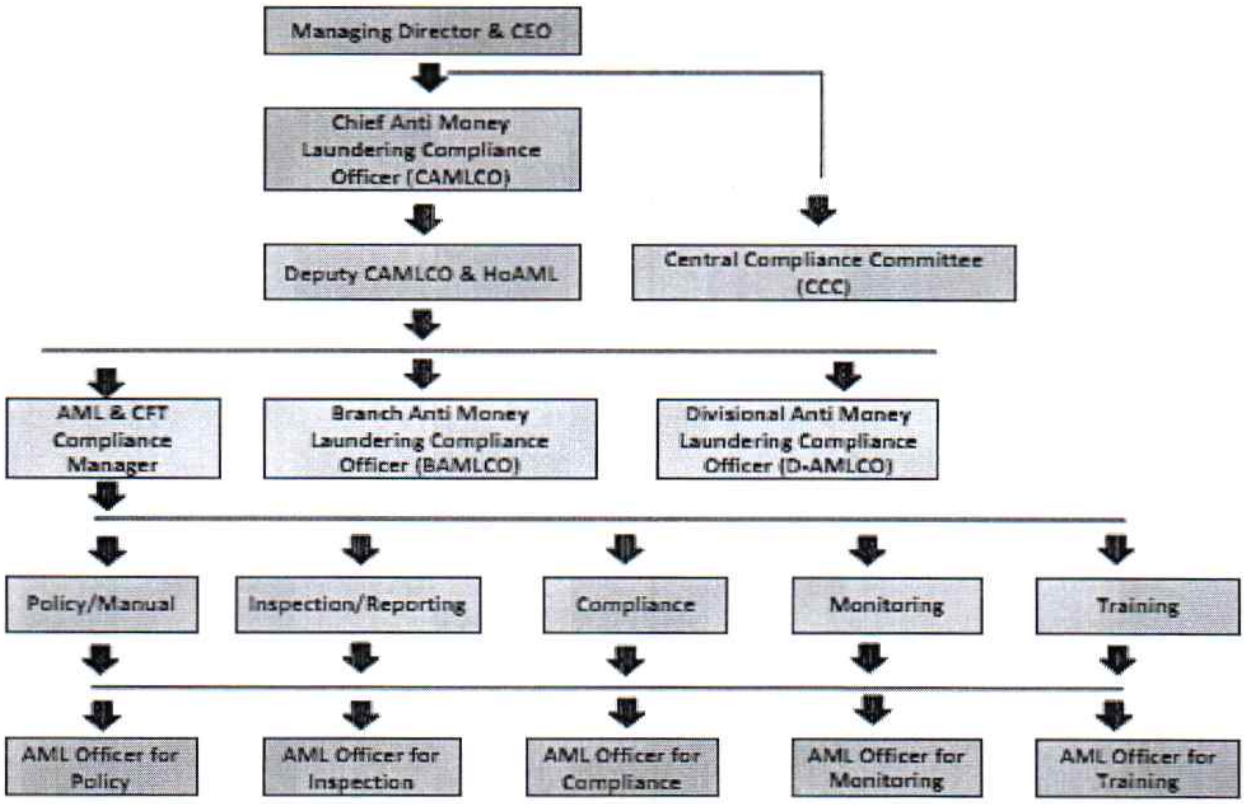
Organizational Structure & Human Resources Division's initiatives

CHAPTER # 5

ORGANIZATIONAL STRUCTURE AND H.R. INITIATIVES

5.1 Organization Structure:

It is very much essential for an organization to build up a proper organogram depicting the position of people working there with their job description and responsibilities for making them accountable to the organization for their activities for successful implementation of any policy. Giving priority and importance of Anti-Money Laundering & Combating the financing of terrorism, MMBPLC has established a separate Anti-Money Laundering Division namely "AML&CFT Division" at Head Office level under supervision of the CAMLCO (Chief Anti-Money Laundering Compliance Officer) and the Division is Headed by the Deputy CAMLCO. Apart from this division, Central Compliance Committee (CCC) is established as a Committee comprising heads of various concerned divisions.



Notes:

* Refers actually to a Committee which is formed and work as per Regulatory prescription, compromising of relevant functional Heads/Deputy to assist the CAMLCO in implementing AML/CTF Agendas. The CCC meets formally at least on Quarterly basis.

Branch Compliance Unit Comprises of key officials - to assist the BAMLCO in implementing AML/CTF Agendas at Branch. The BCU meets formally at least on quarterly basis but practically almost **every day/week** they are informally meeting & executing all Branch issues.

Internal Control & Compliance Division (IC&CD) Conducts Inspections of each Branches & respective Agent Banking Offices/units once a year and on Risk based approach Agent Points.

5.2 Central Compliance Committee (CCC):

Central Compliance Committee is a committee for review of the AML process and makes further recommendation on AML and compliance issues. As per latest directives of BFIU it must be consisted of minimum 7 members including the CAMLCO and the Deputy CAMLCO. For constituting the *CCC* there should be members from General Banking, Operations, IT, HRD, Credit, Retail & Corporate, Foreign Trade, Card Division and information technology department etc. and other related division/ department, but no officials from IC&CD would be the *CCC* member. The *CCC* consists of head of some core divisions of the Bank. The *CCC* sits periodically & at least quarterly to examine and review the existing AML process and its compliance functions; formulate new strategy for implementation of the AML process. If required, the CCC can be called for meeting any time at any numbers. IC&CD will perform their duties regarding prevention of money laundering and terrorist financing *CCC* as independent separate wing.

5.2.1 Responsibilities of CCC:

The committee shall have the following responsibilities:

- To develop and implement the Bank's Policy, Procedure and Strategies in preventing Money Laundering (ML), Terrorist Financing (TF) & Proliferation Financing (PF) and review thereon.
- To ensure a satisfactory compliance on Bank's AML & CFT as per the guidelines.
- To supervise AML Division for the proper implementation of yearly programs on AML & CFT.
- To co-ordinate and monitor Bank's AML & CFT compliance initiatives.
- To co-ordinate the ML & TF risk assessment of the Bank and review thereon.
- To arrange at least 4 meetings in a year; to make necessary decisions and give necessary instructions by reviewing the overall status of the Bank on AML & CFT issues.
- To submit a report to the Managing Director on Half Yearly basis related to AML & CFT issues containing action taken by Bank, implementation progress and recommendations.
- To instruct AML Division to issue instructions, for the Branches to follow on know Your Customer (KYC), Transaction Monitoring, Internal Compliance etc.
- To nominate one employee from each Branch as BAMLCO to ensure Internal Monitoring and Control System.
- To impart training, workshop, seminar related to AML & CFT for the employees of the Bank.
- Committee may incorporate any member in the committee if they feel the necessity.
- Formal minutes of the meeting shall be maintained to document the AML & CFT activities and decisions.
- Any other issues regarding AML & CFT as & when required by the Bank.

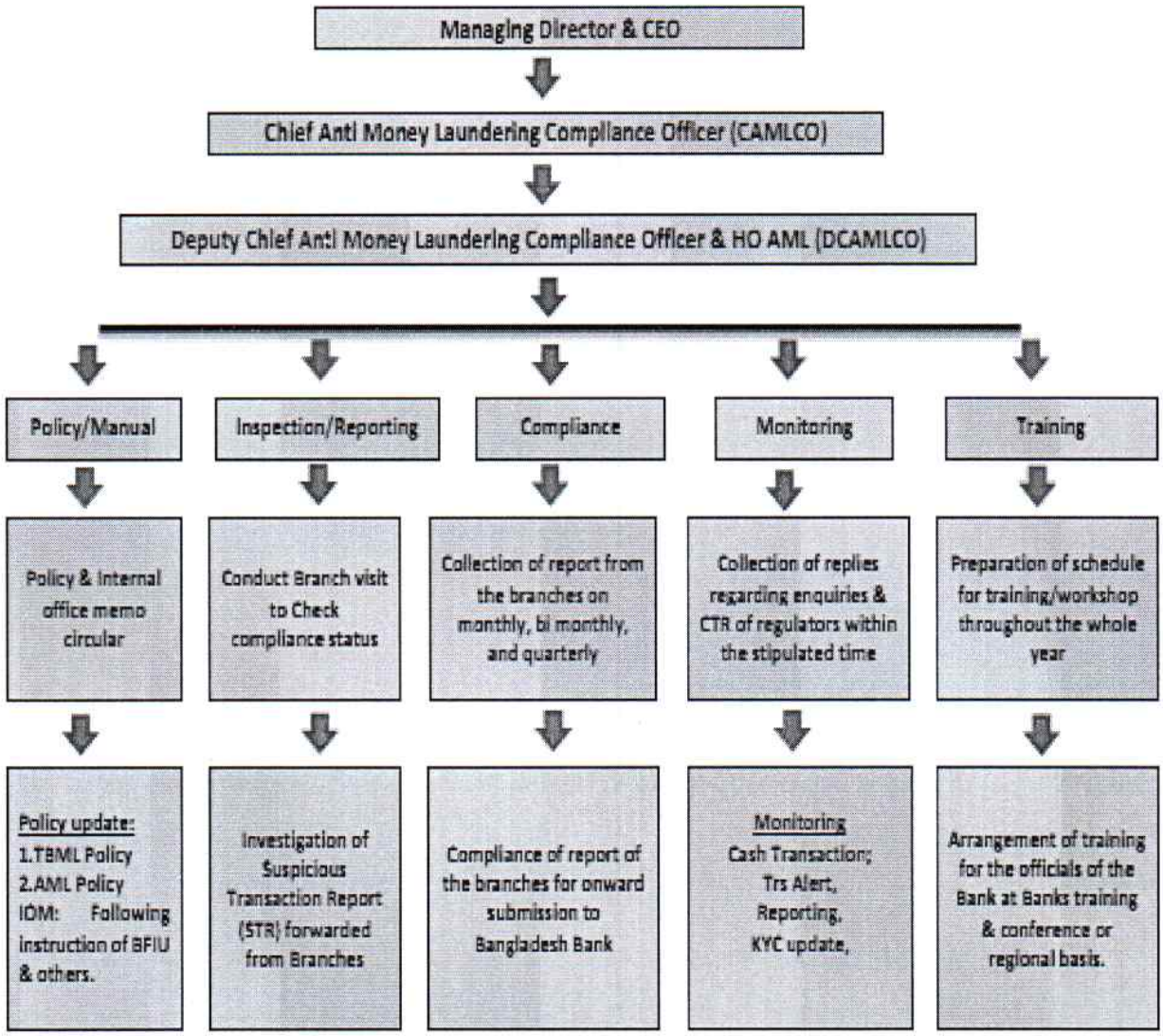
Members of the Central Compliance Committee (CCC) of MMBPLC are as follows:

Sl.	Divisional Portfolio	Position in CCU
1	The CAMLCO of the Bank	Chairman
2	Chief Risk Officer (CRO)	Member
3	Head of International Division	Member
4	Head of Human Resources Division	Member
5	Head of Operations Division	Member
6	Head of Credit Risk Management Division	Member
7	Head of Corporate & Inv. Banking Division	Member
8	Head of Retail Banking Division	Member
9	Head of Trade Services Division	Member
10	Head of ICT Division	Member
11	Head of SME Division	Member
12	Head of Agent Banking Division	Member
13	Head of AML&CFT Division & D-CAMLCO	Member Secretary

AML&CFT Division is the operational entity of *CCC* to ensure AML&CFT compliance issues. Ensure deployment of manpower in AML&CFT Division considering number of branches, business portfolio & product diversity, number of customer and institutional risk. Head of AML&CFT Division will be the Deputy CAMLCO and his rank would not be below of SVP or DGM.

Functional Organogram of AML&CFT Division

Under purview of the MD&CEO and DMD & CAMLCO



5.2.2 **The responsibilities of 'AML &CFT Division':**

a) To supervise, monitor, review and coordinate AML/CTF compliance issues of the Bank;

b) To accommodate the changes of laws/regulations and directives of BFIU and revise its internal policies accordingly;

c) To assist in review of control procedures in the bank to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;

d) To respond to compliance questions and concerns of the staff and advise regional offices/ branches/units and assist in providing solutions to potential issues involving compliance and risk;

e) To monitor the business through self-testing for AML/CTF compliance and take any required corrective action;

f) To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;

g) Preparing an overall assessment report after evaluating the self-assessment reports received from the branches and submitting it with comments and recommendations to the chief executive of the bank;

h) Preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Audit Department on that particular quarter;

i) Periodical reporting to the higher authority and the regulators;

The coordination & part execution of the responsibilities of the *CCC* will be accomplished by the 'AML& CTF Division.

5.2.3 Manpower for Anti-Money Laundering & Combating Financing of Terrorism Division (AML&CFTD)

The Bank shall ensure adequate human resources and other logistic support based on the size and nature of the Bank. The division shall be established consisting appropriate number of employees. The Head of the Division will be the Deputy CAMLCO of the Bank. The employee of the AML&CFTD must have enough knowledge on AML & CFT measures of Bangladesh including MLPA, ATA and rules and instructions issued by BFIU or Bangladesh Bank.

5.3 Separation of AML&CFTD from Internal Control & Compliance (ICC)

To ensure the independent audit function in the Bank AML&CFTD should be completely separated from internal audit or compliance and control (ICC). In this regard ICC also examines the performance of AML&CFT Division and the Bank's AML & CFT compliance program. To ensure this autonomy there shall not be any member from ICC to AML and vies-a-vies; but there should be enough co-ordination and co-operation in performing their responsibility and information exchange. Also no official from ICCD can be a member of the CCC. There should not be any impediment to transfer employee from ICC to AML&CFTD and vis-à-vis but no one should be posted in these 2 (two) departments/units at the same time. Both AML&CFTD and ICCD will independently perform their respective jobs regarding AML & CFT issues.

5.4 Appointment of Chief AML/CFT Compliance Officer (CAMLCO)

The Managing Director of the Bank will nominate a Chief Anti-Money Laundering Compliance Officer (CAMLCO) at its Head Office with sufficient authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures. The CAMLCO will directly report to the Chief Executive Officer/Managing Director. If CAMLCO is entrusted with any other responsibilities, it must be ensured by the bank management that AML-CTF function will not hamper. In case of change of CAMLCO it must be informed to BFIU immediately.

5.4.1 Position of CAMLCO and Deputy CAMLCO

The Chief AML/CFT Compliance Officer will be the delegated authority/ Reporting Head of AML&CFT Division whatever its name is. In this case, 'High official' will be considered as an official up to 2 (two) steps below of the Managing Director & CEO. MBBL shall inform of any change of the CAMLCO to BFIU without delay. It will also ensure the involvement of CAMLCO regarding AML & CFT activities in case of assigning him to other duties of the bank. The position of the Deputy CAMLCO should be at the minimum rank of DGM/Senior Vice President as per BFIU directive. As per BFIU Circular the Deputy CAMLCO will act as the Head of AML&CFT Division.

5.4.2 Qualification and Experience

The CAMLCO and the Deputy CAMLCO must have good knowledge in AML/CTF related laws, regulation and relevant guidelines/rules/circulars issued by the competent authority from time to time. The CAMLCO should have a working knowledge of the diverse financial products offered by the financial

institutions with an added qualification of relevant certification, like CAMS. The person could have obtained relevant financial institutional and compliance experience as an internal auditor or regulatory examiner, with exposure to different financial institutional products and businesses. Product and financial institutional knowledge could be obtained from being an external or internal auditor, or as an experienced operational staff. The CAMLCO and DCAMLCO have to have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML & TF. Job Descriptions of the relevant staff have been prepared & shared with HR.

As per BFIU Guidelines (SEP15):

5.4.3 Authorities and Responsibilities of the CAMLCO

5.4.3.1 *The CAMLCO has the following Authorities:*

- CAMLCO is able to act on his own Authority;
- Without taking any prior permission from /with MD or CEO , CAMLCO can submit of STR/SAR and any document or information to BFIU;
- He/She shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He/ She must have access to any information of the Bank;
- CAMLCO shall ensure his/her continuing competence.

5.4.3.2 *The CAMLCO has the following Responsibilities:*

- CAMLCO must ensure overall AML & CFT compliance of the Bank;
- oversee the submission of STR/SAR or any document or information to BFIU in time;
- maintain the day-to-day operation of the Bank's AML&CFT compliance;
- He/She shall be liable to MD , CEO or BoD for proper functioning of CCU;
- He/She shall review and update ML & TF Risk Assessment of the Bank;
- Ensure that corrective actions have taken by the Bank to address the deficiency identified by the BFIU or Bangladesh Bank.

5.4.5 Functions of the Chief Anti Money Laundering Compliance Officer (CAMLCO) will be:

Key Responsibilities of the CAMLCO	Frequency
1. Monitor, review, coordinate application and enforcement of the Bank's compliance policies including Anti Money Laundering Policy, Customer Acceptance Policy, Know Your Customer Policy and Anti-Terrorism Financing Policy. These will include: an AML Risk Assessment; practices, procedures and controls for account opening; KYC procedures; ongoing account/ transaction monitoring for detecting suspicious transactions/account activity, and a written AML training plan.	On-going
2. To monitor changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit that may require revisions to the Policies and making these revisions.	On-going
3. Ensure the Bank's Policies are complete and up-to-date; maintain ongoing awareness of new and changing business activities and products and identify potential compliance issues that should be considered by the Bank.	On-going
4. Respond to compliance questions and concerns of the staff and advice branches/ divisions and assist in providing solutions to potential issues involving compliance and money laundering and terrorist financing risk.	As required
5. Actively develop the compliance knowledge of all staff, especially the compliance personnel. Develop and conduct training courses in the Bank to raise the level of awareness of compliance in the Bank.	On-going

6. Develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, Branch/Division Heads and Compliance resources to assist in early identification of compliance issues.	On-going
7. Assist in review of control procedures in the Bank to ensure legal and regulatory compliance and in the development of adequate and sufficient Independent Testing Procedures to prevent and detect compliance lapses.	On-going
8. Monitor the Bank's Self-Assessment for AML&CFT Compliance and any corrective action.	Half Yearly
9. Inspect branches and concerned divisions of Head Office regarding anti-money laundering and terrorist financing compliance.	As required
10. Manage the STR & SAR Process: a. Review the transactions referred by branch or divisional compliance officers as suspicious. b. Review the Transaction Monitoring reports. c. Ensure that internal Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) - are prepared when appropriate, - are accompanied by documentation of the branch's decision to retain or terminate the account as required under the Policy, - are advised to other branches of the Bank who are known to have a relationship with the customer, - are reported to the Managing Director & CEO and/or the Board of Directors of the Bank when the suspicious activity is judged to represent significant risk to the Bank, including reputation risk. d. Manage the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultation.	On-going
11. Ensure timely Anti Money Laundering and Terrorist Financing reporting and compliance to Bangladesh Financial Intelligence Unit, including CTR, Central Taskforce Biborony, Independent Testing Procedure, Self-Assessment Report etc. as per specific schedule.	Monthly, & Half-Yearly
12. Ensure timely compliance of Bangladesh Financial Intelligence Unit (BFIU) Inspection Team, Internal Audit Team and External Audit Team.	As required
13. Ensure that a message from the MD & CEO is issued on an annual basis to all officials of the Bank highlighting the commitment of senior management of the Bank to the development and enforcement of the Anti-Money Laundering objectives as per Section 5.1 of this Policy.	Annually
14. Maintain liaison with the delegates of foreign Banks, local Banks, Bangladesh Bank and various law enforcement agencies.	On-going
15. Collect and review KYC profiles of Correspondents through FI & Correspondent Relationship Banking Department at Head Office.	On-going
16. Prepare/Complete KYC Questionnaires of MMBPLC for correspondents.	As required
17. Arrange AML&CFT training programs for the officials of different scheduled Banks of different districts as and when advised by Bangladesh Financial Intelligence Unit.	As required
18. Perform Bank Account Enquiry function as requested by Bangladesh Financial Intelligence Unit (BFIU) on different persons/companies.	As required
19. Perform Bank Account Freeze function as requested by Bangladesh Financial Intelligence Unit (BFIU) on different persons/companies.	As required

5.5 Deputy Chief Anti Money Laundering Compliance Officer (Deputy CAMLCO)

The Bank shall nominate one or more executive in the rank of Senior Vice President or equivalent and above as Deputy CAMLCO. CAMLCO may choose to delegate duties or rely on the Deputy CAMLCO in absence of CAMLCO for their practical performance whilst remaining responsible and accountable for

the operation of the designated functions. The Deputy CAMLCO shall be the Head of Anti Money Laundering & Combating Financing of Terrorism Division and will report directly to the CAMLCO.

5.6.1 Appointment of 'Divisional Anti Money Laundering Compliance Officer (D-AMLCO)':

Divisional Head/Deputy Head/Key responsible Person may be selected as **'Divisional Anti-Money Laundering Compliance Officer (D-AMLCO).**

DAMLCO will perform the duties as **'Divisional Anti Money Laundering Compliance Officer (DAMLCO)"** of **Business/Operational Units**, Head Office in addition to his/her present responsibilities. Accordingly, he/she will supervise and monitor the activities of AML&CFT compliance of the Division.

- **Scope and Purpose of the Position:** To ensure AML & CFT Compliance of the Division
- **Reporting/Supervision Channel for this Purpose:** The CAMLCO and Head of AML&CFTD & D-CAMLCO

5.6.2: Job Description of 'Divisional Anti Money Laundering Compliance Officer' (D-AMLCO):

Job Description of Divisional Anti-Money Laundering Compliance Officer (D-AMLCO) of a **Division** of the Bank may be as follows, which may be further reviewed and settled by respective Central Compliance Committee (CCC) member or the CAMLCO:

1. Have updated knowledge about AML&CFT related rules & regulations related to International trade (local & international) and Financial Crime & Compliance related issues. Have **adequate understanding** about CDD/EDD/MEDD for Credit/Foreign Trade customers, their risk grading and other requirements as per Credit Manual/Foreign Trade Operation Manual and also about Credit backed Money Laundering (CBML) indicators/alerts and Trade Based Money Laundering (TBML) indicators/alerts;
2. Have **update knowledge** about AML&CFT related policies/guidelines, circular and instructions given by BFIU and AML&CFTD, Head Office; Impact special focus on the understanding and implementation of BFIU Master Circular and other instruction circulars;
3. Ensure **fulfilment of requirements** as per 'MMBPLC Policy on Prevention of Money Laundering & Combating Terrorist Financing (P-ML&CFT)' and 'MMBPLC Guidelines for Prevention of Trade based Money Laundering (P-TBML)' and ensure necessary update/revision at regular interval;
4. Assist the Head of the Division in setting up **Action Plans** against Prevention of ML, TF & TBML corresponding to trade business of the Bank and take measures to execute;
5. Identify Key **ML/TF risks and challenges** associated with trade business and also financial crime compliance in the AML&CFT perspective in consultation with AML&CFT Division and initiate measures to mitigate those risk;
6. Recheck or revalidate information/data as provided by the Branches in the proposal/activities/assignment about AML&CFT Compliance issues (EDD of customers related issues or other activities)
7. Recheck or revalidate information/data (on random sampling basis on RBA) relating to **person/entity screening** (Director/Beneficial Owner/Buyer/Supplier/Indenter/Vessel/Port/Country of Origin /Product etc. check through reliable sources) prior to escalate proposal/serve the purpose to the Management for approval;
8. Ensure analysis of data/information (EDD of customers & its activities & audited/unaudited financials) as stipulated in the credit/loan/business proposal/LC/LG/functional assignment from the AML point of view (consider any predicate offense prevail in the business/activity of the entity whether really exists or only creates suspicion)
9. Take effective measures to **establish procedure** to check prevailing CBML (intension/suspicion of ML&FT) /TBML technique (Under/over invoicing of goods, under/over/phantom shipment, false declaration and so forth) and keep/collect records of such practices;
10. Ensure periodical monitoring of the prevailing red flags as raised against credit related issues and trade issues/transactions at Branches and Head Office and identify suspicious

transactions/activity. Also report STR/SAR to AML&CFTD, if suspicion is established through investigation.

11. Ensure following up the **media report** regularly on terrorism, terrorist financing or others offence and find out any relationship of the involved person; if so, the DAMLCO should initiate a SAR/STR to AML&CFTD.
12. Arrange **quarterly meeting** with the officials of the division on different AML/CFT/CBML/TBML compliance issues and status of compliance thereof; Keep records/**minutes** in appropriate manner and forward a copy of minutes to AML&CFT Division for their record and regulators inspection purpose;
13. Participate in the AML meetings/CCC meeting (if required & invited) to discuss various credit/trade/assignment based ML issues and implement CCC decisions from time to time where applicable;
14. Ensure **record keeping** as per the requirements of regulatory guideline;
15. Ensure completion of **formal/refreshers training** for all officials of your division on AML&CFT compliance and prevention of Trade based Money Laundering (TBML)/CBML in consultation with AML&CFT Division, HR Division on yearly basis (In-house & external) or as and when necessary;
16. Assess ML & TF risk under banking business profile of the Bank through **RISK Register** as per Policy Guidelines and adopt appropriate mitigation process; (Submit the Risk Register to AML&CFTD on yearly basis)
17. Extend full **cooperation to BFIU**/IC&CD Audit/Inspection/DBI, Bangladesh Bank/other Competent Authority and take appropriate action for timely mitigation; Acts as liaison and be available to discuss with D-CAMLCO/ CAMLCO or the BFIU matters pertaining to the AML/CFT functions of the Bank;
18. Ensure that **corrective action** have been taken by the division to address the deficiency identified by the BFIU or Bangladesh Bank from time to time;
19. Ensure compliance and implementation of other instructions as and when issued by BFIU and/or the CAMLCO/AML&CFTD, Head Office;

5.7 Branch Level Organization Structure

For the implementation of all existing acts, rules, BFIU's instructions and Bank's own policies on Preventing Money Laundering & Terrorist Financing, HRD in consultation with the CAMLCO shall nominate an experienced Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch.

Branch Manager, Branch Operations Manager of the branch or a high official experienced in general Banking shall be nominated as the BAMLCO. The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and Bank's own policies on preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in the appointment letter.

5.7.1 Appointment of Branch Anti Money Laundering Compliance Officer (BAMLCO)

The Branch Manager/ Branch Manager Operations/GB In-charge/Credit In-charge/any responsible experienced official of every branch shall be designated as the Branch Anti Money Laundering Compliance Officer (BAMLCO). BAMLCO should have a clear understanding about AML & CFT Acts, Rules & Regulations; BFIU Instructions and Bank Policy regarding AML & CFT issues. The BAMLCO shall implement and enforce Anti Money Laundering Policies, Procedures and Measures within the branch and shall report directly to Chief Anti Money Laundering Compliance Officer (CAMLCO) at Head Office through Head of AML&CFT Division regarding all AML&CFT matters. Branch Manager shall have overall supervision ensuring that the AML & CFT program is effective within the branch. All other officials of the branch shall also assist BAMLCO to this effect. All staff engaged in each branch at all levels must be made aware of the identity of the respective BAMLCO of the branch.

5.7.2 *Branch Compliance Unit (BCU)*: Every branch shall create a Branch Compliance Unit (BCU) consisting at least with the following members:

1. Branch Manager/Head of Branch

2. Branch Manager Operations
3. General Banking In charge
4. Credit In charge
5. Foreign Exchange In charge
6. Cash In Charge (Teller)

5.7.3 BCU Quarterly Meeting: The BAMLCO shall arrange quarterly meetings with Branch Compliance Unit (BCU) to review the Anti-Money Laundering compliance activities of the branch at the end of every quarter and shall take effective measures on the following matters after reviewing the compliance of the existing acts, rules and regulations, BFIU's instructions on Preventing Money Laundering & Terrorist Financing:

- Know Your Customer,
- Transaction monitoring & Investigation
- Identifying and reporting of Suspicious Transactions,
- Implementation of Local Sanction List along with the resolutions of UN Sanctions Security Council,
- Self- Assessment Related activities,
- Record keeping,
- Training.

5.7.4 BCU Meeting Minutes: The BAMLCO shall maintain minutes of the meeting in documented form and shall send a copy of the minutes to AML&CFT Division in standard & updated format. A copy of the minutes should be forwarded to the CAMLCO along with Self-Assessment Report at Head Office for their information & records. A format is annexures (**Annexure-....)**

5.8 Individual Responsibilities (Branch Officials):

Whilst complying with rules and regulations is the responsibility of each individual in the Bank in the normal course of their assignments, the following individuals and functions, along with the CAMLCO, all play vital roles in the effectiveness of the Bank's AML program:

5.8.1 *Branch Manager (BM)* *(May be appointed as BAMLCO, in that case BAMCLO's responsibility will be added):*

Key Responsibilities of the Branch Manager	Frequency
1. Owner of the business & compliance for the branch. Main objective is to achieve numbers towards enhancement of Bank's profit in strict compliance with applicable AML and ATF laws, regulations and policies.	On-going
2. Ensure that the AML and ATF program are effective within the branch.	On-going
3. Issue job description to all individuals as per their nature of activities.	On-going
4. Arrange quarterly meeting of the Branch Anti Money Laundering Compliance Committee (BAMLCC) to review the AML and ATF compliance status of the branch at the end of every quarterly and maintain minutes in documented form.	Quarterly
5. Perform half yearly Self-Assessment on AML performance of the branch and ensure compliance and any corrective action.	Half yearly
6. Ensure good rating of the Independent Testing Procedure (ITP) conducted on the AML&CFT Compliance of the branch by internal auditors as well as Bangladesh Bank inspectors.	On-going
7. ***Job Rotation***: Maintaining proper communication with HR and other Divisions at Head Office for timely transfer of all Branch officials including the Branch Manager him/herself once in every 2 or 3 years[2].	On-going
8. ***Leave Management***: Ensure that all branch officials including the Branch Manager him/herself have taken 15 continuous days leave at a time each year as mandatory leave[3].	On-going

5.8.2 Role & Responsibility *Branch Anti Money Laundering Compliance Officer (BAMLCO):*

Key Responsibilities of the BAMLCO	Frequency
1. Check the complete documentation of Account Opening, Maintenance and Closing. a. Check the AOF is properly. b. Check whether all required documents have been collected and ensure that the KYC of all customers have been performed properly and for the new customer KYC is being done properly. c. Comply with related policies, manuals and circulars meticulously.	Daily
2. Ensure that the UN Security Council and domestic sanction list ***(see at Annex-11)*** checked properly before opening of account and while making any international transaction.	Daily
3. Keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction.	On-going
4. Ensure regular transaction monitoring to find out any unusual transaction (In case of an automated Bank, the Bank should follow a triggering system against transaction profile or other suitable threshold. In case of a traditional Bank, transaction should be examined at the end of day against transaction profile or other suitable threshold. Records of all transaction monitoring should be kept in the file).	On-going
5. Review cash transaction to find out any structuring.	On-going
6. Review of CTR to find out Suspicious Transaction Report (STR)/Suspicious Activities Report (SAR).	Monthly
7. Follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so, BAMLCO should make an STR/SAR.	As required
8. Reports any Suspicious Transaction, Suspicious Activity (STR/SAR), Structuring and Media Report to the CAMLCO/AML&CFTD.	As required
9. Ensure the checking of UN sanction list before making any foreign transaction.	On-going
10. Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction.	On-going
11. Arrange quarterly meeting of the Branch Anti-Money Laundering Compliance Committee (BAMLCC) to review the AML&CFT Compliance status of the branch at the end of every quarter, maintain minutes in documented form and send a copy to the AML Division.	Quarterly
12. Perform Half Yearly Self-Assessment on AML performance of the branch and ensure compliance and any corrective action and submit the report to the CAMLCO.	Half Yearly
13. Accumulate the training records of branch officials and take initiatives for AML training to branch staff including reporting to AML&CFTD, HR and Learning & Talent Development Center.	As required
14. Ensure all the required information and document are submitted properly to AML&CFTD and any freeze order or stop payment order are implemented properly.	As required
15. Submit branch returns including CTR, Structuring, KYC Exception Report, Money Movement reports etc. to the AML&CFTD as per specific schedule.	Monthly, & Half Yearly
16. Communicate the updated policies including AML and CFT laws/regulations to all staff.	On-going
17. Ensure that the branch is maintaining AML & CFT files properly and record keeping is done as per the requirements of chapter 7.	As required
18. Ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.	As required

19. Audit/Inspection related activities including timely compliance of the same:	
a. ***During Audit (Internal or External)/Inspection (Bangladesh Bank)***: When audit/ inspection teams visit a branch, BAMLCO will be the coordinator. Whenever any document/statement/files/registers are required by the audit/inspection team, BAMLCO has to inform the BM/Head of Branch, who shall arrange for supply of the same.	Adhoc
b. ***After Receiving the Audit/Inspection Report***: Distribute the report to respective Department or any other related wing of Head Office with mentioning a deadline prior to the deadline of the main report.	
c. ***Continuous Monitoring about the progress of Compliance to the Report***: In case of any deviation, inform Branch Manager or related Head of Division immediately.	
d. ***Compliance of All Parts and Send to AML&CFTD within Stipulated Time Frame***: The response should be vetted by respective BAMLCO and Branch Manager.	

5.8.3 Role & Responsibilities of GBCO (General Banking Compliance Officer)

To enhance the effectiveness of the AML/CFT program at the branch level, an officer of the General Banking Department of each branch of the Bank, preferably in charge of the General Banking Department, shall be designated as the General Banking Compliance Officer (GBCO) for their respective branch. The GBCO will have specific duties and responsibilities related to AML/CFT compliance. The nomination of the GBCO shall be the responsibility of the Branch Compliance Unit (BCU) and this information must be promptly communicated to the Anti-Money Laundering Division (AMLD) at the Head Office in Dhaka. He will assist the BAMLCO to ensure General Banking related AML/CFT Compliance of the Branch.

Sl.	Key Responsibilities of General Banking Compliance Officer (GBCO)	Frequency
1	Perform due diligence on prospective clients prior establish any new relationship/opening an account. Evaluate the customer's risk profile (low/high).	Daily
2	Be diligent regarding the identification of customer/accountholder(s) and the source of funds related to the account. Verify beneficial ownership for customers.	On-going
3	Ensure KYC forms are filled accurately and updated. Ensure all required documentations are completed satisfactorily.	Daily
4	Compliance with AML/CTF laws and regulations, AML/CFT policies and procedures has been maintained to mitigate operational risk.	As required
5	Complete, update and monitoring the KYC and TP for the new customer and existing customers.	Daily
6	Ensure the transaction monitoring process and keep record.	On-going
7	Ensure Bank Account enquiry/freeze/unfreeze etc. as when received from BAMLCO/AML & CFTD.	On-going
8	Identify politically exposed persons (PEPs) and high-risk customers.	As required
9	Observe and report unusual or suspicious transactions (e.g., large cash deposits, frequent transfers).	As required
10	Raise flag inconsistencies between customer profile and transaction behavior.	On-going
11	Ensure records are stored securely and are retrievable for audits or investigations.	On-going
12	Escalate suspicious transactions to the bank's BAMLCO/AML compliance officer or designated authority.	As required
13	Cooperate with internal investigations and provide necessary documentation.	As required
14	Stay updated on AML policies, typologies, and red flags.	As required
15	Avoid tipping off customers about investigations or reports.	On-going
16	Participate in regular AML training programs.	As required

5.8.4 Role & Responsibilities Cash Compliance Officer (CCO)

BAMLCO is required to appoint an officer from the Cash Department, preferably the department In-Charge, to act as Cash Compliance Officer (CCO) of the branch shall undertake the following roles and responsibilities to ensure the effective implementation of AML/CFT compliance and the prevention of money laundering and terrorist financing within the branch under the guidance of BAMLCO.

Sl.	Key Responsibilities of the Cash Compliance Officer (CCO)	Frequency
1	Be diligent at the time of customer transactions for the purpose of prevention of money laundering, fraud etc.	Daily
2	Verify customer identity before transactions especially for large cash deposits or withdrawals.	On-going
3	Ensure proper documentation and KYC (Know Your Customer) procedures are followed. Verify beneficial ownership for customers.	On-going
4	Identify and report structuring (smurfing) where large transactions are broken into smaller ones to avoid detection.	As required
5	Be alert to high-risk customers or jurisdictions	On-going
6	Maintain accurate records of transactions, customer interactions and identification documents.	On-going
7	Maintain confidentiality and avoid tipping off customers about investigations.	As required
8	Reports any suspicious activity to the BAMLCO/AML & CFTD.	As required
9	Promote a culture of compliance among junior staff and peers.	On-going
10	Document and escalate concerns as per internal AML protocols	As required
11	Ensure attend AML/CFT training sessions to stay updated.	As required
12	Ensure records are stored securely and are retrievable for audits or inspections.	On-going
13	Follow AML/CFT guidelines issued by Bangladesh Bank and other regulatory bodies.	As required
14	Flag suspicious or incomplete customer profiles for further review. Ensure timely reporting and resolution of flagged issues.	As required

5.8.5 Role & Responsibilities Credit Risk Compliance Officer (CRCO)

In the modern banking landscape, the fight against money laundering and terrorist financing has become a cornerstone of regulatory compliance. To ensure effective implementation of prevention CBML at the grassroots level, BAMLCO appoint designated Credit In-Charge as Credit Risk Compliance Officer (CRCO). The CRCO act as the first line of defense in identifying, monitoring and reporting suspicious financial transactions/activities of borrowers/loan account. CRCO and other officers of credit division are expected to conduct proper customer due diligence (CDD), monitor transactions and escalate red flags to the BAMLCO.

Sl.	Key Responsibilities of the Credit Risk Compliance Officer (CRCO)	Frequency
1	Ensuring accurate identification and verification of all loan applicants go through complete KYC (ID verification, address verification, beneficial ownership for businesses). Validate authenticity of submitted documents and screen for forged or mismatched information.	On-going
2	Assessment and review of Credit necessary CDD/EDD/PEP/IP/Exception approvals and place for approval of CAMLCO/DCAMLCO, as delegated.	On-going
3	Ensure Sanctions and screening that no loan is approved before clearing all screening results against: UN Sanctions, OFAC, Local FIU lists, Bank's internal blacklists etc.	On-going
4	Review adverse news or reputational risks associated with the borrower.	As required
5	Ensure reviewing and approving escalated transaction monitoring alerts from loan, bad loan and fund diversion and recommending appropriate measures to BAMLCO/AMLD or relevant authority.	On-going
6	CBML alert mitigation; analyzing the reports, triggering the anomalies and regular follow-up, escalating risk issues, providing approvals and ensuring proactive reporting.	On-going
7	Ensure all loan processing follows internal AML/CFT frameworks.	On-going

8	Enhanced Due Diligence (EDD) for High-Risk Customers: • Obtain additional financial documents and explanation of source of funds. • Perform site visits to verify the legitimacy of business operations. • Assess ownership structure for possible shell or front companies. • Seek approval from Compliance or Senior Management where required.	As required
9	Ensure the loan is aligned with the borrower's cash flow capacity, the business has genuine economic activity and financials are not artificially inflated.	On-going
10	Ensuring use of disbursed loans are used for the stated purpose.	On-going
11	Ensuring monitor of disbursed loan are not used for: quick withdrawal of full loan amount, transfer to unrelated third parties, usage in high-risk jurisdictions Investment in non-declared businesses and repayments made by unrelated third parties.	On-going
12	Continuously monitor customer behavior throughout the loan lifecycle; review changes in business activity, ownership, or transaction patterns; track unusual turnover or circular movement of funds after loan approval.	On-going
13	Assemble data and prepare periodic and special reports, manuals and correspondence to escalate issues to BAMLCO/AML&CFTD.	On-going
14	Support audit team at the time of systems check inspection and relevant correspondences with regulators, Bangladesh Financial Intelligence Unit and AML&CFTD.	As required
15	Reports any suspicious activity to the BAMLCO/AML & CFTD.	As required
16	Participate in regular AML training programs.	As required

5.8.6 Role & Responsibilities of Trade Compliance Officer (TCO)/TSD-TCO

In order to ensure strong & effective compliance regarding prevention of Trade Based Money Laundering of the Bank, Foreign Trade In-Charge of each AD Branch/ Head of TSD/ OBU In-Charge shall be designated as BTCO/TSD-TCO/OBU-TCO of the Bank. BTCO/TSD-TCO/OBU-TCO of the Bank shall help to implement the Policy for Prevention of Trade Based Money Laundering of the Bank. BTCO/TSD-TCO/OBU-TCO of the Bank will perform following role/responsibilities for preventing ML, TF & PF especially through Trade:

Sl.	Key Responsibilities of the Trade Compliance Officer - Trade Service Division	Frequency
1	Ensure that Risk Assessment of new trade customers is being performed properly before initiating any trade transactions.	On-going
2	Ensure that Trade Transaction Profiles (TTP) of all trade customers is being performed properly.	On-going
3	Ensure that the Trade related CDD/EDD of all Trade customers is being performed properly.	On-going
4	Ensure that the review and assessment of all Trade Customers is being performed properly.	As required
5	Ensure that the level-1 officials of your branch/units are performing their roles & responsibilities at the transaction level for risk assessment & mitigation against all trade transactions.	As required
6	Ensure that the Sanction Screening against all related parties of all trade transactions is being performed properly.	On-going
7	Ensure that the Price Verification of the goods/services of all trade transactions is being performed properly.	On-going
8	Ensure that the Vessel tracking against trade transactions is being performed properly	On-going
9	Ensure that the ongoing Trade Transaction Monitoring is running to find out unusual trade transaction.	On-going
10	Ensure that all the employees of Trade Department of the branch/OBU/CTSD are well aware and capable to identify any unusual trade transaction or any unusual attempt by trade customer.	As required
11	If found any trade transaction or any attempt of trade customer is unusual, the BTCO/OBU-TCO/TSD-TCO shall make an STR/SAR through BAMLCO of the Branch/directly to AML&CFT Division.	As required

12	Ensure that the branch is maintaining files and keeping records on the files properly in accordance with the Policy for Prevention of Trade Based Money Laundering of the Bank: 1) Branch Trade Compliance Officer File 2) Trade Customer Risk Assessment File 3) Trade transaction Profile File 4) Review on Risk Assessment File 5) Vessel Tracking File 6) Price Verification File 7) Sanction Screening File 8) Trade Transactions Monitoring File 9) Adverse Media News on Trade File 10) Trade Alert Escalation File 11) SAR/STR related to Trade 12) Brach Trade officials and Training update File 13) Trade Related Circulars File 14) Any others File if you required.	On-going
13	As a level 2 official at Trade Transaction Level according to related section of the Policy for Prevention of Trade Based Money Laundering, your responsibilities as under: I. Review and examine the TBML Alerts raised by level 1. II. Review Trade Transaction Profile (TTP) on certain Alerts. III. Disambiguate with proper rationale and justification. IV. If not disambiguate the Alerts, escalated to Level 3 properly. V. Documentation properly.	On-going

5.8.7 Role & Responsibilities of Sub-Branch Compliance Officer (SBCO)

A responsible officer of the **Sub-Branch**, preferably the Sub-Branch In-Charge or an experienced official, shall be nominated as the Sub-Branch Compliance Officer (SBCO) for AML/CFT compliance. The nominated officer must have sufficient knowledge of the relevant laws, Bangladesh Financial Intelligence Unit (BFIU) instructions, UN and domestic sanctions, and the AML/CFT compliance Program of the Bank.

The SBCO shall conduct quarterly AML/CFT meetings with other officials of the Sub-Branch and ensure effective implementation of AML/CFT measures, including:

- Know Your Customer (KYC) compliance,
- Transaction monitoring,
- Identification and reporting of Suspicious Transactions,
- Compliance with UN Security Council Resolutions and domestic sanctions,
- Conduct of self-assessment exercises,
- Proper record-keeping, and
- Staff training on AML/CFT.

Sl.	Key Responsibilities of the Sub-Branch Compliance Officer (SBCO)	Frequency
1	Ensure that KYC procedures for all new and existing customers are properly completed.	Daily
2	Verify UN Security Council and domestic sanctions lists before opening accounts or executing international transactions.	On-going
3	Monitor dormant accounts and ensure no withdrawals occur without full compliance with BFIU instructions.	On-going
4	Conduct regular transaction monitoring to detect unusual or suspicious activities: ○ Automated sub-branches should utilize system-generated triggers based on transaction profiles or thresholds. ○ Manual sub-branches should examine transactions daily against customer profiles or thresholds. ○ Maintain records of all monitoring activities.	On-going

5	Review cash transactions to detect structuring or attempts to evade reporting requirements.	On-going
6	Review CTRs to identify potential STR/SARs and report to AMLD.	As required
7	Ensure all sub-branch officers are trained and capable of detecting unusual transactions or suspicious activities.	On-going
8	Compile the sub-branch's self-assessment reports and coordinate quarterly meetings.	As required
9	Maintain comprehensive training records of sub-branch Officers and facilitate training programs in coordination with HR and the Training Academy.	As required
10	Ensure timely submission of required information and documents to AMLD and implement any freeze or stop-payment orders.	As required
11	Monitor media reports related to terrorism, terrorist financing, corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping, or other predicate offenses; assess any links with sub-branch customers or transactions, and file STR/SAR if needed.	On-going
12	Ensure corrective actions are taken to address deficiencies identified by BFIU or Bangladesh Bank.	As required
13	Ensure proper maintenance and record-keeping of the following AML/CFT files at the sub-branch: • CTR Qualifying Data File (Monthly) • STR File • Self-Assessment File (Half-Yearly) • AML/CFT Meeting Minutes File (Quarterly) • Transaction Profile Exception Report File (Monthly) • High-Risk Accounts List • Structuring File • BFIU Circulars/Circular File • MMBPLC Internal Circulars File • System Check / AML & CFT Compliance Report File • AML Training File • Transaction Profile Update File • KYC Update File • False Positive Report File • Account Inquiry File • Adverse Media Report File • Other Miscellaneous AML/CFT Files.	On-going
14	In case of AML/CFT issues, the SBCO shall report related to AML/CFT to the BAMLCO of the Tag Branch of the Bank.	As required
15	Keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction.	On-going
16	Review of CTR to find out Suspicious Transaction Report (STR)/Suspicious Activities Report (SAR).	On-going
17	Reports any Suspicious Transaction, Suspicious Activity (STR/SAR), Structuring and Media Report to the CAMLCO/AML&CFTD.	As required
18	Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction.	As required
19	Arrange quarterly meeting of the Sub Branch Anti-Money Laundering Compliance Committee (SBAMLCC) to review the AML&CFT Compliance status of the branch at the end of every quarter, maintain minutes in documented form and send a copy to the AML Division.	Quarterly

20	Perform Half Yearly Self-Assessment on AML performance of the branch and ensure compliance and any corrective action and submit the report to the CAMLCO.	Half Yearly
21	Submit branch returns including CTR, Structuring, KYC Exception Report, Money Movement reports etc. to the AML&CFTD as per specific schedule.	Monthly, & Half Yearly
22	Audit/Inspection related activities including timely compliance of the same: a. During Audit (Internal or External)/Inspection (Bangladesh Bank): When audit/ inspection teams visit a sub branch, SBCO will be the coordinator. Whenever any document/statement/files/registers are required by the audit/inspection team. b. After Receiving the Audit/Inspection Report: Distribute the report to respective Department or any other related wing of Head Office with mentioning a deadline prior to the deadline of the main report. c. Continuous Monitoring about the progress of Compliance to the Report: In case of any deviation, inform In-Charge or related Head of Division immediately. d. Compliance of All Parts and Send to AML&CFTD within Stipulated Time	Adhoc

5.8.8 Roles & Responsibilities of Other Employees

Besides the above, a brief description of role and responsibilities of individual officer/ executive involved in anti-money laundering program of the Bank in branch level/head office level is given below:

Officers involved in Account opening	:	• To exercise due diligence in establishing the identity of customer prior to opening the Account. • To obtain as much information as possible on the customer that might help proper consideration of the nature and type of account. • To ensure that all required documents in respect of account opening are obtained and proper documentation is complete in case of loan account. • To ensure that transaction profile is obtained and reviewed when transactions are being carried out. • To obtain documentary evidence of large cash transactions are being carried out. • To report to Branch Manager and concerned higher authority for any suspicious transaction, he deems it necessary.
Customer Service Officer	:	• To support the account officer in respect of the above. • To perform the jobs of Account Officer in his absence.
Manager Operation	:	• To ensure that all control points are taken into account prior to taking place of any transaction. • To exercise ongoing due diligence in respect of trends of transactions on customers' accounts. • To update customer transaction profile in the ledger.
Foreign Exchange Officer		• Perform AML Risk Assessment for the business of the client. • To ensure that all control points are taken into account prior to taking place of any foreign exchange transaction. • To exercise ongoing due diligence in respect of trends of foreign exchange transactions on customers' accounts. • To exercise enhanced due diligence on trade Based Money Laundering.
Credit Officer		• Perform AML Risk Assessment for the business of the client. • To ensure that all control points are taken into account prior to taking place of any investment related transaction. • To exercise ongoing due diligence in respect of trends of transactions on customers' investment accounts.
Others Officer	:	• To ensure that AML program is effectively accomplished in the Branch or Booth. • To act as first point of contact in respect of any AML issue.

5.8.9 Independent Audit of the AML & CFT Program

Bank shall assess its AML & CFT programs regularly to ensure their effectiveness and to look for new risk factors. The audit must be independent (i.e., performed by people not involved with the organization's AML/ CFT compliance staff), and individuals conducting the audit shall report directly to the board of directors. Those performing the audit shall be sufficiently qualified to ensure that their findings and conclusions are reliable.

With a goal of establishing an effective AML and CFT regime in MMBPLC, it shall have to be ensured that the Internal Control & Compliance Division (IC&CD) of our Bank is equipped with enough manpower who have enough knowledge on the existing acts, rules and regulations, BFIU's instructions on preventing money laundering & terrorist financing and Bank's own policies in this matter to review the Self-Assessment Report received from the branches and to execute the Independent Testing Procedure appropriately.

5.8.9.1: Role & Responsibilities of Internal Control and Compliance Division

MMBPLC's IC&CD is well resourced and enjoys a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable.

Sl.	Key Role & Responsibilities of the Internal Control and Compliance Division	Frequency
1	Understand ML, TF & PF Risk of the Bank and check the adequacy of the mitigating measures;	On-going
2	Examine the overall integrity and effectiveness of the AML & CFT Compliance Program;	On-going
3	Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;	On-going
4	Determine personnel adherence to the Bank's AML&CFT Compliance Program;	On-going
5	Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);	On-going
6	Assess the adequacy of the Bank's processes for identifying and reporting suspicious activity;	On-going
7	Where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;	As required
8	Communicate the findings to the board and/or senior management in a timely manner;	As required
9	Recommend corrective action to address the identified deficiencies;	As required
10	Track previously identified deficiencies and ensures correction made by the concerned person;	As required
11	Examine that corrective actions have taken on deficiency identified by the BFIU or BB;	As required
12	Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;	As required
	Determine when assessing the training program and materials: • The importance of the board and the senior management place on ongoing education, training and compliance, • Employee account ability for ensuring AML&CFT compliance, • Comprehensiveness of training, in view of specific risks of individual business lines, • Training of personnel from all applicable areas of the Bank, • Frequency of training, • Coverage of Bank policies, procedures, processes and new rules and regulations, • Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity, • Penalties for noncompliance and regulatory requirements.	As required

5.8.9.2 Role & Responsibilities of External Auditor

As financial institutions become increasingly interconnected and exposed to sophisticated criminal schemes, regulatory bodies have tightened compliance requirements and placed greater emphasis on robust internal controls. Within this environment, external auditors play a critical role in safeguarding the financial system. Their independent assessment of a bank's financial reporting, internal control environment, and compliance practices provides an essential layer of oversight that helps detect weaknesses, irregularities, and potential indicators of illicit activities. By evaluating whether the bank adheres to anti–money laundering (AML) regulations, risk-management standards, and financial reporting guidelines, external auditors contribute directly to the prevention, early detection, and mitigation of financial crimes. External auditors support in strengthening their AML frameworks and maintaining transparency, accountability, and trust within the broader financial system.

Sl.	Key Role & Responsibilities of the External Auditor	Frequency
1	External auditor shall also play an important role in reviewing the adequacy of AML & CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report.	As required
2	External auditor shall be risk-focus while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient.	As required
3	External auditors shall report incidences of suspected criminal activity uncovered during audits in its audit report.	As required

5.9 Individual Responsibilities of officials relating to CBML & TBML analysis:

1. Have adequate understanding about AML Policy, Trade Based Money Laundering (TBML) and Credit backed Money Laundering (CBML); Have updated knowledge about AML&CFT related rules & regulations related to International Trade (local & internal) and credit related tasks & process flows;
2. Ensure fulfilment of requirements as per MMBPLC AML Policy & 'MMBPLC Policy on Prevention of Trade based Money Laundering'. Ensure CDD/EDD done properly and all directives have been complied with as per respective policy (Credit Manual/ Foreign Trade Operation Manual);
3. Identify Key ML/TF risk and challenges associated with credit/loan sanction and disbursement flow and trade business in consultation with the respective head of division;
4. Recheck internal/external (IC&CD, BFIU, DBI, Bangladesh Bank) inspection observation regarding CBML/TBML related issues or relevant points;
5. Ensure entity screening (Director/Beneficial Owner/Buyer/Supplier/Indenter/Vessel/Port/Country of Origin /Product etc. check through reliable sources) prior to establishing any form of trade relationship including processing of documentary bills discounted;
6. Follow procedure/process to screen Shell Bank/Shell Companies/Shelf companies and ensure that the Bank does not maintain relationship with Shell Bank/Shell Companies under any circumstances (In case of related business relationship and transactions).
7. Take effective measures to establish procedure to check prevailing TBML technique (Under/over invoicing of goods, under/over/phantom shipment, false declaration and so forth) and keep/collect records of such practices;
8. Ensure regular monitoring of trade related transactions at Branches and Head Office against the prevailing red flags and identify suspicious transactions and report STR/SAR to AML&CFTD if suspicion is established through investigation. Apply EDD on transaction with customers of high risk jurisdiction/ tax heaven jurisdiction.
9. Ensure record keeping as per the requirements of regulatory guideline;

10. Extend full cooperation to BFIU/IC&CD Audit/Inspection/DBI, Bangladesh Bank/other Competent Authority and take appropriate action for timely mitigation; Acts as liaison and be available to discuss with D-CAMLCO/ CAMLCO or the BFIU matters pertaining to the AML/CFT functions of the Bank;

5.10 Key Responsibilities of the Managing Director & CEO:

Key Responsibilities of the MD & CEO	Frequency
1. Overall responsibility to ensure that the Bank has an AML and CFT programs in place and those are working effectively.	On-going
2. On behalf of the Senior Management, Managing Director & CEO shall send a statement to all employees on an annual basis that clearly sets forth the Bank's policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. If necessary, MD & CEO will also monitor the overall status of the compliance issue.[4]	Yearly

5.11 Initiatives by Human Resources Division

For proper implementation of AML & CFT measures, following process will be incorporated in MMBPLC HR Policy

- Revised Code of Conduct & Ethics for the employees of Modhumoti Bank Limited which is the integral part of the Service Rules and Regulations:
- Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- Proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vies a vies for non-compliance;
- Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;
- Other measures that shall be taken in case of non-compliance by the Bank.

5.12 *Know Your Employee (KYE) Procedure in Appointment of Employees*: One of the major purposes of combating money laundering activities is to protect the Bank from risks arising out of money laundering. To meet this objective, Human Resources Division shall have to undertake proper ***Screening Mechanism*** in its different appointment procedures so that Modhumoti Bank does not face any money laundering risk by any of its staffs

5.13 *Recruitment Procedure*: To minimize ML & TF risks arise by or through its employees, Human Resources Division shall have to undertake fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Bank shall have to follow at least one from the following measures:

- reference check
- background check
- screening through or clearance from Law Enforcement Agency
- personal interviewing
- personal guarantee etc.

According to Clause # 5.14 (Employee Screening) of the Recruitment & Selection Policy, in compliance with Money Laundering & Terrorist Financing Risk Management Guidelines of BFIU 2015, all selected

candidates (fresh or lateral entrants) for employment with MMBPLC shall go through the following verifications before issuance of Appointment Letter. The Bank will strive to comply with any three of the following background verifications either through internal resources or nominated 3rd Party Agency:

a. Previous employment check.
b. Academic and professional qualification verification.
C. Police Verification
d. Independent identity checks (Passport or NID). e. Self-declaration on Credit history.

Any discrepancies in the information provided by the candidate will cancel the letter of offer/ appointment and may lead to termination.

As such, currently Human Resources Division of the Bank is conducting the following:

1. **Background verification:** Background and criminal history of the finally selected candidates are checked through Police verification.
2. **NID verification:** NID of finally selected candidates are verified from the web portal of Election Commission of Bangladesh Government.
3. **Academic certificate verification:** Academic certificates of the finally selected candidates are verified either through internal resources or nominated 3rd Party Agency. Please note that we have started the above verification from September 2017.
4. **Corporate Memory Management System (CMMS):** CMMS of Bangladesh Bank is used for checking disciplinary actions record of the entire job history of concerned candidates during recruitment.
5. **Self-declaration** by the finally selected candidates on (a) Relative Declaration, (b) Declaration of Accounts of Staff, (c) Personal and/or Individual Borrowing, (d) Outside Business Interest. Finally, selected candidates undertake to take prior permission from the Bank in case he/she wants to involve in any outside business interest which includes (but not limited to) becoming a director/ beneficiary/partner/ active participant/ sponsor/ volunteer for any organization outside Modhumoti Bank Limited. In the event if this declaration is found to be false at a later stage of employment with Modhumoti Bank Ltd., appropriate disciplinary action(s), up to separation from service, may be taken by the Competent Authority of the Bank.

5.14 Administrative Action on Breaches and Non-Compliance:

If any Non-Compliance found or Complaints is associated under Predicate offences under Money Laundering Prevention Act (MLPA) - 2012(amendment -2015), HR Division will follow the procedure as set out in the Policy "Disciplinary Action Policy against Money Laundering and Terrorist Financing Activities".

Under disciplinary Action Policy of MMBPLC following 4.5 clause action taken given bellow:

1. ***Non-compliance or violation of Bank's Anti-Money Laundering (AML) & Combating Financing of Terrorism (CFT) policy/manual or any other AML/CFT guidelines subsequently issued by the Management;***
2. ***Any other behavior or act, which in the opinion of this Manual constitutes misconduct. Any act or utterance which damages congenial working environment of the Bank or threatens/destroys image of the Bank.***

4.5 Others:

i. Non-compliance or violation of Bank's Anti-money Laundering (AML) & Combating Financing of Terrorism (CFT) policy/manual or any other AML/CFT guidelines subsequently issued by the Management;

ii. Any other behavior or act, which in the opinion of this Manual constitutes misconduct. Any act or utterance which damages congenial working environment of the Bank or threatens/ destroys image of the Bank.

5.15 Training Program:

Obligation Under; "Money Laundering & Terrorist Financing Risk Management Guidelines -2015	As per section 9.4 of "Money Laundering & Terrorist Financing Risk Management Guidelines" issued by BFIU, every employee should have at least day long basic AML & CFT training.

Before assigning an employee in a particular job or desk, banks shall examine the consistency and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.

As a part of the MMBPLC's AML & CFT Compliance program, all Employees are expected to be fully aware of the MMBPLC's AML & CFT policy and procedures. Each Employee is required to read and comply with this Compliance policy and procedures, address concerns to the Compliance Officer and ensure that he/she has read and understands MMBPLC's AML & CFT policy and procedures. All Employees are required:

- To undertake training programs on AML & CFT policy and procedures.
- To get trained in how to recognize and deal with transactions which may be related to money laundering. To timely escalate and report the matter to the Compliance Officer.
- To get themselves acquainted with Anti Money Laundering Rules & Regulations.
- To comply with the requirements of Rules & Regulations.

a)Customer contact staff/RM/Front desk officials: This is the front line of defense against money laundering; the ones who need the deepest practical understanding of why anti money laundering efforts are important and what they need to do to be vigilant against money laundering and Terrorist financing.

b) **Back office personnel:** These employees may also need special training, like TSD, LOD, CMO, Treasury back-office, NRB Operations & CRM.

c) **Audit and compliance staff:** These are the employees charged with overseeing, monitoring and testing AML & CFT controls, and they should be trained about changes in regulation, money laundering methods and enforcement, and their impact on the institution.

d) **AML Compliance staff:** These are the employees who are placed in AML & CFT Division or CCC member of the Bank. While they likely do not need the general AML course that would be provided to most employees, this group needs specialized advanced training to be able to stay on top of new trends or changes that impact the institution and the way it manages risk. Often, this will require attending conferences or AML specific presentations that go into greater detail.

e)**Senior Management and Board of Directors:** Money laundering issues and dangers should be regularly and thoroughly communicated to the Senior Management & Board of Directors. Arrange conferences/seminar on AML & CFT to keep Senior Management & Board members aware of the reputational risk that money laundering & terrorist financing poses to the institution.

f) Awareness of Customer

The customers of the bank are the core groups that should be made aware of AML & CFT activities occurring through the banking channels. The customers should be made aware of the bad effects of executing ML & TF like harming the economy of the country, tarnishing the image of the country and developing a tendency to neglect the related laws & rules. In this connection, the

branch/concerned division/department will place the awareness festoon in the suitable place of Branch premises and arrange awareness building initiatives like the distribution of leaflets, handbills, brochures, etc.

g) Awareness of Mass People

The mass people should be made aware of the AML & CFT activities and their bad effects on the society, economy and all over the country. In this connection, the bank should take different steps like circulating/ broadcasting/ telecasting appropriate advertisements and documentaries on radios, televisions and/ or other mass media, whichever deems best. The bank should also participate in awareness building initiatives often arranged by BFIU, Bangladesh Bank, the government and other regulatory bodies. Additionally, the bank will take different steps like using billboards, posters, festoons, distributing leaflets, handbills and using other media as well.

Human Resources Training & Development Center (HRTDC) and AML & CFT Division jointly/individually should design an effective training program to identify the target audience.

5.16 Annual Performance Evaluation:

- Adequate Knowledge on AML & CFT;
- Training Status on AML & CFT;
- Job performance on AML & CFT issues on Branch/Division;
- Non-compliance on AML & CFT issues on Branch/Division;

During the performance evaluation of the employees, his/her knowledge and skill of compliance of laws/bye-laws, rules/regulations, orders and any instructions of the Bank or regulatory authority are taken into consideration under the Performance Appraisal System which has been approved by the Board of Directors. Besides, AML audit rating (Audit conducted by AML & CFT Division or Internal Audit Department), disciplinary issues of the respective employees due to audit objections or non-compliance of AML & CFT issues are also taken into consideration during finalize their performance rating.

5.17 AML Compliance Effectiveness Reviews:

Bank will re-evaluate the Human Resource Policy on AML & CFT in reasonable time or time-to-time that will assess how well our compliance program is functioning.

The management should be aware of the fact that vested groups in connection with Money Laundering try to entice employees of banks and financial institutions for transacting their ill-gotten money in and out of the banking channel. For that reason, we have to utilize an elaborate and industry standard screening mechanism to attract and retain employees with the highest level of integrity and competence. The Human Resources Division must ensure that employee screening mechanism is an integral part of the recruitment process.

5.18 Training and Awareness

5.18.1 Training for Employee: Every employee of the Bank shall have at least basic AML & CFT training that should cover all the aspects of AML & CFT measures in Bangladesh. To keep the employees updated about AML & CFT measures, Bank shall require imparting refreshment training programs of its employees on a regular basis. As per section 11.2 of BFIU Circular 26 dated 26JUN2020, Proper training should be ensured for targeted officials as per their job description & related with job assignment. Refreshers Training will be provided to all the officials after a regular interval.

5.18.2 **Job Rotation:** Human Resources Division shall ensure that all branch officials including the branch managers must be transferred once in every 2 or 3 years.

5.18.3 **Leave Management:** Human Resources Division shall monitor leaves taken by employees to ensure that all branch officials including the branch managers have taken 15 continuous days (or other days as per policy) leave at a time each year as mandatory leave.

Chapter # 6

Customer Acceptance Policy (CAP) & Customer Due Diligence (CDD)

CHAPTER # 6
Customer Acceptance Policy (CAP) & Customer Due Diligence (CDD)

6.1: Customer Acceptance Policy

In line with section 2.0 of the BFIU Circular 26 (Master) dated 16JUN2020; every bank shall have a specific policy regarding selection of its customer which may be a part of its main policy on Prevention of Money Laundering and Terrorist Financing. Accordingly, MMBPLC has a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place to set-up any kind of business relationship with the bank. A concrete Customer Acceptance Policy is very important so that inadequate understanding of a customer's background and purpose for utilizing a bank account or any other banking product/service may not expose the Bank to a number of risks. The primary objectives of the MMBPLC Customer Acceptance Policy are –

- No account can be opened in anonymous or fictitious name. To prevent opening of this kind of Account, appropriate cautionary measures must be taken.
- Parameters of risk perception are clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status to categorize customers into different risk grade.
- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.

However, MMBPLC's Customer Acceptance Policy is not intended to be used against the disadvantaged people. Its policy rather encourages the ultimate goal of transparent, accountable & inclusive financial system in Bangladesh with Risk Based Approach.

MMBPLC ensures that it will accept only those customers whose appropriate identity is established by conducting due diligence to the risk profile of the client. Parameters of risk perception is clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. in ***Annexure # 02 (Risk Register)*** - to enable categorization of customers into different risk grades.

MMBPLC does not open an account where it is unable to apply appropriate customer due diligence measures i.e. if it is unable to verify the identity and/or obtain documents required as per with the risk categorization due to non-cooperation of the customer, bank will not open or allow withdrawal of money (with notice). Decision by the bank to close an account should be taken at a high level (COO, CAMLCO or CEO) after giving due notice to the customer explaining the reasons for such decision, in line with section 3.6 of the BFIU Master Circular#26 (Master Circular) dated 16JUN20.

MMBPLC makes necessary checks before opening a new account so that it can ensure the identity of the customer does not match with any person with known criminal background or with proscribed entities such as individual terrorists or terrorist organizations etc.

In line with BFIU, **MMBPLC also Prohibits** following as customers, i.e.:

- No account in anonymous or fictitious name or only with numbers shall be opened;
- No banking relationship shall be established with a Shell Bank; [Here shell bank refers to such banks as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group; and
- No account in the name of any person or entity listed under United Nations Security Council Resolutions (UNSCRs) or their close alliance adopted under Chapter VII of the Carter of UN on suspicion of involvement in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government shall be opened or operated.
- Any other instructions as issued by BFIU from time to time shall have to be complied with.

6.1.1 Prohibited Individuals & Entities by MMBPLC as Customer:

In addition to the above 3 prohibited types, MMBPLC will also not open accounts for:

- individual or entity from &/or operating in Sanctioned countries (particularly under OFAC Sanction, UK & EU Sanction);
- any sanctioned individual or Entity (SDN) in any of the international or local Regulatory Sanction list;
- individual or entity that has direct or indirect link with any Sanctioned - party/ Country/ SDN;
- any individual or entity that has any link with the Banned-entities (under section 18 of the ATA, 2009 of the Govt. of Bangladesh
- individual or entity that has been criminally convicted under MLPA2012 or ATA2009 or convicted severely for committing any 'Predicate Offence' under the MLPA;
- individual or entity that is linked to highly-sensitive Adverse media news, potential terrorist activities and severe negative-reputational concern;
- any individual or entity that appears to fall under High-Risk Customers but it cannot provide adequate document or information up-to satisfaction of MMBPLC to complete its required Enhanced Due Diligence;
- No account or business relationship shall be opened or related to activities or operation that is not permitted by Bangladesh Bank or statutory law (e.g. Private banking; illegal trade of firm-arms, drug-dealing, gambling/casino, etc.);
- No online account can be opened without physical presence of the customer*[3];
- No account to be opened for dealing/ business in Virtual Currency/unauthorized currency;
- No account shall be opened or operated by violation of AML/CTF laws and rules;

Exception: Only CAMLCO, if required, consulting CEO or BFIU, can approve any exception. For example, in case of Military or Police officials working under the UN Peace-Mission but stationed in any Sanction Country, the branch needs to prudently & politely ask for necessary documents from the customer and if it reveals that they have required license like from OFAC, &/or only salary to be credited from UN offices located outside the sanctioned country and no local transactions to & from the respective sanction country- then CAMLCO may approve such cases.

[if documents of Non-Resident Bangladeshis are attested of High-Commission of Bangladesh, exceptionally A/C can be opened]

6.1.2 High Risk Customers:

Some types of customers though not prohibited but possess significant risk or concerns from ML/TF aspects; MMBPLC needs to be very careful & extra vigilant on those customers during on-boarding and maintaining their accounts. Some of these customers are:

- Non-Government /Non-Profit Organization (NGO/NPO) s – particularly those, which receives foreign donations & no clear modus of operation &/or linked with religious activities or based on any ideology
- Charity, Trusts, Cooperative –Societies, MLM Companies and non-reputed & vulnerable clubs, association, Money-Changer, dealer of Jewelry- Precious stone etc.
- Customers & A/Cs on which there were any query/Hold/Freezing instruction from BFIU or ACC or similar Regulatory Authority within couple of years
- Legacy A/Cs for which there is doubt on the Veracity of Identification
- Customers refused by other bank for any facility &/or classified in CIB report
- Customers with huge High-Net Worth &/or Turnover/ Transactions
- Non-face to face & Non-Resident customers
- A/Cs of House-wife, Student, Land sale-purchase, etc. where the customer himself is not generating /owning the source of Fund and Beneficial owner's CDD is not clear/ unusual
- If Pay-Order is Directly purchased by huge Cash without clear supporting document

- Huge online transactions using various channels, Internet, etc. without legitimate justification
- Frequent Cash Withdrawal just following Cash deposits (Washout transaction & temporary repository A/C)
- Export/ Import related A/Cs with potential link with adverse news on Bonded Warehouse, Under/ Over-Invoicing and/or link with high-risk jurisdiction or risky commodity
- Pre-mature Encashment of large FDR/ Facility, etc.
- Regular trend of Structuring (Txns just below the CTR limits)
- A/Cs in Border-Area or related to parties in Border/ publicly-known-Vulnerable areas (e.g. Cox's Bazar, Teknaf, Benapol, Hilly, Tamabil, etc.)
- A/Cs from High-Risk Jurisdictions indicated in FATF Mutual Evaluation Report,
- A/Cs from Territories known as tax-heaven, &/or with high level of Corruption/Criminal activities
- A/Cs from Sanction countries or jurisdiction with embargos
- Accounts related to any Terrorist Activities/ Organization, etc.
- Accounts related to any Adverse Media News
- Accounts related to any PEP, IP, HoIOs
- Accounts related to any STR/SAR, etc.

What action to be taken: If the Branch had to On-board a customer falling under High-Risk category, they must conduct Enhanced Due Diligence (EDD) and mitigate the associated risks following the 'Risk Register'. In all such cases BAMLCO is advised to consult the AML&CFT Division and in some cases (e.g. PEP/IP /HoIO or Sanction related), mandatory approval from the CAMLCO has to be obtained, prior to establishing the banking relationship. Guidance Notes on Politically Exposed Persons (PEPs) for all Reporting Organizations is annexed at ***Annex-8.***

Instructions regarding Annual KYC & Enhanced Due Diligence (EDD) Review of High Risk and High Transacting Accounts have been illustrated in specific Inter Office Memo and also refer to AML&CFTD's related emails regarding Management and Monitoring process of High-Risk Accounts to mark High Risk A/Cs – so that staff can conveniently notice & monitor them.

Moreover, considering potential risks of ML & TF through remittance of foreign funds into the country through the NGO/NPO/Charity Organizations, a detailed questionnaire for collecting information for conducting due diligence on NGO/NPO/Charity Organization as provided by BFIU should be followed. As BFIU wants confirmation from Bank on this, hence proper CDD on NGO/NPO/ Charity, etc. is very important.

6.1.3 Low Risk Customers:

For the purpose of risk categorization, individuals and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts conform to the known profile, may be categorized as low risk.

Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic status of the society whose accounts show small balances and low turnover. Some more examples:

- Accounts related to any licensed Bank, Insurance /Leasing co./ FIs
- Accounts related to any Government offices
- Accounts related to reputed foreign govt. offices/ entities
- Accounts related to Salary or Pension, regular school-fee, scholarship, etc.
- Accounts related to reputed entities listed in DSE/ SEC, etc.
- Low-value A/Cs like farmer, school-saver, garments-shoe-worker, etc.

6.1.4 Risk Assessment & Acceptance of Customer (on-boarding):

Staff to consider the matter relevant to prospective customer details in the light of following indicators/factors:

- Customers' background, Country of origin & linked countries
- Public or high-profile position
- Linked accounts
- Business activities
- Politically Exposed Person (PEP)
- High net worth whose source of fund is un-clear,
- Non-resident or Non-face-to-face
- Complex structure or multi-layered ownership,
- To operate A/C for another person/s (Delegate, Trust, intermediary)
- Products & banking channels to be used, etc.

Customers are to be categorized into low & high risks - for identified risks in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc.; - as assessed as per Unique AOF Risk assessment, if the risk is within tolerance level – the customer will be accepted and commensurate due diligence to be done i.e. either Mandatory Enhanced Due Diligence – MEDD with CAMLCO approval, or EDD or Standard/ Simplified – SDD during on-boarding.

For any confusion or clarification needed on a prospective customer whether it will fall under high or low, or how to assess the risk in a complex situation, &/ or whether to accept or reject the customer, etc. – the BAMLCOs are strongly advised to consult the D-CAMLCO/ CAMLCO well in ahead; as later complexity & risk in terms of regulatory, reputational or legal will increase with such sensitive customers.

Reviewing some recent incidents; it is advised that, Branches should **not** establish relationship or open account for sensitive-risk concerns; for example:

1. Non-reputed & small News-medias, papers, on-line platforms, YouTube-channels, particularly associated with political, religious or fundamental /ethnic extremist beliefs – that may lead to adverse news/ propaganda – under the 'Bangladesh Digital Security Act, 2018 and the 'Information & Communication Technology Act, 2006' or similar regulations;
2. Small club, co-operatives, associations, NGOs, etc.- that does not have clear source of fund or proper presence & activities – that may lead to potential terrorist financing, drug-dealing, hundi, MLM or organized crimes – violating the 'Foreign Donations (Voluntary Activities) Regulation Act, 2016' or the 'Co-operative Societies Act,2001' or similar regulations;
3. A/Cs opened only to receive gift, lottery, unrelated remittances or digital currencies (bit-coin, etc.).

6.2 Risk Based Approach (RBA) and Risk Management:

Risk Based Approach (RBA):

According to FATF:

a. A RBA to AML/CTF means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CTF measures commensurate to those risks in order to mitigate them effectively. In case of risk assessment, it should be considered customer's nature of business, customer identity, product & services, countries, geographical location etc. Mentioned Risk assessment statement will be used or applicable to mitigate AML risk of the Bank.

b. As per Risk Assessment report, where it will be identified High Risk, it should conduct Enhanced Due Diligence;

c. When risk will assess as low; Bank can conduct SDD (Simplified Due Diligence) process;

d. When assessing ML/TF risk, countries, competent authorities, and financial institutions should analyze and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for the risk-sensitive application of AML/CTF measures. The RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CTF risks, but it is still used for ML or TF purposes.

An RBA does not exempt countries, competent authorities and financial institutions from mitigating ML/TF risks where these risks are assessed as low.

In a Risk Based Approach following are required:

- Assessing risk
- Risk management and mitigation

6.2.1 Risk Assessment:

BFIU issued guidelines titled "Money Laundering and Terrorist Financing Risk Assessment guidelines for banking sector in January 2015 (circular Letter No. 01/2015) for providing the basic ideas of identifying, assessing and mitigating ML & TF risks that banks may encounter in doing their business. In compliance, MMBPLC assessed its Business & Regulatory risk and prepare a **Risk Register** which is attached in this manual for compliance of all concerned ***(Annexure# 2).***

Risk can be defined as the combination of the probability of an event and its consequences. In simple term, risks can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur. While assessing Risk following broad categories may be considered:

- **Business risk and**
- **Regulatory risk**
- **customer risks**
- **products or services risks**
- **business practices and/or delivery method risks**
- **Country or jurisdictional risks.**

Customers: followings are some indicators (but not limited to) to identify ML&TF risk arises from customers of the bank:

- a new customer;
- a new customer who wants to carry out a large transaction;
- a customer or a group of customers making lots of transactions to the same individual or group;
- a customer who has a business which involves large amounts of cash;
- a customer whose identification is difficult to check;
- a customer who brings in large amounts of used notes and/or small denominations;
- customers conducting their business relationship or transactions in unusual circumstances, such as: significant and unexplained geographic distance
- between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations;
  - a non- resident customer;
  - a corporate customer whose ownership structure is unusual and excessively complex;
  - customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates;
  - customers submit account documentation showing an unclear ownership structure;

- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income.

Products and services:

- private banking i.e., prioritized or privileged banking;
- credit card;
- anonymous transaction;
- non face to face business relationship or transaction;
- payment received from unknown or unrelated third parties;
- any new product & service developed;
- service to walk-in customers;
- mobile banking, Internet Banking, E-Wallet, E-KYC, SWIFT, Transaction Platform.

Business practices/delivery methods:

- direct to the customer;
- online/internet;
- phone;
- Fax;
- Email;
- third-party agent or broker.

Channels Countries it does business in/with (jurisdictions):

- any country which is unidentified by credible sources as having significant level of corruption and criminal activity;
- any country subject to economic or trade sanctions;
- any country known to be a tax haven and unidentified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country;
- any country unidentified by FATF or FSRBs as not having adequate AML&CTF system;
- any country identified as destination of illicit financial flow.

Regulatory risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012, Anti-Terrorism Act, 2009 (including all amendments) and instructions issued by BFIU. As per BRPD Circular 2 dt 23.02.2020 & BFIU Circular 26 dated 16.06.2020, KYC & Risk Assessment Profiles have been prepared for duly fill-in by the Bank Officials **(See at Annex-5)**.

Examples of some of these risks are:

- ✓ customer/beneficial owner identification and verification not done properly;
- ✓ failure to keep record properly;
- ✓ failure to scrutinize staffs properly;
- ✓ failure to train staff adequately;
- ✓ not having an AML&CTF program;
- ✓ failure to report suspicious transactions or activities;
- ✓ not submitting required report to BFIU regularly;
- ✓ not having an AML&CTF Compliance Officer;

- ✓ failure of doing Enhanced Due Diligence for high risk customers (i.e., PEPs, IPs, HoIO);
- ✓ not complying with any order for freezing or suspension of transaction issued by BFIU/BB
- ✓ not submitting accurate information or statement requested by BFIU or BB.

6.2.2 Risk Management:

Risk management is a systematic process of recognizing risk and developing methods to both minimize and manage the risk. This requires the development of a method to identify, prioritize, treat (deal with), control and monitor risk exposures. In risk management, a process is followed where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

The Risk Management framework at a glance

Risk identification –

Identify the main ML&TF risks

Identify the main regulatory risks

Risk assessment/evaluation –

Measure the size & importance of risk:

- likelihood – chance of the risk happening
- impact – the amount of loss or damage if the risk happened
- likelihood X impact = level of risk (risk score)
- minimize and manage the risks
- apply strategies, policies and procedures

Manage the regulatory risks:

- put in place systems and controls
- carry out the risk plan and AML&CTF program

Risk monitoring and review –

Monitor and review the risk plan:

- develop and carry out monitoring process
- keep necessary records
- review risk plan and AML&CTF program
- do internal audit or assessment
- do AML&CTF compliance report

In connection with above, officials are advised to conduct due diligence of their - customer, product, channel, services, transactions, monitoring, follow-up, investigation, reporting, archival, training, etc., on Risk-Based-Approach (RBA); i.e. simply, more the Risk... more the due diligence.

SL	Criteria	Feedback	Low	Medium	High	Remarks
	A. Entity & Ownership					
1	Is the Bank subject to regular supervision of regulatory authority/ FIU & Operating with proper Licensing?	Yes	√			
2	Does the Bank have any branch in abroad or does the revenue from any oversee segment is more than 10%?	No	√			
3	Is the Board & Senior Management committed on Compliance Governance and attend required Meetings regularly?	Yes	√			
4	Is any member of the board of directors/officers or shareholders a Politically Exposed Person (PEP)?	No	√			

5	Total number of accounts/ customers		√			Minimum numbers
6	Total number of branches/ channels		√			Only 54 branches & few channels
	B. PRODUCTS & SERVICES					
1	Does it offer Correspondent Banking/Payable Through Accounts?	No	√			
2	Does MMBPLC conduct business with any of the sanctioned countries?	No	√			
3	Does MMBPLC have policies and procedures to prohibit any accounts/relationships with shell banks/organizations?	Yes	√			
4	Does the Entity's AML & CTF EWRA cover the inherent risk components of Client, Product, Channel & Geography?	Yes	√			
5	Does the Bank proactively assess the AMLCFT Risks of New products/ technologies/services/ channels?	Yes	√			
6	Is Services to walk-in customers are at minimum level?	Yes*	√			* as per regulatory prescription
C.	**AML, CTF, SANCTIONS & ABC PROGRAM, POLICY & PROCEDURES**					
1	Does MMBPLC have an Anti-Money Laundering /Counter Terrorism Financing (AML/CTF) program?	Yes	√			
2	How many individuals are centrally dedicated to this program?	5	√			
3	How many individuals are indirectly dedicated to this program?	105	√			
4	Does the Entity have a program that sets minimum AML, CTF and Sanctions standards regarding the following components?					
	Appointed Officer with sufficient experience/expe rtise	Yes	√			
	Cash Reporting (CTR) & other regulatory reporting	Yes	√			
	KYC/ CDD/EDD/MEDD	Yes	√			
	Beneficial Ownership & their KYC	Yes	√			
	Independent Testing	Yes	√			
	Periodic Review (High-Annually, Low-5yrs' cycle & Trigger event)	Yes	√			
	Policies, Procedures & uniform SOP/ Flow-charts	Yes	√			
	Risk Assessment	Yes	√			
	Details of Sanctions	Yes	√			
	PEP/IP/HoIO's Screening, MEDD (higher approval), Monitoring, etc.	Yes	√			
	Adverse Information Screening	Yes	√			
	Transaction Monitoring	Yes	√			
	Training and Education (both staff & customer)	Yes	√			
	Record retention & archiving	Yes	√			
	Suspicious Activity Reporting	Yes	√			
5	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee?	Yes*	√			*If any change come from the regulator

6	Does Bank have all required System, Software & technological Support to reasonably ensure CDD, Txn-Monitoring, Sanction & Adverse-news screening, Vessel Tracking, Price Verification, etc.?	Yes	√			
7	Does Bank provide mandatory training with comprehensive module?	Yes	√			
8	Does the Entity have a Sanctions Policy approved by management regarding compliance with sanctions law applicable to the Entity, including with respect its business conducted with, or through accounts held at foreign financial institutions?	Yes	√			
9	Does Bank have automated systems to screen transactions against lists of sanctioned/blocked persons, entities or countries ("sanctions lists") issued by governments/competent authorities?	Yes	√			
10	Does MMBPLC have policies and procedures accounts/relationships to prohibit with banks?	Yes	√			
11	Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to [reasonably] prevent, detect and report bribery and corruption?	Yes	√			
12	Does Regulator, External Auditor & Internal Auditor Reviews Bank's AMLCFT, Sanctions etc. Programs Annually?	Yes	√			
13	In addition to inspections by the government supervisors/regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?	Yes	√			
14	Has MMBPLC been subject to any investigations, indictments, convictions or enforcement actions related to money laundering or terrorism financing within the past 5 years?	No	√			
15	Does the Bank as a whole have a Satisfactory Audit Rating & Good rapport with the Regulator?	Yes	√			

*As a whole MMBPLC as an Enterprise has a Low Risk status on AML, CFT, Sanctions & ABC Standards

6.3 Customer Due Diligence (CDD)

Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, Physical/Legal Identification & transaction monitoring based on the information and data or documents collected from reliable and independent sources.

As per section # 25 of MLP Act-2012 (Amendment 2015), it is mandatory to ensure i.e. obtain & verify the **complete and accurate** identification & information of customers throughout the operation of the A/C. The CDD obligations compel banks to understand who their customers are, to guard against the risk of committing offences under MLPA, 2012 including 'Predicate Offences' and the relevant offences under ATA, 2009.

Complete means, generally a compilation of a legal ID (Photo ID &/or Registration), Name, Date of Birth/ Registration, Addresses, Contact numbers and completion of all necessary information of the uniform A/C Opening Form (AOF).

Accurate means, process of authentication of document from a dependable & reliable source/ information has been found correct.
Throughout the operation – refers typically to ensuring updated KYC through Periodical Review (05 Years for Low Risk Customers and 01 Year for High Risk Customers under section 3.6.4 of BFIU Circular#26 [Master Circular]) and Dynamic Risk Review (on trigger-event).

Banks are required to be certain about the customer's identity and underlying purpose of establishing relationship with the bank, and should collect sufficient information up to its satisfaction.
"Satisfaction of the bank" means satisfaction of the appropriate authority, that necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

6.3.1 Who is a Customer? (Know your Customer-KYC)

For the purpose of KYC Procedure, a "Customer" is defined in BFIU Circular No. 26 (Master Circular) as:

- any person or institution maintaining an account of any type (be it conventional bank account, agent banking account, card related account or others) with a bank or financial institution or having any business relationship using banking facilities;
- the person or institution as true 'Beneficial Owner' in whose favor the account is operated (Guidelines on **Beneficial Ownership is annexure- 7**);
- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional Intermediaries (such as lawyer/law firm, chartered accountant, etc) under the existing legal infrastructure;
- While high value single transaction conducted in a single Demand Draft, Pay Order, Telegraphic Transfer by "any person or institution or any person/institution" involved in a financial transaction that may pose reputational and other risks to the institution. (In this case if a transaction appears abnormal in relation to the usual transaction of the concerned person or institution that transaction will be treated as —high value);
- Any other person or entity as defined by BFIU from time to time.
- It is required to use BRPD, Bangladesh Bank circulated Unique AOF, though considering facilities of modern technology to use e-KYC, if available, Bank may on-board customers through completion of e-KYC formalities. When it will not be possible to open A/c through e-KYC, hard copy of AOF will be considered.

6.3.2 Phases of CDD:

To protect bank from risks of money laundering or/and terrorist financing by customers' willful or unwilling activities, Customer Due Diligence (CDD) must be conducted as per this policy manual and on RBA at different stages such as:

a) establishing a business relationship;
b) carrying out an occasional Transaction* having value of BDT5.00 Lac (BDT Five Lac) and above by the Walk-in-Customer*; (*Walk-in Customer is the one who is not an account holder of the Bank)*
c) at the time of occasional transaction via wire transfer;
d) If there is possibility of Tipping-Off during conducting of CDD for suspected involvement in money laundering and/or terrorist financing, STR must be reported without CDD;
e) Suspicion regarding the veracity of documents, data or information previously obtained for the purpose of identification or verification.

- To be sure about the customer 's identity and underlying purpose of establishing relationship with the bank, branch shall collect adequate information to the Satisfaction of the Bank*. Mentionable, the CDD process should be considered as an ongoing process. Information of High-Risk customers will be updated keeping transactions under close monitoring, evaluation and cross check of all related information.

- Correctness of identity information of customer or beneficial owner to be verified at the time of on-boarding or after opening of account but before making any transaction. But for walk-in customer or occasional transaction, the customer information must be verified at the time of transaction. Where the risk categorized as low or identified risk mitigation tools/ process is exist, or where no need to interrupt transaction/ close business relationship, in that case, information and documents should be verified within shortest possible time.
- Beneficial Owner (BO Guidelines is at annexure-**7**) for every account must be identified. The identity of the Beneficial Owner must be ensured by collecting information from independent and reliable source to the satisfaction of the Bank –
  a) If a person operates an account on behalf of the customer, the branch must satisfy itself that the person has due authorization to operate. Complete and accurate information of that person as well as the customer shall have to be collected and preserved,
  b) Apparently, if it seems, a person has control/influence over the customer, complete and accurate information of that person shall have to be collected and preserved,
  c) For Company account, complete and accurate information of the Beneficial Owner of the account shall have to be collected and preserved; In this case, person(s) who has Controlling/ownership interest* in the Company shall be considered as Beneficial Owner,
  d) To comply with the instructions of clause b-c, if Natural Person cannot be identified, then complete and accurate information of the Chief Executive Officer (CEO) shall have to be collected and preserved.
  e) To identify beneficial owner of the account & to take measures there against, it is required to follow instruction as contained in the Guidelines on Beneficial Owner as provided by BFIU.
- Legal status and accuracy of information of the operators are to be ascertained in case of the accounts operated by trustee and professional intermediaries (such as lawyers/law firm, chartered accountants, etc.).
- While establishing and maintaining business relationship and conducting financial transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories listed as high risk country in FATF's public statements) enhanced due diligence shall have to be ensured.

* *Walk-in Customer is the one who is not an account holder of the Bank,*
* *All transactions including Wire Transfer will be treated as Occasional Transaction,*
* *Satisfaction of the Bank shall mean that in the light of existing instructions, the relevant authority has been satisfied through completion of CDD by collecting necessary information/data/documents considering customer's risk*
* *A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 20%)*

6.3.3 Types of CDD:

The gravity, scope & depth of the CDD will vary according to the risk-level of the customer. Typically, it might be EDD or MEDD for High-Risk and SDD for usual/ low risk customers.

6.3.3.1 EDD & MEDD

Banks should conduct **Enhanced Due Diligence (EDD)** measures, when necessary, in addition to normal CDD measures. Bank should conduct Enhanced Due Diligence (EDD) under the following circumstances i.e. typically for High Risk customers:

- Individuals or legal entities scored with high risk;
- Individuals who are identified as Politically Exposed Persons (PEPs), Influential Persons (IP) and chief executives or top-level officials of any international organization;
- Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes;

- While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering and terrorism
- financing (such as the countries and territories enlisted as High – Risk and Non- Cooperative Jurisdictions in the Financial Action Task Force's Public Statement).

Enhanced CDD measures include:

- Obtaining additional information preferably from independent and reliable sources on the customer (occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship when applicable.
- Conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Making aware the concerned bank officials about the risk level of the customer.

Mandatory Enhanced Due Diligence (MEDD), refers to the critical part of EDD, when BAMLCO has to carefully review the CDD with additional verification/documentation, site visit & may need to complete separate assessment and obtain senior management Approval, that are termed as MEDD. In MMBPLC, for opening A/Cs of PEP/IP/HoIO and for

A/Cs that are linked (potentially) to Sanction country/ Parties – approval from CAMLCO is a pre-requisite to open such A/C. Moreover, AML&CFT Division has introduced an efficient KYC Review Form to facilitate collection of relevant & updated information on High Risk Customer during periodical review process.

6.3.3.2 Standard and Simplified Customer Due Diligence (SDD)

For normal or usual types of customers, Bank will follow Standard Due Diligence and where the customer may be treated as Low-Risk as referred above in section 6.1.3, bank may conduct Simplified Due Diligence (SDD). In such SDD the minimum requirement of KYC/CDD must be accomplished.

Moreover, in light of the instructions of BFIU Circular# 26 (Master Circular), Simplified Due Diligence (SDD) may be required in the following cases-

a) For Walk-in/ One-off Customer, SDD can be conducted for transaction below Tk.50,000/- (Taka fifty thousand), where Name, Address & Telephone number of applicant & beneficiary to be collected.
b) If the transaction is over Tk.50,000/- and below Tk.5,00,000/- (Taka Five lac), then attested copies of NID/ Photo ID of applicant & beneficiary will be obtained, beside taking information as mentioned in (a).
c) In case of opening or operating low risk accounts (e.g. School Banking account, Farmer's Account and other No-Frill Account*) with the intention for Financial Inclusion, Simplified Customer Due Diligence may be adopted.
d) Simplified customer identification process as stipulated in e-KYC Guidelines may be applied/ followed in this case.

* *'No-Frills' Account is a basic banking account. Such account requires either nil minimum balance or very low minimum balance. Charges applicable to such accounts are low. Services available to such account are limited.*

6.4. e-KYC

e-KYC is a digital process where Bank can open a customer account by filling up a digital form, taking photograph on the spot, and authenticate the customer's identification data (ID No., biometric information, address proof) instantaneously. This is a combination of paperless customer onboarding, promptly identifying and verifying customer identity, maintaining KYC profile in a digital form and determining customer risk grading through digital means. It is a faster process of doing KYC of customer verifying his/her identity document or bio-metric data. BFIU issued e-KYC Guideline vide Circular#25 instructing all banks to implement e-KYC by December 2020 (see the related annexure ***at Annex-12)***. We have taken initiative to select vendor for purchasing required software and the process will be started soon in compliance with the instructions of BFIU.

On the basis of customer's risk exposure, e-KYC module is divided into following two types:

A) Operational Process Flow for Self Registered (Customer through Mobile App or Web portal) account opening through Modhumoti Bondhon (e-KYC):

Step-1: Customer will download Mobile App or Log into Web Portal for account opening.

Step-2: Customer will provide Mobile Number for One Time Password (OTP) Verification.

Step-3: After successful verification customer will upload or Capture NID (Front & Back Side) for Optical Character Recognition (OCR) and will Capture photograph for liveliness checking or fraud detection.

Step-4: After successful liveliness checking or Fraud Detection, OCR Data will viewed and customer will input mandatory fields as guided by Mobile Apps or Web portal.

Step-5: After necessary inputs, customer will have to accept Terms and Conditions of e-KYC and will provide Nominee information of the customer and will complete the request.

Note:

- Customer will get confirmation of request submission in the Mobile App Screen and also get a SMS Notification with reference number.
- Customer selected Branch will receive a notification email that a customer has placed a request through e-KYC so that he can log in and execute customer request.

Step-6: Customer Selected Branch GB Officer (Modhumoti Bondhon Maker) will log into e-KYC system and will select Self Registered option for review and approval.

Step-7: GB Officer (Modhumoti Bondhon Maker) will verify customer data with Election Commission and review the application.

Step-8: GB Officer (Modhumoti Bondhon Maker) will initiate account opening request using reference number by selecting Type of Account, Transaction Profile and reviewing the whole application and will complete the Account opening Maker activities.

Turnaround Time (TAT) for step 6, 7 & 8: Within 1 Working Hours of Request Generation.

Step-9: GB Incharge or Manager Operations (Modhumoti Bondhon Checker) will go into e-KYC solution and will review the application by generating the Digital Forms (PDF), Signature Card (PDF) and will approve or decline the Account opening request. Modhumoti Bondhon Checker will print the Digital Form as Application Form (AOF) which will be stored in the branch for audit trail. Customer will get SMS Notification for Successful account opening or Decline request. For successful cases, customer will deposit account opening amount in the Teller Counter.

Turnaround Time (TAT): Within 1 Working Hours of Request completion by Maker.

Step-10: e-KYC system will request CBS to open account through Middle Ware. As we don't have Application Process Interface (API) in the CBS and we will be using Middle Ware for CBS integration, we will not be able to open Zero Balance Account in the CBS. So CBS will Debit (-) BDT 1 from GL Account and Credit (+) BDT 1 to customer account for opening account in the CBS for the interim period unless system make necessary development.

Step-11: For Decline Cases, GB Officer (Modhumoti Bondhon Maker) will rectify the application requests and will submit again for account opening through GB Incharge or Manager Operations (Modhumoti Bondhon Checker).

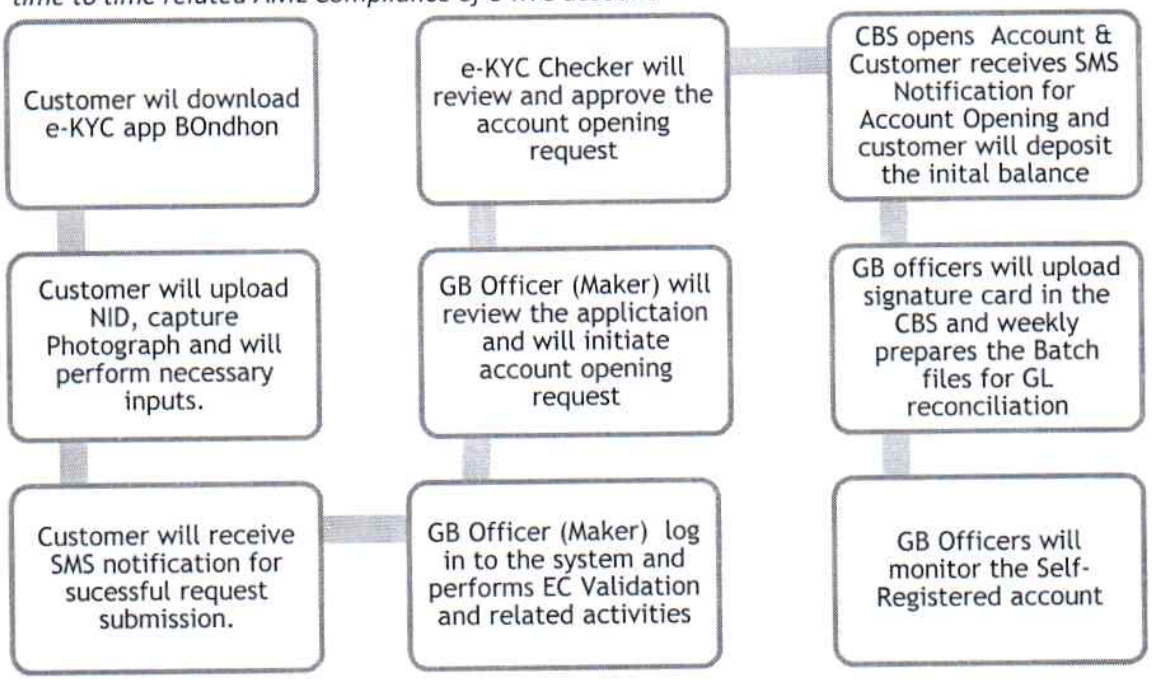
Step-12: Account Opening Officer (GB Officer/GB Incharge/Manager Operations) will login to the CBS and will upload the Signature Card in the Core Banking System (CBS).

Turnaround Time (TAT): Same day of Account approval.

Step-13: Every week, Branch will prepare a Batch File with number of account opened through e-KYC solution to Debit customer (BDT 1-) customer account and will adjust GL Account for the interim period unless system make necessary development.

Note:

- *If customer does not deposit initial amount within 1 month of account opening, Branch General Banking (GB) team will email to the customer to deposit initial amount.*
- *If customer does not deposit initial amount within 2 months of account opening account will be closed by sending an email to the customer branch.*
- *Operations Division will monitor and will guide branches and related stake holder time to time related to e-KYC and Compliance.*
- *AML & CFT Division of the Bank will monitor and will guide branches and related stake holder time to time related AML Compliance of e-KYC account.*



Customer Level Associated Risk:77

- Customer try to open account using other person NID
- Wrong nominee information & photo
- Existing Customer can be created by creating new Customer ID instead of existing one

Risk Mitigation Strategy:

- ✓ Liveliness check and NID and photo verification with EC data
- ✓ Respective Br/Div on will check manually before removing post no debit
- ✓ System will stop and tell customer to visit nearest branch
- ✓ Respective Br/Div will check and adjust/shift customer to existing customer ID

Branch Level Associated Risk:

- Negligence from respective Br/Division manpower approves an account which should not be approved;
- Invalid card /cheque application
- Insufficient fund for Cheque Book
- Lack of proper validation/Identification of customer
- Validation of provided documents

Risk Mitigation Strategy:

- ✓ Tell customer the proper reason or suggest them to visit nearest branch
- ✓ System to create Demand for realization of Cheque Book fee post facto (in **case** of insufficient fund);
- ✓ Proper Due Diligence should be ensure at the time of face to face customer serving by Sighting Original NID/Document
- ✓ Branch needs to check required/ pending Flow/archival workflow to identify customer & documents;

B) Operational Process Flow for Assisted Model (Branch) Account Opening through Modhumoti Bondhon (e-KYC):

Step-1: Customer will visit Modhumoti Branch for account opening.

Step-2: Branch Modhumoti Bondhon Maker (GB Officer) will greet customers and will start account opening through e-KYC by login into the e-KYC solution. **TAT**: Immediate

Step-3: GB Officer (Modhumoti Bondhon Maker) will collect customer NID and Photograph from the customers and will scan the documents for e-KYC. **TAT**: Immediate

Step-4: GB Officer (Modhumoti Bondhon Maker) will upload NID Front and Backside in the e-KYC system for Optical Character Recognition (OCR). GB Officer will also upload customer Photograph.

Step-5: GB Officer (Modhumoti Bondhon Maker) will verify customer NID data with Election Commission and e-KYC system will also complete Sanction Screening through AML solution.

Step-6: GB Officer (Modhumoti Bondhon Maker) will verify Customer Mobile Number through OTP Validation.

Step-7: After successful EC Validation, Sanction Screening and Mobile Phone validation, GB Officer (Modhumoti Bondhon Maker) will inputs customer personal information, Nominee information and will submit the application for customer creation. A reference number will generated by system for customer creation.

Step-8: GB Officer (Modhumoti Bondhon Maker) will initiate account opening request using reference number by selecting Type of Account, Transaction Profile and reviewing the whole application and will complete the Account opening Maker activities.

Step-9: GB Incharge or Manager Operations (Modhumoti Bondhon Checker) will go into e-KYC solution and will review the application by generating the Digital Forms (PDF), Signature Card (PDF) and will approve or decline the Account opening request. Modhumoti Bondhon Checker will print the Digital Form as Application Form (AOF) which will be stored in the branch for audit trail. Customer will get SMS Notification for Successful account opening or Decline request. For Successful Cases, customer will deposit account opening amount in the Teller Counter or can Transfer Fund through EFT. **TAT**: Within 1 Working hour of Request generation by Maker.

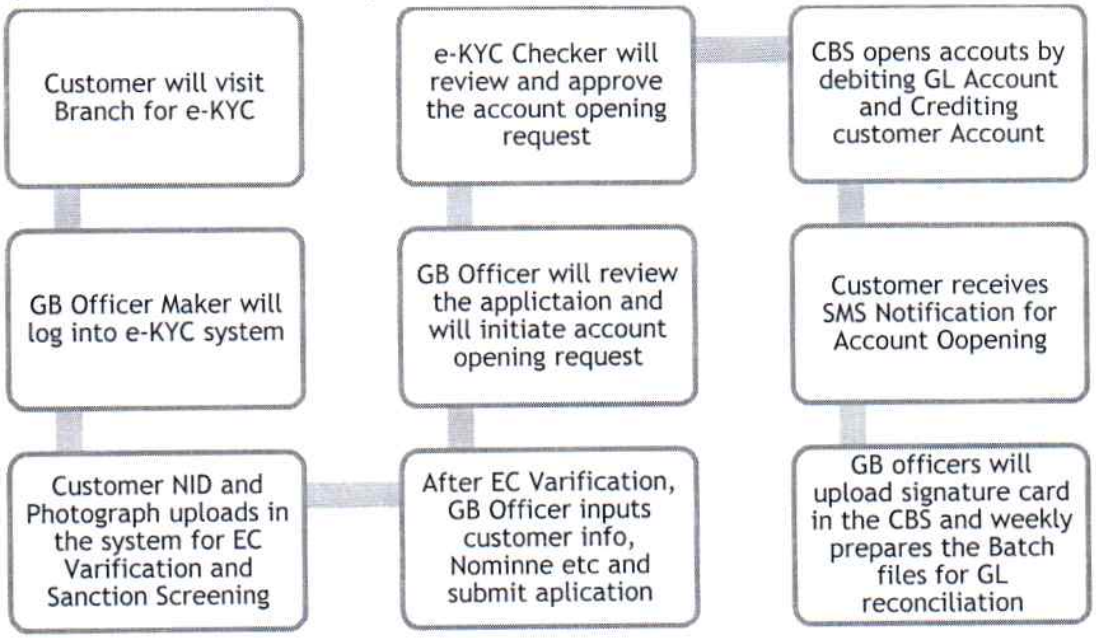
Step-10: e-KYC system will request CBS to open account through Middle Ware. As we don't have Application Process Interface (API) in the CBS and we will be using Middle Ware for CBS integration, we will be not able to open Zero Balance Account in the CBS. So CBS will Debit (-) BDT 1 from GL Account and Credit (+) BDT 1 to customer account for opening account in the CBS for the interim period unless system make necessary development..

Step-11: For Decline Cases, GB Officer (Modhumoti Bondhon Maker) will rectify the application requests and submit will again for account opening through GB Incharge or Manager Operations (Modhumoti Bondhon Checker). **TAT**: Within 1 Working Hours of Request rejection by Approver

Step-12: Account Opening Officer (GB Officer/GB Incharge/Manager Operations) will login to the CBS and will upload the Signature Card in the Core Banking System (CBS).

TAT: Same day of Account approval

Step-13: Every Week, Branch will prepare a Batch File with number of account opened through e-KYC solution to Debit customer (BDT 1-) customer account and will adjust GL Account for the interim period unless system make necessary development.



C) Operational Process Flow for Assisted Model (Agent) account opening through Modhumoti Bondhon (e-KYC)

Step-1: Customer will visit Modhumoti Agent Points for account opening. (**TAT**: Immediate)

Step-2: Modhumoti Bondhon Maker (Agent) will greet customers and will start account opening through e-KYC by login into the e-KYC solution.

Step-3: Agent (Modhumoti Bondhon Maker) will collect customer NID and Photograph from the customers and will scan the documents for e-KYC.

Step-4: Agent (Modhumoti Bondhon Maker) will upload NID Front and Backside in the e-KYC system for Optical Character Recognition (OCR). Agent will also upload customer Photograph or Capture Photograph.

Step-5: Agent (Modhumoti Bondhon Maker) will verify customer NID data with Election Commission and e-KYC system will also complete Sanction Screening through AML solution.

Step-6: Agent (Modhumoti Bondhon Maker) will verify Customer Mobile Number through OTP Validation.

Step-7: After successful EC Validation, Sanction Screening and Mobile Phone validation, Agent (Modhumoti Bondhon Maker) will input customer personal information, Nominee information and will submit the application for customer creation. A reference number will be generated by system for customer creation.

Step-8: Agent (Modhumoti Bondhon Maker) will initiate account opening request using reference number by selecting Type of Account, Transaction Profile and reviewing the whole application and will complete the Account opening Maker activities.

Step-9: GB Incharge or Operations (Modhumoti Bondhon Checker) will go into e-KYC solution and will review the application by generating the Digital Forms (PDF), Signature Card (PDF) and will approve or decline the Account opening request. Modhumoti Bondhon Checker will print the Digital Form as Application Form (AOF) which will be stored in the branch for audit trail. Customer will get SMS Notification for Successful account opening or Decline request.

TAT: Within 1 Working Hour of request submission by Maker.

Note: Agent Banking Field Officer may act as Checker for e-KYC module only for emergency during bulk Social Safetynet Account opening; however CBS Activities like: Signature Card (PDF upload should be done by Branch Officers. **TAT:** Within 1 Working Hour of request submission by Maker

Step-10: For Successful Cases, Agent will capture customer Finger Print by logging into Agent Banking System and will also collect account opening amount from the customer by following existing deposit with digital printout.

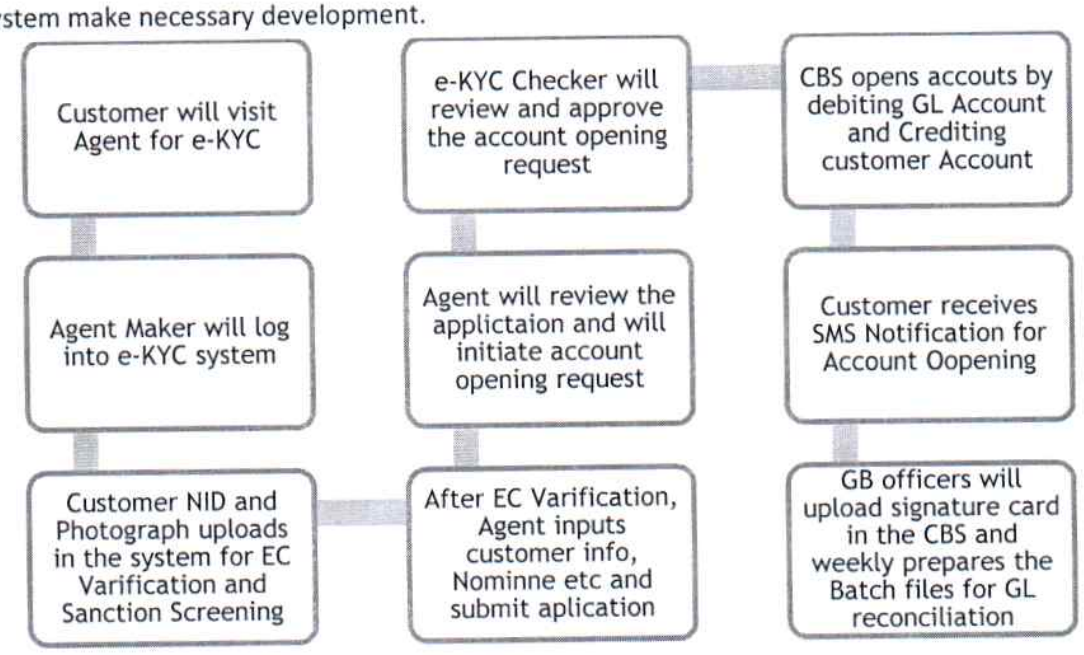
Step-11: e-KYC system will request CBS to open account through Middle Ware. As we don't have Application Process Interface (API) in the CBS and we will be using Agent Banking Middle Ware for CBS integration, we will be not able to open Zero Balance Account in the CBS. So CBS will Debit (-) BDT 1 from GL Account and Credit (+) BDT 1 to customer account for opening account in the CBS.

Step-12: For Decline Cases, Agent (Modhumoti Bondhon Maker) will rectify the application requests and submit will again for account opening through GB Incharge or Manager Operations or Agent Banking Field Officer (Modhumoti Bondhon Checker).

Step-13: GB Officer/GB Incharge/Manager Operations will login to the CBS and will upload the Signature Card in the Core Banking System (CBS).

TAT: Same working day of Request Approval.

Step-14: Every week, Branch will prepare a Batch File with number of account opened through e-KYC solution to Debit customer (BDT 1-) customer account and will adjust GL Account for the interim period unless system make necessary development.



Additional Queries:

- Nominee Photograph (attested by the Customer) & Nominee's legal ID to be collected, in general. However, if customer can provide NID Number & Date of Birth of Nominee; Branch will Verify & Print NEC database Report on the Nominee and get it attested by the Customer. Branch will scan the photograph of the Nominee from the Verification Report in e-KYC System. In this later case, customer does not need to provide separate photograph to Branch. *
- ICT will arrange to make field on Nominee's Name, DOB, Legal ID type, & Number of NID/ Passport/ Birth-Regt. Certificate/ School-College ID, etc.
- If Source of Fund is mainly provided by Parents, Spouse, or immediate family members and monthly transaction is within BDT1lakh; No need to complete KYC of Beneficial Owner

- Need to complete 'KYC of Beneficial Owner with photo' as per BFIU Circular#26 of 16JUN20 and to be completed under Regular e-KYC in case of Beneficial Owner of A/C is: a) different and Source of Fund is not provided by– Parents, Spouse, or immediate family members (even if monthly transaction is within BDT1lakh); and b) if fund is provided by Parents, Spouse, or immediate family members and monthly transaction is above BDT1lakh.
- ICT will also ensure sending SMS notification to customer instantly that, a) Thanks for opening A/C with MMBPLC (if all complete), or b) Thanks for opening A/C & you need to submit pending docs within30 days to MMBPLC to activate you're A/C (if any docs pending).
- ICT will try to fetch as much as possible information from the NID into the e-KYC Template automatically (like Gender, etc.)
- ICT will try to put an Identifier in the UBS to distinguish e-Accounts that are opened under a) Simplified KYC or b) Regular KYC – so that later for any Regulatory query or for any KYC-Remediation exercise or for Monitoring purpose, Branch can accomplish correct tasks.
- For Address Verification (if different from the NID), please take any of the following: a) copy of Utility Bill (preferably not older than 3months')/ Card, like: Water/ GAS/ Electricity/ Telephone, etc.
b) Residential address appearing on any official document prepared by a Government Agency, like:Letter or Notice from Tax-office, Land-Register, City-Corporation, Passport-office, etc.
- If customer (Male below 65 or NOT gazette war-wounded-freedom fighter)'s Annual Taxable income is more than BDT3lac, or more than 3.5lac (if Female, & male above 65yrs), or above BDT4.75 lac in case of said freedom fighter - Bank should ask for TIN and annotate on the form, if customer does not have TIN, he/she must write-down on the form clearly that, he doesn't have TIN. Bank should not take the risk of Tax-evasion (as one of the Predicate offences of MLPA, 2012).
- Currently for complexities, we are not going for Joint-A/C under e-KYC process.
- Branch must keep at-least one key-page of Sanction screening proof with the full AOF.

** **Note**: If not readily available, Branch may proceed putting 'Hold on Withdrawal' and giving 1month time to customer to provide supporting document);*

For Audit trail & checking, following documents should be in place:

Sl.#	Simplified	Regular
1	Completed 4 pages' AOF with all Signatures	Completed 4 pages' AOF with all Signatures
2	Proof of Address (if different from NID)	Proof of Address (if different from NID)
3	Photo & ID of Nominee (if NID Number & DOB available, photo not required)	Photo & ID of Nominee (if NID Number & DOB available, photo not required)
4	Proof of Sanction Screening	Proof of Sanction Screening
5	N/A	Proof of Profession/ Source of Fund
6	N/A	If BO- Completed KYC of Beneficial Owner with Photo
7	N/A	If PEP/Sanction/Adverse news- Approval of ML&TFPD

6.4.2 Periodic KYC Review

Periodic KYC review involves the simple procedure of submitting the latest identity and address documents to the bank. There is regulatory guidance for doing periodic KYC review/update in every 5 (five) years for the low-risk accounts and 1 (one) year for high-risk accounts [BFIU circular No. 26 dated 16th June, 2020 (section no 3.6.4)].

6.4.2.1 Customer Communication

a. Letter communication
b. Email Communication
C. SMS Communication
d. Call over phone/mobile
e. KYC Review Pending Alert during OTC Cash/Fund Transfer

6.4.2.2 Standard KYC Review Procedure

Following procedure will be followed as standard KYC review procedure for Personal & Non-Personal Account, however following may be reviewed & updated at a reasonable time or time-to-time based on legal/regulatory or business/ operational changes which should be approved by CAMLCO & respective Business Unit.

6.4.2.3 Collection of documents & process

- Customers may provide/submit their updated documents to RM or at any of his/her nearest MMBPLC branch.
- RM/BAMLCO/ DAMLCO must fill-up the KYC profile Form with a complete risk rating including Monthly Transaction Amount (TP).
- Personal Information Form (PIF) must be signed by the Customer, where there is any change in customer data (i.e. Passport, Address, Mobile, email & **etc.).**
- Any changes in Non-personal Account (i.e. Address, Mobile, email & etc.)
- We should obtain the signature of customer or operators and/or directors based on customer types, where Branch/RM should use page 1&2 of Non-personal Account Opening Form.
- If there is no change found in the customer's personal information or entity's information, BAMLCO/RM will collect the updated documents of the Customer and BAMLCO/RM fill-up only KYC Profile Form with the declaration "No changes found".
- RM/DAMLCO of Head Office may upload documents
- Operations/LOD should update the information in CBS with a proper KYC review date.
- In case of inadequate documents found, Operations/LOD may refuse or return the documents to Branch or RM with proper reason.
- Hard copies of KYC review documents should preserve in the customer file of the respective Branch.

6.4.2.4 Posting restriction:

- Posting restrictions **such** as **"Post** No Debit" shall impose to the accounts of non-response customers if there is no positive response from the account holder or unable to conduct proper CDD by Branch/RM/BAMLCO/DAMLCO.
- Before impose posting restriction, the Operations/AML/KYC project Team will provide the account list to Branches and Division.

6.4.3 Transaction Monitoring

A well-designed transaction monitoring (TM) system is an important component of an effective anti-money laundering (AML) compliance program. It supports the efforts to combat money laundering and terrorist financing by helping financial institution to identify unusual or suspicious activity that must be reported to regulatory in tracking and prosecuting criminals involved in ML/TF.

An effective monitoring system comprises the following two key components: -

(i) Monitoring performed by staff who deal directly with customers (e.g. relationship managers) or process customer transactions (e.g. counter staff/front-line staff); and

(ii) Regular reviews of past transactions to detect unusual activities by BAMLCO/DAMLCO. Branches/ concern Division/Department of Head Office needs to monitor the transactions of customer on **a** regular basis. The complex transaction - transactions that deviate from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring.

6.4.3.1 Key requirement for setting Transaction Profile (TP)

Transaction Profile (TP) is first effective tool for transaction monitoring (TM) system to identify unusual transactions.

Initial TP Limit-Setting

In this step, TP is set-up at the time of account opening based on the information provided by the customer such as nature business/occupation, net worth/business turnover, monthly income/source of fund & etc.

Some examples of TP setting techniques:

1. While a house wife declared in the TP that her husband's income as her main source of funds then the responsible bank official should justify her husband's nature of business/profession, account activity, proof of the sources of funds and its true entity; **etc.** through proper scrutiny.
2. While a businessman declared that his/her business income is the main source of funds then the responsible bank official should justify the true entity, business turnover and its reality, nature of business, account activity and the entity's customers; etc. through proper scrutiny.
3. While a student declared that his/her parent's income as his/her main source of funds then the responsible bank official should justify his/her parent's nature of business/profession, account activity, reality of the sources of funds and grounds for operating the account; etc. through proper scrutiny.

TP Limit Review/Modification:

According to section 3.6(3) of BFIU Circular No-26, every after 6(six) to 12(twelve) months from the establishment of relationship with customer, Bank shall take reasonable and appropriate measures to update/modify Transaction Profile (TP) of each customer. Customer notification/communication is not required for reducing the existing TP amount as an outcome of TP amount analysis against transactions.

6.4.3.2 Over-the-counter TP Breach Alert

Monitoring Action Parties

- Branches

Monitoring Actions

- Branch desk official **to** send the customer to account opening/review officer where account transaction records generated from Bank Ultimus /Dashboard to be analyzed and customer to be questioned accordingly.
- In case of TP Breach, TP updated with the availability of supporting document(s)/proof, if latest information varies significantly with the earlier provided information in bank records or seems suspicious by Branch, respective official may report in ISAR form.
- Respective Branch/Division to maintain/update TP on the respective information filled-up in KYC Profile Form / TP Form.

6.4.3.3 Regular Transaction Monitoring Activities

(a) TP Brach reports (High Risk, Low Risk and Newly opened accounts)

Key Takeaways

Branch to generate TP breach reports by themselves from AML System (others system)

Highly deviated transaction amount against the existing TP.

Whether any Internal SAR (ISAR) raised by Branch?

i. A common task will be issued from AML portal for all the branches and AML supervisor to follow-up his/her portfolio branches.

ii. Action time by branches: **1st** to 15th day of the following month.

(b) Transaction structuring report

Key Takeaways

Branch to generate reports by themselves from AML System;

Whether any Internal SAR **(**ISAR) raised by Branch?

i. A common task will be issued from AML portal for all the branch and AML supervisor to follow up his/her portfolio branches.

ii. Action time by branches: 1st to 15th day of the following month.

(c) Cash Transaction Report (CTR)

Key Takeaways

- Are there any KYC lapses in CTR accounts?
- Whether KYC reviewed or pending?
-Whether sufficient documents or supporting paper collected against CTR transactions?
-Are there special findings against the accounts like as SB or Housewife / Students accounts and new accounts in CTR?
-Whether any Internal SAR (ISAR) raised by Branch?
-Whether any STR detected by Branch from last month CTR data?

i. Responsible AML Officer will ensure the data availability for the Branch.

ii. A common task will be issued from AML portal for all the branch and AML supervisor to follow up his/her portfolio branches.

iii. Action time by branches: within 21st day of the following month.

(d) Threshold / Channel based /Monthly High Amount Transaction Accounts

Branches/ concern Division/Department of Head Office should monitor **the** high-volume transaction from all types of transactions (i.e. Teller/Cash, ATM, Clearing (BACH), RTGS, EFT, ¡BANKING transactions) on a regular basis and keep record as well to identify unusual transactions.

Key Takeaways

- Are there any **KYC** lapses in High volume transacted accounts? Whether KYC reviewed or pending**?**
-Whether sufficient documents or supporting paper collected against High volume transactions?
- Whether any Internal SAR (ISAR) raised by Branch?
- Whether any STR detected by Branch from last month High value transactions?

i. Responsible AML officer will provide data to all AML Supervisor.

ii. Individual AML supervisor will issue a task from AML Portal and collect response from Branch. iii. Action time by branches: 21st to 30th day of the following month.

(e) Online Transaction Analysis/Monitoring:

Branches/concern Division/Department of Head Office should monitor the online transactions of customers on a regular basis and generate online transactions reports from Bank Ultimus/Dashboard to detect suspicious transactions.

Key Notes:

Find-out who perform this activity as a top & frequency.

Find where the transaction performed **(i.e.** geographical area). Compare online transaction with customer Business area & activity. Find out unusual deposit and followed by withdrawals.

(f) Transaction Monitoring on PEPS/IPS Customer:

Branches/ concern Division/Department of Head Office should monitor the transactions of PEPS/IPs customers on a regular basis and analyzed the reports to detect suspicious transactions.

Key Notes:

Use of corporate vehicles without valid business reason

Transactions which do not commensurate with source of fund. Transactions by usual third-party.

Compare transactions with customer Business area & activity. Find out unusual deposit and followed by withdrawals.

(g) Trade Transaction Analysis to prevent TBML: (As describe TBML Risk Management Guidelines**)**

6.5 Elements of CDD:

By Elements of CDD, we referred to the documents & information that constitutes a totality or profile-picture of a customer. As advised in section 3.4 (1) of the BFIU#26 (Master Circular), MMBPLC uses Uniform A/C opening form (version of 2020) which has been prepared in light of BRPD & BFIU's A/C Opening Form, KYC & Risk Assessment template and as per Annexure - KA of BFIU Guidelines on ML&TF Risk Management (SEP15), MMBPLC ensures proper documents for -- Identification, Source of Fund & Occupation and Address Verification. Please refer to related section of this Manual related to "Records relating to CDD & verification of identity will generally comprise" for broad guideline. For various types of Customer, various types of documents may be required to adequately complete the CDD.

- KYC & Risk Assessment Form (as per annex-KA of Master circular) must be filled in by the Bank Officials, as its not the part of Account Opening Form.
- If the same customer maintains more than one account, to avoid repetition and transaction monitoring & evaluation, the Bank will allocate/ use Unique Customer Identification Code (UCIC). This UCIC will help to track the provided services to the customer and also be helpful for monitoring transaction.
- Bank Officials will prepare Transaction Profile (TP) of the customers upon discussion with the customer considering AML&CFT risk. Bank will update TP upon scrutiny & evaluation of 6 / 12 months transactions and Bank will determine a probable TP for the customer. Upon evaluation, if the TP differs noticeably, Bank will investigate into the matter, if satisfied, TP will be updated, otherwise if suspicion created, STR/SAR will be initiated. In this case, Bank will take cautionary measure to avoid harassing the customer.
- For privileged customer (like VIP Banking or others), besides CDD, it should conduct EDD with additional information.
- To maintain or continue any A/c relationship or conduct any transaction with a person or entity (Legal persons, legal entity, financial organization or any other organization) of **FATF listed** countries or ***'Jurisdiction Under Increased Monitoring & High Risk jurisdiction Subject to a call for Action',*** increased/ extra cautionary measured to be taken or if required counter measured to be taken as per FATF guidance.
- To maintain and conduct transaction of foreign trade, instructions to be followed as per BFIU's "Guidelines for Prevention of Trade Based Money Laundering" and also MMBPLC TBML Guidelines.

For this staff should refer to - Annexure - KA BFIU Guidelines on ML&TF Risk Management. Some crucial issues to note by MMBPLC staff:

6.5.1 Identification of Customer:

Our preference will be to obtain National Identification Card (NID) as this can be verified through the independent & reliable source, i.e. National Election Commission's Database via on-line with verification printed result under official agreement. Then we may rely on Passport & then Birth Registration Certificate (particularly for Minors) with any valid photo ID. For all IDs staff must see the Original and keep a photocopy of the document after seeing the original and annotate as "Original Seen" before attesting the copy with full signature and seal.

6.5.2 Documents for Source of Fund &/or Occupation

Annexure B of the BFIU Guidelines on ML& TF Risk Management has illustrated details on various types of documents for Source of fund & occupation. Sometimes, for some informal business or earning or rentals in Upazillas – formal documents are not always available; in such cases sourcing staff can give a site visit report and customer will give a written declaration describing detail on his/her nature of occupation, monthly income, associated parties, mode of transaction etc.- which should be upon satisfaction to the BAMLCO.

6.5.3 Address Verification

Annexure B of the BFIU Guidelines on ML& TF Risk Management has illustrated details on various types of documents for Address Verification. Where document not available 'Proof-of-Delivery (POD); of Thanks-letter should be kept with AOF. Similarly, the sourcing staff can give a site visit report describing detail on locations with nearest 'landmarks', etc.

6.5.4 Persons without Standard Identification Document

It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, street children or people, students and minors shall not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach should be followed consulting the AML&CFT Division. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph. Bank shall not allow 'high value' transactions to this kind of customers.

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number.

In these cases, it may be possible for the bank to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc.) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

6.5.5 Walk-in/ One-off Customer

Banks should collect complete and correct information while serving Walk-in customer, i.e. a customer without having account, with a simplified KYC Format. Banks should know the sources of fund and purpose of transaction while issuing any Pay-Order for job-application/paying utility bill or endorsing FCY in a Passport for Travel with visa & ticket. Usually Walk-in customers should not be allowed for large or unjustified grounds. Banks also collect complete and correct information of any person other than customer during deposit or withdrawal using on-line facilities. One photo-Id must be retained for such Walk-in customers and their name must be checked in S3. To ensure unique practice among

branches, as per Regulatory directive – KYC format for walk in customer and TP Exception declaration form had been introduced and communicated through e-mail.

6.5.6 Introducer:

To identify the customer and to verify his/her identity, an introducer may play important role. An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach account opening procedures as a favor to an applicant. For individual Account, Introducer is not mandatory, if the Account holder has a National Identity Card and that is duly verified.

6.5.7 Minor

For minor, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s). Under normal circumstances, a family member or guardian who has an existing relationship with the bank concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

6.5.8 Corporate Bodies and other Entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, and struck off, wound-up or terminated. In addition, if the institution becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;

- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding controlling/ownership interest or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

Where the business relationship is being opened in a different name from that of the applicant, the bank should also satisfy itself that the reason for using the second name makes sense.

The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:

- All of the directors who will be responsible for the operation of the account / transaction.
- All the authorized signatories for the account/transaction.
- All holders of powers of attorney to operate the account/transaction.
- The beneficial owner(s) of the company
- The majority shareholders of a private limited company.

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again.

When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

6.5.9 Companies Registered Abroad

Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, bank should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh's. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

6.5.10 Partnerships and Unincorporated Businesses

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the bank, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable).

An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

6.5.11 Powers of Attorney/ Mandates to Operate Accounts

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third-party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.

6.5.12 Transaction limit for Walk-in/ One-off customer: As a response to the enhanced concerns of the global as well as local regulators, banks are required to follow a Risk Based Approach (RBA) to assess the nature, purpose & transaction volume/limit for One-off/Walk-in Customers. Accordingly, following instructions are put forward for the branches/divisions for their compliance -

- With reference to the BRPD Circular letter#08, dated 19 July 2004 and section 3.5 of the BFIU Circular# 26 of 16JUN2020 on Simplified Customer Due Diligence (CDD); bank has to allow transaction for Walk-in/ One-off Customer, including issuance of Pay-order for legitimate purposes and for relatively small values.
- Few services like PUPID (Payable Upon Proper Identification) against inward remittance from wage-earner, small value Pay order (for specific purpose like Job application, admission in College, Utility services, etc.), or for small purchase/ sale of Fey e.g. for travelling to India/abroad - can be provided to walk-in non-customers. However, all walk-in/ non-customers transaction requires to comply with the following:

  i) Obtain customer vital KYC information (i.e. name, address, contact detail, source of fund & transaction purpose) & complete a simplified KYC form (available in branch);
  ii) Sanction Screening of non-customer's detail & Beneficiary Name (in case of Pay-Order) through Compliance Link;
  iii) Verification of National Identification Card (NID)/ Passport of the non-customer (NID is verified through NEC data base, Passport seen in original);
  iv) Copies of Passport, Visa, Air/train ticket are obtained for FCY travel-endorsement;
  v) For issuance of Pay-Order the name of Beneficiary should be Entity, not individual;

- It can be related to Job-Application or T&T/ WASA/ Titas/ BTCL utility Bill etc. or for ender participation in Government works or favoring any Government Organization or Fee of University, College or Reputed firm, embassy, Visa-office, VAT/ Tax/Customs, etc.
- Branch should prudently & humbly know the purpose of underlying transaction & apply CDD and if required obtain supporting document;
- Typically, the maximum limit for such transaction should not be more than BDT50,000/- (up-to BDT5,000/- Branch may allow without Photo-ID of the walk-in customer but above that, Photo-ID has to be collected). On RBA, the limit of FCY transaction should be within USD200-300/-;
- If intended transaction is above BDT50,000/- & below BDT500,000/- Enhanced Due Diligence must be conducted, Branch Manager must be consulted & if required senior management/ AML&CFT Division should be consulted and only in justified grounds Branch may allow such transaction for Walk-in Customers;
- Need to keep all documents in records for 5 years (as per BFIU guideline);

Exception to the above can be only allowed by Branch Managers, if needed consulting senior management/ AML&CFT Division.

6.5.13 Non-Face to Face Customers

Bank should assess money laundering and terrorist financing risks while providing service to non-face to face customers and typically MMBPLC does not open A/C without customer's physical presence &/or

face to face interaction with Bank staff. As stated in section 16.3 of the BFIU Guidelines on ML& TF Risk Management - 'Non face to face customer' refers to "the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the bank branch". Therefore, A/Cs sourced by staff Fast-Track, Agent points – must be scrutinized very carefully by Branch & Compliance Unit of Agent Banking, so that no Prohibited Customer or A/C with poor CDD –is approved for on-boarding. In this case, e-KYC Guidelines as circulated by BFIU will be applicable.

6.5.14 Beneficial Owner (BO):

BFIU recently issued a Beneficial Owner guideline for banks which is annexed (**Annex-7**) with this policy for necessary compliance of all concerned. However, Banks should consider following aspects while identifying beneficial ownership includes:

- Any natural person operating accounts on behalf of customer;
- Any person (whether acting alone or together) who has controlling interest or ownership interest on a customer who might be legal entity or legal arrangements. Where there is any doubt identifying controlling interest, the banks should consider other means to determine controlling interest or ownership of a legal entity or arrangements. In addition to that bank should also consider reasonable measures to verify the identity of the relevant natural person who hold senior management position;
- Any person or entity who has controlling or 20% or above shareholding within any or legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should consider for other types of legal arrangements.

Typically, in MMBPLC staffs are advised to complete basic KYC in PIF for BO with a supporting document of source of fund/occupation; however, it is not mandatory to obtain signature of BO on the PIF and those will be in general for A/Cs of House-wife, Student, Minors, etc. Where, a natural or legal person who holds controlling interest, listed on a stock exchange and subjects to disclosure requirements or majority owned subsidiaries of such listed companies may exempted from identifying or verifying beneficial ownership requirements.

6.5.15 Government A/Cs

For Government accounts simplified CDD can be followed and BRPD & BFIU has also prescribed a simplified Personal Information Form (PIF) to follow.

6.5.16 Unique Customer Identification Code (UCIC)

Banks should use unique identification code for any customer maintaining more than one account or availing more than one facility. Such unique identification system could facilitate banks to avoid redundancy, and saves time and resources. This mechanism also enables banks to monitor customer transactions effectively and detect any linked problematic /risky A/Cs promptly. MMBPLC has a mechanism to link such A/Cs and staff has been also advised to obtain information of all A/Cs in MMBPLC on the AOF's particular section.

6.5.17 Timing and Duration of Verification

The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed. However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this shall be subject to stringent

controls which shall ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority. In MMBPLC – approval from CAMLCO should be obtained for such deferral. This authority shall not be delegated, and should only be done in exceptional circumstances. Any such decision shall be recorded in writing.

Verification, once begun, shall normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is in itself suspicious.

6.5.18 In case where Conducting the CDD Measure is not possible

If conducting the CDD measure becomes impossible because of the non-cooperating behavior of the customer or if the collected information seemed to be unreliable, that is, bank could not collect satisfactory information on customer identification and could not verify that, bank should take the following measures as per section 3.7 of the BFIU master circular #26:

(a) must not carry out a transaction with or for the customer through a bank account;
(b) must not establish a business relationship or carry out an occasional transaction with the customer;
(c) must terminate any existing business relationship with the customer, providing Notice to the customer and according approval from Senior Management/ CAMLCO;
(d) must consider whether it ought to be making a report to the BFIU through an STR.

Banks should always consider whether an inability to apply CDD measures is caused by the customer. In this case, the bank should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the bank should consider whether there are any circumstances which give grounds for making a report to BFIU.

If the bank concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be sent to the BFIU. The bank must then retain the funds until consent has been given to return the funds to the source from which they came.

If the bank concludes that there are no grounds for making a report, it will need to make a decision on the appropriate course of action. This may be retaining the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or returning the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

6.5.19 Screening through Automated Sanction Screening Software:

To implement an effective sanction screening system in the Bank MMBPLC has implemented an automated sanction screening software namely S3. Branch concerned official will primarily be responsible to ensure screening of new customer before on boarding (i.e. before opening of any new account, disbursement of any foreign remittance, Letter of Credit both export and import).

Screening of Connected Parties (e.g. Directors of company, Non-signatory or mandate holder etc.) must also be done as a part of a robust and comprehensive screening process and to ensure that MMBPLC does not get involved unknowingly with any financial relationship with any sanctioned individual or entity and violate sanction law. A detailed guideline in this regard has been promulgated to the branches.

For screening of existing customer with updated sanction list ICT Division will arrange batch screening with a regular interval or as and when the sanction lists are updated. All BAMLCOs will check the screening result through Automated Screening Management (ASM) of S3 regularly. If any unsolved matched case is found in the ASM of S3 it must be attended by the concerned BAMLCO immediately

and check the matched data with available information of the MMBPLC customer and solve the matched case either it is a "False match" or "True" match. If the BAMLCO feels that the match case is critical to solve, he/she should escalate the case to the AML&CFT Division via email at **amlct@modhumotibankltd.com**.

Respective officer of AML&CFT Division will review the case & consult the AML Head /CAMLCO for decision. CAMLCO will take the call whether it is a False or True match. In case of True match-the A/C will be not on-boarded, transaction will be stopped and BFIU to be notified, as required. AML Head/ CAMLCO will consult with the MD&CEO if the matter is very sensitive before taking decision and upon merit of the particular case may notify the MD&CEO in due course of his decision. Escalation process of case Management is furnished below:

Escalation process of Automated Screening Management

6.5.20 Customer Exit Process:

In line with section 3.7 of BFIU Circular #26 (Master), banks may close/exit relationship with the existing customer on ground of non-co-operation/inability of customer to provide necessary information/documents to fulfill KYC process. Accordingly, AML&CFT Division has outlined a general guideline on customer exit process, which is as per followings-

As the global as well as domestic regulators are very much concerned regarding ML, TF and Sanction, it is prescribed that the financial relationship are exited/closed where there are potential risks of ML, TF and Sanction violation. Accordingly, AML&CFT Division has formulated a specific guideline regarding customer exit process where it has been clearly stated when branch should consider customer exit process and how to do it. Officials can also consult the matter with General Banking Manual.

i) **When there are Repetitive SAR/STRs:**

After lodging Suspicious Activity/ Transaction Report (SAR/STR), the particular A/C is treated as high Risk and thus remains within monitoring. If Branch &/or AML&CFT Division notices frequent alerts on that A/C -which may lead to further SAR/STR, active consideration should be given to Exit the customer. Prudently customer should be contacted if any deficiencies could be regularized. However, if there are no positive update from the customer or good justification and particularly if there are 3 such internal or external SAR/STR situation, A/C should be closed without tipping-off. We will provide notice in writing and just stating a general reason "for Administrative Reason, Bank is unable to provide him/her banking services with effect from .... (date)". As per section, 7(6) of the BFIU circular#26 of 16 June 2020; AML&CFT Division will prudently discuss with BFIU respective official on this and retain all pertinent documents in records.

j) **When there is explicit & proven case of ML/ TF/ Sanction Violation:**

If MMBPLC notices an A/C having direct Violation of Sanction, or proven case of Money Laundering or Terrorist Financing- instantly AML&CFT Division will consult BFIU, put hold on the A/C, decline

transaction, lodge STR/SAR and arrange to Exit the relationship consulting BFIU, based on the gravity of the issue.

k) When such CDD Deficient A/Cs are also commercially not viable.

MMBPLC Branches consulting AML&CFT Division can exit relationship where the A/C itself is not commercially viable and having ML/TF minor concerns. Though on commercial ground, lodging STR is strongly recommended.

6.6 Politically Exposed Persons (PEPs), Influential Persons (IPs) and Head of International Organizations (HoIOs)

As per Sections 3.9, 3.10 & 3.11 of BFIU Circular#26 (Master Circular) and section 6.16 of the ML& TF Risk Management Guidelines (BFIU, Sep15), - all clients must be subject to an assessment to determine whether they are PEP's or IPs or HoIOs and their linked parties. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption. Relationships with these customers may increase the risk to the bank due to the possibility of that individuals holding such positions may misuse their power and influence for personal gain or advantage or for the personal gain or advantage of their Close Family Members and Close Associates. The person's status (i.e. PEP's/IP's/HoIO's) itself does not incriminate individuals or entities. It does, however, put a prospective or existing client into a higher risk category. It has been seen globally that number of banks has been penalized heavily for not adopting & exercising proper Enhanced Due Diligence for such sensitive customers.

** Instruction to be followed as contained in the BFIU's "**Guidance Notes on "Politically Exposed Persons (PEPs) for all reporting organizations**".

6.6.1 Definition of PEP's/IP's/HoIO's as Illustrated in MMBPLC

Politically Exposed Persons (PEPs) refer to individuals who are or have been entrusted with prominent public functions ***in a foreign country***, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. The following individuals of **other foreign countries** must always be classed as PEPs:

a. heads and deputy heads of state or government;
b. senior members of ruling party;
c. ministers, deputy ministers and assistant ministers;
d. members of parliament and/or national legislatures;
e. members of the governing bodies of major political parties;
f. members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
g. heads of the armed forces, other high-ranking members of the armed forces and heads of the intelligence services;
h. heads of state-owned enterprises.

Influential Persons (IPs): As per Section 3.9 of BFIU Circular No-26 dated June 16, 2020, **Influential Persons (IPs)** mean "individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials".

Section 6.16.3 of Money Laundering and Terrorist Financing Risk Management Guidelines indicates the following individuals as **Influential Persons (IP):**

1	Heads and Deputy Heads of State or Government
2	Senior Members of the Ruling Party
3	Ministers, State Ministers and Deputy Ministers
4	Members of Parliament and/or National Legislatures
5	Members of the Governing Bodies of the Major Political Parties
6	Secretary, Additional Secretary, Joint Secretary in the Ministries
7	Judges of the Supreme Courts, Constitutional Courts or other High-Level Judicial Bodies whose decisions are not subject to further appeal, except in exceptional circumstances
8	Governors, Deputy Governors, Executive Directors and General Managers of Central Bank
9	Heads of the Armed Forces, other High-Ranking Members of the Armed Forces and Heads of the Intelligence Services
10	Heads of State-Owned Enterprises
11	Members of the Governing Bodies of Local Political Parties
12	Ambassadors, Chargé D' Affaires or other Senior Diplomats
13	City Mayors or Heads of Municipalities who exercise genuine political or economic power
14	Board Members of State-Owned Enterprises of national political or economic importance

Whether an individual is an influential person or not will depend on the prominence or importance of the function that he/she holds, and the level of corruption in the country, the reputation and personal links of the individual and whether he/she has any links to industries that are prone to corruption. If the individual does not hold sufficient influence to enable them to abuse his/her power for gain, they should not be classified as an influential person.

In the Section 6.16.1 of Money Laundering and Terrorist Financing Risk Management Guidelines "immediate family" /"a close associate" of an Influential Person are categorized as under:

Close Family Members	Close Associates
Spouse, children and their spouses, parents	An individual who is known to have joint beneficial ownership or control of legal entities or legal arrangements, or any other close business relations with the IP; and
Estrangement, divorce	
Siblings, cousins, relatives or in-laws by marriage	An individual who has sole beneficial ownership or control of legal entity or legal arrangement which is known to have been set up for the benefit of the IP.

In addition, it should include any person publicly or widely known to be a close business colleague of the IP, including personal advisors, consultants, lawyers, accountants, colleagues of the IP's fellow shareholders and any person(s) that could potentially benefit significantly from close business associations with the IP.

** HoIO- High officials means important designated high official like 'Director, Deputy Director, Board Member or equivalent high officials)*

6.6.2 CDD Measures for PEP's/IP's/HoIO's

MEDD i.e. Mandatory Enhanced Due Diligence shall have to be exercised. In general, following instructions shall have to be followed to ensure EDD:

- Bank has to adopt a suitable system to identify whether the Customer or Beneficial Owner is a PEP/IP/HoIOs;
- Approval from the CAMLCO has to be obtained for establishing business relationships or to maintain the same with existing PEP/IP/HoIOs;
- Enhanced Due Diligence as mentioned in this manual has to be conducted for the PEP/IP/HoIOs;
- The above instructions will be applicable for the family members and close associates of the PEP/IPs. No middle ranking or junior individuals will be considered as PEPs.

In related IOM as provided through email – guidance has been provided along with an Assessment Template that needs to be completed by Branch after proper EDD and sent to the AML&CFT Division for final Approval (to ensure MEDD). This A/Cs to be treated as high-risk A/C but not prohibited and will warrant close monitoring & annual review of KYC. Related elaborate addendum will be provided separately through IOM, which will be included as annexure later on.

Shell Bank: Bank will not establish correspondent relationship with Shell Bank (defined later) and the bank is maintaining relationship with Shell bank. [Here shell bank refers to such banks as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group.
Bank should be certain /confirm that Respondent Bank do not provide service/ facilities to any Shell Bank.

Trust/ Nominee or Executors, Administrator's Account: Branch should determine whether customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so branch may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain detail of the nature of the trust or other arrangement in place.

While opening an account for a trust should take reasonable precautions to verify the identity of the trustees and the settlers of trust, guarantors, protectors, beneficiaries and signatories.

Beneficiaries should be identified when they are defined. In the case of a "Foundation", Branches should take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

6.7 Correspondent Banking

Instructions for establishing corresponding relationship are as follows:

i) For the purpose of this circular correspondent banking shall mean providing services which are approved by BFIU like credit, deposit, collection, clearing, payment, cash management, international wire transfer, drawing arrangement for demand draft or other similar services by one bank (correspondent) to another bank (respondent).

ii) While establishing and continuing correspondent banking relationship following drill should be observed so that banking system cannot be abused for the purpose of money laundering :

- Before providing correspondent banking service, approval from the CAMLCO to be obtained on being satisfied about the nature of the business of the respondent bank through collection of information. If necessary, additional information shall have to be collected from open source;
- Before establishing a correspondent banking relationship with a proposed respondent bank, the bank must collect sufficient information as per (Porishisto - Ka of Master Circular- Questionnaire for Correspondent Relationship) about the proposed respondent bank to enable it to understand fully the nature of the proposed respondent bank's business.
- Banks should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.
- Banks should not establish or continue a correspondent banking relationship with any shell bank.
- Correspondent banking relationship shall not be established or continued with those respondent banks that have correspondent banking relationship or maintain account with a shell bank.
- Bank should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories

enlisted in the public documents of Financial Action Task Forces as High Risk and Non cooperating Jurisdictions). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.

- Enhanced Due Diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customers to transact business on their behalf (i.e. payable through account); in fact, in MMBPLC we try to avoid such arrangements.
- The instructions described in this manual shall be applicable to the entire existing correspondent banking relationship.
- The Wolfsberg Group has published a New Due Diligence Questionnaire on Correspondent Banking which may be followed in due course of time by the correspondent banks for renewal of relationship with the existing respondents.
- To maintain or continue any A/c relationship or conduct any transaction with a person or entity (Legal persons, legal entity, financial organization or any other organization) of FATF listed countries or *'Jurisdiction Under Increased Monitoring & High Risk jurisdiction Subject to a call for Action'*, increased/ extra cautionary measured to be taken or if required counter measured to be taken as per FATF guidance.

6.8 Trade Based Money Laundering:

A separate Guideline under the title- "MMBPLC Guidelines for Prevention of Trade Based Money Laundering- 2020" has already been enacted by Modhumoti Bank Ltd. to address the TBML issues of the Bank more effectively. All Concerned of the Bank shall comply with that guidelines to combat Trade Based Money Laundering. The TBML Guidelines has been preserved in the Bank's Common Folder: R:*10.10.10.116\ANTI MONEY LAUNDERING\1. BFIU related Policy & Circular\MMBPLC Guidelines for Prevention of TBML*. As anti-money laundering controls evolve, criminals find new ways to transform the financial proceeds of crime into legitimate funds. One of the most prevalent global money laundering strategies is to exploit the vulnerabilities of cross-border trade via Trade Based Money Laundering (TBML). TBML takes the advantage of the complexity of trade system, most prominently in international context where the involvement of multiple parties and jurisdictions make KYC and AML checks and customer due diligence processes more difficult. TBML primarily involves the import and export of goods and the exploitation of a variety of cross broader trade finance instruments. FATF defined Trade Based Money Laundering as, "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins". FATF & Egmont Group identified the most common TBML methods: Over-invoicing of goods & services, Under-invoicing, Multiple-invoicing, Over-or under-shipment, Phantom/ghost shipment, Illicit cash integration etc. (Annexure# 19).

6.8.1 TBML Risk Indicators

The FATF-Egmont report ***(Annexure#* 15**) aims to help public and private sector with the challenges of detecting trade-based money laundering. Using numerous case studies from around the FATF's Global Network, it explains the ways in which criminals exploit trade Global Network, it explains the ways in which criminals exploit trade recommendations to address the trade-based money laundering risks. These include using national risk assessments and other risk-focused material to raise awareness with the public and private sector entities involved in international trade, improving information-sharing of financial and trade data, and cooperation between authorities and private sector, including through public-private partnerships.

RED FLAGS INDICATING TRADE BASED MONEY LAUNDERING:

1. Significant differences between the description of the goods on the bill of lading and the invoice.
2. Significant differences between the values of the goods reported on the invoice and the fair market value of the goods.
3. Documentation showing a higher or lower value or cost of merchandise than that declared to customs or paid by the importer.
4. Shipment locations, shipping terms, or description of goods not consistent with letter of credit.
5. Customer significantly deviates from regular business activities.
6. Customer conducts business in or ships items through high-risk jurisdictions.
7. Customer engages in potentially high-risk activities, e.g., trade in defense articles or services, chemicals, sensitive technical data, and crude oil.
8. Commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities.
9. Commodity is transshipped through one or more jurisdictions for no apparent economic reason.
10. Commodity being shipped appears inconsistent with the customer's regular business activities.
11. Size of the shipment appears inconsistent with the scale of the customer's regular business activities.
12. Shipment does not make economic sense, e.g., the use of an oversized container for a small volume of goods.
13. Method of payment appears inconsistent with the risk characteristics of the transaction, e.g., the use of an advance payment for a shipment from a new supplier in a high-risk country.
14. Request to pay proceeds to unrelated third-party entities that have no apparent connection with the transaction.
15. Use of front (or shell) companies.
16. Transaction structure appears unnecessarily convoluted.
17. Imposition of irrelevant Debit Note(s).
18. Weight and other details of the goods declared in any other documents are inconsistent with the value/ quantity of the goods stated (depict Data Conflict).
19. Inconsistent with the FATF (40 re-commendations).

With a view to overcoming money laundering activities in trade finance and international trade, we have taken initiatives to include some directives for trade finance and international trade transaction in respect of prevention of Trade Based Money Laundering and Combating Financing to Terrorist (TBML & CTF). Beside this to prevent TBML, respective division/department will follow bank's "Guideline for Prevention of Trade-Based Money Laundering".

IMPORT:

1. It is mandatory to obtain updated/renewed copy of Trade License, Import Registration Certificate (IRC), etc. from respective authority for all corporate customers and individual for new approval, renewal, enhancement etc. Bank also shall take KYC of all its customers at a regular interval.
2. For facilitating/ serving Foreign Exchange /Trade related customers through LC or other mechanism, Bank check whether the nature of business support with the transaction under reference. If there is any conflict, the transaction/ service must not be done.
3. No walking customers are entertained in Trade Finance Business.
4. Bank's official will also regularly visit the corporate customers' factory/premises to observe the work in process /business operation, relating to the trade finance business.
5. Import shall be made at the most competitive price and it is obligatory for importer at any time to submit documents to import control authority regarding price paid or to be paid on time.
6. Commodity price must be verified through international commodity market and from different suppliers/ sources before establishing any LC.

7. Bank must check whether the goods to be imported are permissible by the law of the land as per existing Import Policy.
8. Bank will be confirmed, whether proper H.S. Code is being followed as per First Schedule of Customs Act 1969 based on harmonized commodity description and coding.
9. Bank must not issue LC Authorization form (LCAF) to open LC without valid H.S. Code.
10. Bank must check whether LC value commensurate with the LCAF value.
11. Bank must check whether LC is issued within the validity of LCAF or special permission has been taken from Statutory Authority in this regard.
12. Bank must check whether the validity of shipment of goods are as per IPO in force.
13. Bank must check all relevant papers of C&F Agents in case of their permission/renewal as enlisted agent of the bank.
14. For deferred payment LC, Bank must follow existing Guideline for Foreign Exchange Transaction and also Circulars issued by Bangladesh Bank from time to time.
15. Proper INCOTERMs must be inserted in LC Application and LC.
16. The LC clauses must be in accordance with Uniform Customs Practice for Documentary Credit (UCPDC-600) Publication no.600 and local law.
17. Bank must not allow import restricted goods.
18. Bank can insert pre-shipment clause if applicable and requested by the applicant.
19. Country of Origin must be mentioned in all cases of Import and reflection of the same must be in the package and container with exceptions as per IPO.
20. Importers Name, address and TIN must be inserted in LC application except few exceptions mentioned in existing Import Policy Order.
21. Bank must check whether proper documents are presented as per LC terms.
22. Import excess over limit set by Chief controller of Import and Export (CCI&E) must not be allowed.
23. Before passing any LC through SWIFT, Bank must screen all the outgoing messages with UN, OFAC, and EU sanction list.
24. Each and every SWIFT outward remittance also to be screened by the bank's software to check the true match with UN, OFAC, UK, EU and local sanction lists.
25. Comply FATF recommendations where applicable
26. Bank must ensure timely reporting to Bangladesh Bank.

EXPORT:

1. Bank shall obtain of ERC, VAT, TIN, and Trade License and their updated / renewed copies.
2. Bank shall verify apparent authenticity of Export LC (if required).
3. Bank shall ask the beneficiary to make amendments of adverse clauses, if there is any, before facilitating against them.
4. Before allowing BTB LC limit, related units of the bank must assess factory condition, production capacity business reputation and market credibility of customer.
5. Bank shall check whether the Export LC (ELC) has been transferred properly, if it is transferrable LC.
6. Bank shall check shipment schedule of ELC before opening BTB LC.
7. Bank shall open BTB LC by assessing lead (shipment validity coverage the production or process) time.
8. Bank must scrutinize the shipping documents before presentation for collection of funds.
9. Bank must monitor timely repatriation of export bills.
10. Related units of the bank shall arrange surprise visit to factory to observe production process.
11. Comply FATF recommendations where applicable
12. Bank shall ensure Timely reporting to Bangladesh Bank.
13. Sanction/ SDN/ High Risk Country or Party need to be checked for LC & Sales Contract.
14. Tax Heaven Countries need to be checked (Bank may take help from its corresponding banks to identify this) before executing any action against a LC & Sales Contract.
15. Shell companies/ Banks need to be checked/ identified before executing any action against a LC & Sales Contract.
16. Record keeping in internal database should be introduced.
17. In case of any adverse situation faced previously, precautionary measure needs to be

taken from that point onwards.

18. Identification of the true beneficial owner of the LC/ Sales Contract/ Any transaction before executing any action.
19. Understand the nature of underlying business relationship between/ among the parties in Sales Contract/ LC with the transaction.
20. Buyer credit report has to be checked to identify the buyer status (in terms of line of business, paid up capital, shareholder etc.)

REMITTANCE (WAGE EARNERS) COMPLIANCE:

MMBPLC collects wage earners remittance through different Exchange Houses and Money Transfer companies with whom it has drawing arrangements.

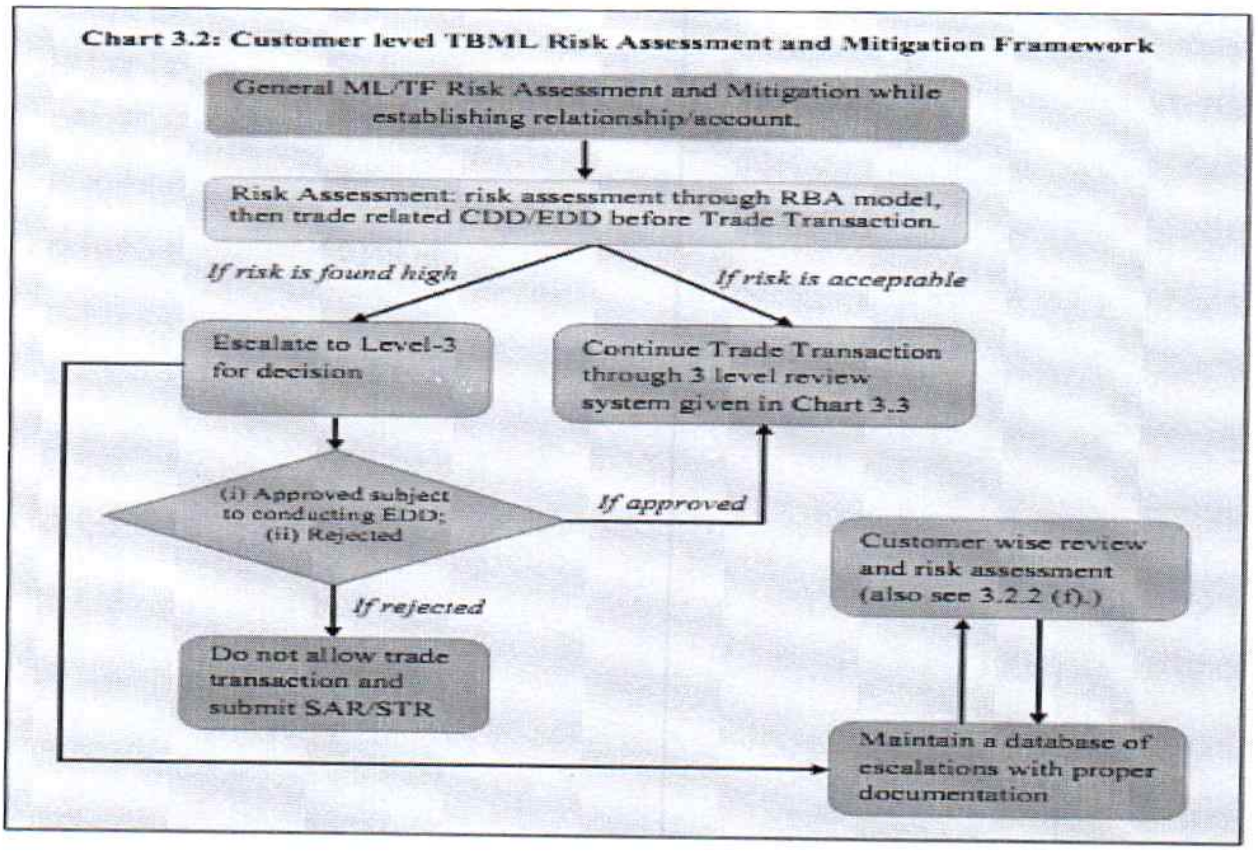
REMITTANCE EXECUTION PROCEDURE COMPLYING AML/CTF GUIDELINES:

With a view to monitor the remittance transactions in compliance with Anti-Money Laundering Act 2012, Anti-Money Laundering Amendment Act 2015, Anti-Terrorism Act 2009 (amendments 2012, 2013), MMBPLC follows the below mentioned steps during execution of wage earners remittances:

1. The Remittance Software which is used respective Branches (through Remit Infinity);
2. The sanction screening system is available at all the branches of the Bank as well as Head Office (HO) and the branches/HO have been advised to screen all the remittances at the branch level before making payment to the beneficiaries/beneficiary owners.
3. The concerned branch officials collect KYC of the beneficiaries or beneficiary owners along with valid photo ID for payment over the counter.
4. Remittances received through SWIFT are also screened in screening system available at Head Office.

6.8.2 TBML Risk Assessment & Mitigation Mechanism

Trade based Money Laundering risk may arise and affect due to inadequate infrastructure of the bank, inaccurate assessment of the customer before on board, poor identification and handling of TBML alert while conducting trade transaction by the officials concerned and; overall for failure of the bank to address the risk at the enterprise or institute level. Hence as per BFIU's instruction, TBML risk assessment and mitigation at infrastructure level, customer level, transaction level and at enterprise level to be established as shown in the flowchart below:



6.8.3 Mitigation & Escalation via 3 Level Review Framework

Depending on TBML risks trade transactions shall be disambiguated at level **1** or shall require escalations to level 2 or level 3 before they are executed or rejected and reported to BFIU as STR/SAR. All three levels, their roles and responsibilities, escalation, review and disambiguation systems have been described below:

Level **1** Official: The transaction processors, i.e. maker, checker, authorizer, reviewer, verifier, designated officials.

Level **2** Official**:** The trade compliance officer/Head of Trade/TSD/FT In-charge or designated officials.

Level 3 Official: DCAMLCO/officials as assigned by CAMLCO.

Level Definition	Roles and Responsibilities
Level 1 generally, will consists of operation i. level officials like transaction processors, i.e. maker, checker, authorizer, reviewer, verifier, designated officials.	i. Ensure that the customer has a current, approved KYC record and TTP in place before processing transactions. ii. Perform TBML Alert analysis and Sanction screening and execute transaction. iii. Escalate TBML Alerts/Potential hits of the transactions to Level 2, where required. iv. Escalate Suspicious Transactions/Activities to Level 2. v. Keep record properly.

Recent TBML Typology:

i) A recent TBML typology gets attention in the TBML world i.e. the both parties (Buyer and Seller-exporter & importer) is same beneficiary in trade transactions. The regulators are very concerned

Level 2 – generally will be officials with adequate i. seniority having skill/expertise to further analyze the merits of an escalation from Level **1** ii. Review TTP on certain Alerts. processor and the relevant suspicion itself. They iii. Disambiguate are likely to require extensive knowledge of trade-based money laundering risk and make appropriate use of third-party data sources to verify key information. Level 2 officials may be trade compliance officer/Head of trade or designated officials.	i. Review and examine the TBML Alerts raised by level 1. ii. Review TTP on certain Alerts. iii. Disambiguate with proper rationale and justification. iv. Document properly.
Level 3 generally will be officials with vast experience and expertise on trade-based money laundering process. Level 3 should be able to II. further assess the merits of an escalation from Level 2 officials. Level 3 generally includes DCAMLCO/officials as assigned by CAMLCO.	I. Conduct comprehensive review and examine the TBML Alerts raised by Level 2 II. Consult TTP if necessary III. Disambiguate with proper rationale and justification IV. File STR/SAR where required V. Document properly

about the issue and AML&CFTD has prepared necessary directives regarding EDD measures of Trade related customers and described in TBML Policy, in brief:

1. Section 24, Chapter 10 of Guidelines for Foreign Exchange Transactions (GFET), 2018 Vol-1 states the criteria for Opening of Branches or subsidiary companies abroad by the residents in Bangladesh, where prior approval of Bangladesh Bank was not required by the residents in Bangladesh for opening of offices/subsidiary companies abroad. They were however required to report the same to Bangladesh Bank within one month of opening of such offices, as per Appendix 5/74 of GFET.
2. Meanwhile, Capital Account Transaction (Overseas Equity Investment) Rules, 2022 published on 16 January 2022 allows only export-oriented companies to be allowed to invest abroad given that, they abide by several conditions and receive permission from Bangladesh Bank. So, now such companies owned by Bangladeshi residents have to meet the criteria.
3. In case of Importer and exporter are related parties, there is common interest which is a common Red flag mentioned in Local guidelines (TBML through import & export using related parties, Importer and exporter are related parties and there is common interest, TBML Guidelines issued by Bangladesh Bank) and also International standards. There is a possibility of higher ease to collude between related parties and it may lead to Phantom shipping, Over/Under invoicing, other TBML risks. In this context, bank should also follow instructions contained in para 2 of Chapter 7 and para 7(b)(iv) & para 7(c) of Chapter 8 of GFET, 2018, also section 4.2.2.2 Trade Related CDD Requirements to be performed by the branches/Division of MMBPLC Prevention of TBML Guidelines V-2020.

ii) Thorough review of Credit Report plays an important role in starting foreign trade relations. The credit report may contain information such as Company Name, Company address, Number of Employees, Line of Business, Ownership Structure including shareholding position, Director/ Principal/ Owner Name, Citizenship, Financial Stress Score, Risk Score, Banking relationship history, Major Supplier etc. Upon reviewing Credit Report, Trade people may get indication of Shell Bank, Front Company, Shell/ Shelf Company, sanction involvement of entity, suppliers, & related stakeholder, banks etc. Google search also give important information (Adverse News & global trends (bonded Warehouse, Panama-papers /Tax-Heaven) in this respect as well.

iii) Price verification is essential part in trade business. Trade People must comply with the related section of TMBL Guidelines and contemporary regulatory guidelines in this respect. Own database to be kept updated & verification to be documented.

iv) Understanding the line of business of buyer, seller & supplier is also crucial in establishing trade relationship. Because any trade transaction that deviates from the customer's existing line of business may have ill-motive to transact against criminal proceeds or may simply move money rather than goods through accommodation of bill etc. Bank will perform KYC of local entity, KYCC - a 360-degree view (customer's customer-Vendors/suppliers linked Risks).

v) Bank will CDD/EDD on account of business entity for eligibility and ensure the fulfillment of terms & conditions of relevant Bangladesh Bank's Circulars before allowing cash incentive against Loan & Trade Facility. It is also needed to monitor whether the client is involved in misusing incentive facility/ diversion of fund etc. or not.

6.8.4 CDD report through IMB (International Maritime Bureau) web portal:

Trade Based Money Laundering (TBML) has become a growing concern now-a-days as huge amount of money are laundered to the Off-shore banks or Tax-Heaven countries through TBML, weakening the country's economy. Moreover, global regulators have also become very much sensitive regarding this issue and imposed large amount of financial penalty to some of the biggest and renowned banks worldwide.

Considering the risks of TBML, MMBPLC has subscribed for IMB (International Maritime Bureau) web portal service from ICC (International Chamber of Commerce) in July 2022 and commenced operation from July 2022. Through IMB web portal service, AD Branches/TSD may check authenticity of Bill of Lading (B/L), request CDD on the beneficiary, information on vessel (e.g. IMO number, Port of calling etc.), whether the carrying vessel or any connected parties of LC have any Sanction concerns, etc. TSD has prepared and circulated the escalation process for referring any case to the IMB portal vide IOM **(Annexed at 16)**.

6.9 Credit Backed Money Laundering (CBML)

Credit backed money laundering is defined as the process of disguising the proceeds of crime and moving value through the credit transaction or credit facilities in an attempt to legitimise their illicit origins. Credit-backed money laundering involves using of the following techniques to disguise the illicit origin of money:

i) Front Components
ii) Offshore Corporations
iii) Willful Defaulter
iv) Phantom/ Ghost Mortgage
v) Fund Diversification
vi) Over Valuation of Primary Securities
vii) Over Valuation of Collateral Securities
viii) Fictitious Assets are used as Securities

6.9.1 Vulnerabilities of Credit / Loan & advance Products and Services in Banks/ FIs

Front company/ any person can take different types of loans & advance facilities (Industrial Loan, Transport Loan, House Building Loan, SME Term Loan, Credit Cards facility, personal loan/ car loan/ home loan/loan for Real Estate, Loan against FDR/ Deposit Schemes, SME/ Women Entrepreneur Loan, Overdraft/ Cash Credit Facility/ Short term loan facility/ Loan against Trust Receipt (LTR), Loan against accepted bill etc. from a financial institution and repay the loan from illegal source, and thus bring illegal money in the formal financial system. The money launderers and terrorist financer can use this financial instrument for placement and layering of their ill-gotten money.

6.9.2 CBML Risk Indicators (Red Flags) & Mitigation:

Red **Flags** during **Initial Documentation**: Insufficient &/or Misrepresented information provided:

- Uses fake ID documents
- Provides incorrect address/ different TIN
- Uses inconsistent signatures on Collateral documents
- Misrepresents occupancy / employment status
- False statements related to ownership of Collateral interests
- Business customer does not want to provide complete information about the nature & purpose of its business, anticipated A/C activity, names of its officers/ Directors or business locations

Red Flags for Mortgage Fraud:

- Straw-buyer/purchases home from family member/ friend
- Purchases another home in same community, having no credible explanation
- Short Sale fraud or collusion
- Misrepresented purpose for loan proceeds
- Illegal debt elimination with the use of newly originated loan
- Ambiguous ownership or chain of possession
- Already mortgaged to others.
- Unusual attitude of Surveyor/Lawyer/Land-vehicle registry office/ associated parties

Red Flags Other Suspicious Activity

- Customer repeatedly uses a branch/ booth/Agent point, location that is distant from customer's home or office and without sufficient business/ personal purpose
- Loans secured by pledged assets held by 3rd parties & unrelated to the borrower
- Offering third party's property as collateral security;
- Borrower requests that loan proceeds be disbursed to unrelated 3rd party
- Unwilling to submit required documents for credit facilities
- Counterfeited documents submitted for credit facilities;
- Customer suddenly pays off a large problem /classified loan with no plausible explanation of source of funds;
- Delinquencies related to cash-secured loans or
- Credit customer presents financial statements noticeably different from these of similar businesses; Sudden change in business or transaction activity that is inconsistent with the type of business stated by the borrower
- Large business presents financial statements that are not prepared by a certified accountant;
- Making pressure to enhance credit limit which is not viable according to the volume of business;
- Frequently attempt to enjoy Excess Over Limit (EOL) facility;
- Diversification of credit (fund) facility;
- Application for credit facility for unproductive sector;
- Willing to pay highest profit/ interest rate without any bargaining;
- To secure an investment, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments;
- Borrower defaults on a cash-secured investment or any investment that is secured by assets which are readily convertible into currency.
- Frequently redemption of contract or switch to other forms of loan/investment without proper explanation;
- Making loan/investments decisions and then cancelling immediately and asking for a refund of documents;
- Making repayments in cash to pay off a business or personal loan;

- Unwilling to pay installment (in case of term loan) in due time;
- Willful defaulter. Unwilling to adjust credit facility within due time though the customer is able to pay;
- Adjustment of long terms loan like house building within short time;
- Existing credit facility is adjusted by the third parties;
- Excess amount deposited in credit card than outstanding amount and then claim the additional amount via a cheque or a Pay Order;
- Sanctioning loan to PEP/IP
- Diverting fund to Share market, Family assets, Medical, 2nd home, settling other banks' loans
- Nepotism of Bank officials
- Aggressive Sales-Target & Greed
- Habitual Defaulters - bad intention from beginning
- Poor KYC & CDD
- Buyer -Supplier corrupted or in high risk jurisdiction
- Association with any Predicate Offences etc.

The Regulator raises their concern to detect CBML and advice banks to take necessary steps for mitigating it. Some mitigating factors may include:

Training: Continuous training courses should be arranged focusing Credit backed Money Laundering for the concerned officers (working in this arena) and general staff who can act as whistle blower.

Risk Assessment: Risk Assessment is a process that analyzes a business's risk of risk of exposure to financial crime. The process aims to identify which aspect of the business put it at risk of exposure of money laundering and terrorist financing. It achieves this by monitoring and assessing known vulnerabilities. Being a reporting agency, it is vital for the bank to establish and maintain robust risk management systems and controls to manage and mitigate the financial crime risks arising from credit business.

Sound KYC & CDD: Knowing customers is a key part of the controls required to mitigate credit backed money laundering risks. CDD is particularly important for banks to manage and monitor risks associated with customers on an ongoing basis throughout the relationship. So all concerned Branches & Divisions should undertake appropriate CDD and collect information in accordance with the AML Guideline of the Bank. We have to ensure that there are effective & reliable channels for information obtained during the customer on-boarding and ongoing review processes, which should include information on typical goods the customer deals in. Moreover, collections of following information are necessary:

- Trading partners or counterparties of the customer (including buyers, sellers, consignees etc.)
- Nature of the goods traded
- Country or countries of origin of the goods (including whether the goods originate from any sanctioned country)
- Trade cycle
- Beneficial owner

6.9.3 Review of CBML/TBML/MLTF Risks in Loan Proposal

BFIU is very much concerned about Credit Backed Money Laundering (CBML) & Trade Based Money Laundering (TBML) and they raised their observations & actionable in different inspection reports in this respect. They instructed the Branches/ concerned divisions (such as CBD, SME, CRMD, LRD & TSD, etc.) to review loan proposals considering the risks of money laundering and include the level of CBML/ TBML risk in Credit Proposal/Memo. In this connection, AML&CFTD prepared a sample CBML review format and circulate the same to all concerned, which has been incorporated in the proposal to fill up.

To conduct due diligence on KYC, Risk Grading, Adverse Media News, etc. as per guidelines of AML & CFT provided by BFIU of Bangladesh Bank: (for the client or any of its Director(s) /owner). **Format:**

SL	Area of concern relating to AML&CFT	Yes	No	Remarks
1	Ensured compliance of KYC formalities at the time of onboarding Customer and relevant information properly incorporated in the CBS			
2	CDD/EDD conducted and KYC reviewed within last 6 months; Last reviewed on			
3	Risk Grading reviewed lastly on .....the Customer is graded / possesses Low / High Risk **(Put √)**			
4	Identification process/formalities of Ultimate Beneficial Owner (UBO) has been completed and related information taken & recorded			
5	Checking/ Screening of Adverse Media News has been completed (if any adverse observation detected, please write in remarks column)			
6	Other related comments/ remarks, if any :			

Inadequacies: -.....

So now, Branch Manager/ RM will review the CBML/ TBML/ Adverse Concern of the loan client/ legal person and mention their observations among others in assessment section of loan application or proposal. On the other hand, DAMLCO in CBD, CRM, CAD, LRD will scrutinize, review overall AML comments/ observations of Branch Manager/RM in Loan Proposal (new/renewal/ limit enhancement), Credit Facilities against Trade (LC/LTR/STL/ Packing Credit/LAAB etc.) and assess Money Laundering risk based on documentations, site visit report, business activities/ dealings, financial dealings & other factors and recommend CBML/TBML elements & risk level in CRM Memo. They will also monitor the transactions of loan accounts to ensure whether the fund is being spent for the purpose for which loan amount was sanctioned. In case of suspicion & adverse concern, concerned Business AMLCO will report SAR/STR to ML & TF Prevention Division.

6.10. Digital Transformation of Financial Services

The main theme of the last CAMLCO Conference was (held on 11-13 March 2022) "Digital Transformation of Financial Services: Challenges and Opportunities" where BFIU (Bangladesh Financial Intelligence Unit) gave 16 particular recommendations for banks and related stakeholders. In line with the directives vide letter reference# BFIU (bank monitoring)/16/2022-1215 of 04 April 2022, it was advised from the CAMLCO to all branches & concerned divisions to comply with the recommendations of CAMLCO Conference 2022 as applicable to their respective areas:

- Concerned divisions (OPD, ABD, ICT, RBD or others) of MMBPLC are instructed to perform necessary ML/TF risk assessment before launching new Digital Financial Service/Product with consultation with AML&CFTD/ the CAMLCO and to submit report to BFIU as instructed.
- Card Operation Division (COD) is instructed to strengthen their Card Transaction monitoring and to ensure customer transactions remain within the approved limit of the card. COD also instructed to report STR to AML&CFTD for unusual over limit transactions (if any).
- Concerned divisions -Card Operations Division (COD)/Card Business Division/ Operations Division/ABD are instructed to ensure necessary due diligence (checking eligibility, capability of the probable merchant/Agents) while acquiring merchant/Agents. They are also instructed to keep regular monitoring of their merchant/Agents to identify any suspicion and to report to AML&CFTD accordingly.

- Concerned divisions- Agent Banking Division, AB Ops Unit, Cards Business Division, and Operations Division etc. are instructed to be vigilant to identify any fraud/forgery through Financial Services and to report immediately to BFIU through AML&CFTD.
- All branches and Divisions are instructed to be vigilant regarding monitoring of their customers so that banking channel cannot be used by criminals for transacting in Crypto currency, Online Betting/ gaming & Forex Trading. Also instructed to monitor Social Media/Web content meticulously to prevent such activities of criminals.
- PRD with help of AML&CFT Division is instructed to publish ML&TF awareness message in Social Media.
- MMBPLC, HRD with assistance of AML&CFT Division is advised to arrange necessary training for bank official to increase competency in preventing ML/TF/Cyber crime and Emerging ML/TF Risk.
- HRD, Training wing is advised to arrange training regarding identification and prevention of ML/TF Risk of Digital Transformation of Financial Services with assistance of ML & TF Prevention Division.
- AML&CFT Division will take necessary action in line with BFIU (Bangladesh Financial Intelligence Unit) & AACOBB's (Association of Anti-Money Laundering Compliance Officers of Banks in Bangladesh) guidance.
- Managers of all Branches and Credit Administration Division (CAD), Loan Recovery Division (LRD), SME Division are instructed to check & review their customers' records who received loan under stimulus package to ensure that stimulus funds are utilized as per sanction advice. In case of any deviation/suspicion, STR/SAR to be submitted immediately to BFIU through AML&CFTD.
- Head of International Division is instructed to review all RMA (Relationship Management Application) to ensure there are no Shell Banks and inform AML&CFTD on periodical basis.
- Head of Human Resources Division (HRD) was advised to ensure KYE of all employees of the Bank during recruiting and all Heads of Divisions & Branch Managers are advised to monitor their staff unusual activities including monthly review of transactions in accounts operated by staff (Department of Off-site Supervision (DOS) Circular# 10 of 09MAY17)- so that no employee can abuse the Digital Financial Services of the Bank.
- Operations Division (OPD)/ ABO Unit is advised to review all e-KYC accounts so far opened meanwhile
  to ensure directives of BFIU circular# 25 of 08JAN20 have been properly implemented.

CHAPTER # 7

Wire Transfers & Money or Value Transfer Services

CHAPTER # 7
Wire Transfers & Money or Value Transfer Services

7.1 Wire Transfers

7.1.1 Wire Transfer Related Definitions

Accurate - is used to describe complete information that has been verified for accuracy.

Beneficiary refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

Beneficiary Financial Institution - refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.

Cross-border wire transfer - refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

Complete - refers to combination of all information for verifying the identity of the person or entity. For example: name and detail address of beneficiary/applicant, account number (if any), passport/national ID card/ birth certificate accompanied by acceptable identification certificate with photo/any other acceptable photo ID, phone/active mobile number, etc.

Domestic wire transfers - refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of wire transfer that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country.

Intermediary financial institution - refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

Meaningful - refers to such complete information which are apparently seems to be correct but not verified for accuracy,

Ordering financial institution - refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

Originator/Applicant-refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

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

Transaction Reference - each Cross-border wire transfer must have a Unique Transaction Reference Number (BFIU-26 dated June 16, 2020].

7.2 General Requirements

7.2.1 The requirements under this chapter are applicable to cross-border wire transfers, money or value transfer services (MVTS) and domestic wire transfers including serial payments, cover payments.

7.2.2 Where relevant, references to a "customer" in this chapter include originators, beneficiaries and beneficiary owners of wire transfers or fund transfers.

7.2.3 Branch or concerned Head Office Divisions will ensure each Cross-border wire transfer must have a Unique Transaction Reference Number according to directives of BFIU Master Circular No. 26 dated June 16, 2020. For batch file upload/transactions Unique Transaction Reference Number should ensure also.

7.2.4 Branch or concerned Head Office Divisions must conduct applicable appropriate CDD measures as specified in the chapter four (Customer Due Diligence) of this guideline before making payment of any inward remittance & executing any outward remittance.

7.2.5 Branches or concerned Head Office Divisions are required to conduct enhanced CDD specified in the Chapter six (Customer Due Diligence) of this guidelines for business relationships and transactions with any person or entity from countries identified by the FATF or BFIU as having on-going or substantial ML/TF risk (higher risk countries).

7.2.6 Branch or concerned Head Office Division shall not execute the wire transfer or provide money or value transfer services (MVTS) if it does not comply with the requirements specified in this Chapter.

7.2.7 Branch or concerned Head Office Division must comply the Bangladesh Bank Guidelines for Foreign Exchange Transactions; circulars issued by Bangladesh Bank & BFIU, & other applicable acts, rules & regulations for-executing any cross-border wire transfer.

7.2.8 Branches or concerned Head Office Divisions are required to screen/check the names of the originator(s), beneficiary (ies), beneficiary owner(s), ordering institution, intermediary institution(s) appearing in any wire transfer message or MVTS instruction against the names in the Targeted Financial Sanctions databases of UNSCR, OFAC & BFIU. If there is any name match, it is required to take reasonable and appropriate measures to verify and confirm the identity of name(s) match. Once confirmation has been obtained about the true matching, branches or concerned Head Office Divisions must immediately stop the payment or transfer of fund and report it to AML&CFTD so that the Division can report it to BFIU within next working day.

7.2.9 Branch or concerned Head Office Division are required to maintain all originator and beneficiary information collected in accordance with record keeping requirements.

7.2.10 Branches or concerned HO Divisions shall not undertake any transactions without face-to-face contact with the customer unless the business relationship with the customer has been first established and CDD measures have duly been conducted as per guideline.

7.3 Ordering Banks/Institutions (Banks/Institutions Conducting Outward Remittance)

Cross Border Wire Transfer according to **[BFIU-26 dated June 16, 2020].**

7.3.1 Branches or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all cross- border wire transfers involving an amount USD1000.00 and above or equivalent in any other foreign currency are accompanied by the following information before transmitting the same to Intermediary/Beneficiary Banks:

a. Collected & preserved the complete and accurate originator/applicant information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

(iii) reason for transactions;

(iv) residential or mailing address;

(v) NID/Birth Registration/Any acceptable ID with Photo;

(vi) Phone/Active Mobile No;

(vii) Additional Documents related to Transaction (if required);

b. Collected & preserved the meaningful beneficiary information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and,

(iii) Details Address.

7.3.2 Branches or concerned Head Office Divisions which are the ordering banks/Branch are required to ensure that the message or payment instruction for all cross-border wire transfers involving an amount below USD1000.00 or equivalent in any other foreign currency are accompanied by the following information before transmitting the same to Intermediary/Beneficiary Banks:

a. Collected & preserved the complete and meaningful originator/applicant information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

(iii) residential or mailing address;

(iv) NID/Passport/Birth Registration with any Photo ID;

(v) Phone/Active Mobile No.

b. Collected & preserved the meaningful beneficiary information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and

(iii) Address in Details.

7.3.3 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain Complete and accurate originator information, and beneficiary information, that is fully traceable within the beneficiary country; and Branches or concerned Head Office Divisions are required to include the originator's account number or unique transaction reference number.

7.3.4 Where required information in the paragraph 7.3.1 indicates "Accurate Information", Branches or concerned Head Office Divisions are required to verify that information to ascertain its' accuracy using reliable, independent source documents, data or information.

7.3.5 The meaningful information required under paragraph 7.3.1 and 7.3.2 need not be verified for accuracy except when there is a suspicion of ML/TF.

***Domestic Wire Transfer according to* [BFIU-26 dated June 16, 2020].**

7.3.6 Branches or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all domestic wire transfers involving an amount USD1000.00 and above or equivalent in any other foreign currency are accompanied by the information in the paragraph 7.3.1 a & b for Domestic wire transfer before transmitting the same to Intermediary Banks/Beneficiary Banks/Organizations.

7.3.7 Branches or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all domestic wire transfers involving an amount below USD1000.00 or equivalent in any other foreign currency are accompanied by the information as mentioned in the Section-9 of BFIU Circular No.26 for Domestic wire transfer before transmitting the same to Intermediary Banks/Beneficiary Banks/Organizations.

7.3.8 Where required information in the paragraph 7.3.6 & 7.3.7 indicate "Accurate Information", Branches or concerned Head Office Divisions are required to verify that information to ascertain its' accuracy using reliable, independent source documents, data or information.

7.3.9 The meaningful information required under paragraph 7.3.6 & 7.3.7 need not be verified for accuracy except when there is a suspicion of ML/TF.

7.3.10 Branches or concerned Head Office Divisions which are the ordering banks/Branches are required to collect & preserve documents and information as per paragraphs 7.3.6 to 7.3.9 in addition to KYC format as supplied by Bangladesh Bank Payment System Department vide their circulars time to time.

7.3.11 Branches or concerned Head Office Divisions which are the ordering banks/Branches are required to collect & preserve documents & information as per paragraphs 7.3.6 to 7.3.9 in case of wire transfer using credit or debit or prepaid cards (except purchase of goods and/or service).

7.3.12 It is not compulsory to comply paragraph 7.6.10 & 7.6.11 in case of wire transfers in favor of Government/Semi-government/Autonomous bodies/organizations. Besides these paragraphs are also no applicable for interbank transactions, i.e., where both the applicant and beneficiary are either banks or financial institutions.

7.4 Intermediary Banks/Institutions

7.4.1 Branches or concerned Head Office Divisions which are the intermediary banks/institutions are required to ensure the followings: |

a. For both cross-border wire transfers & domestic wire transfers, intermediary institutions are required to retain all originator and beneficiary information that accompanies a wire transfer.

b. Where the required originator or beneficiary information accompanying a cross-border wire transfer or domestic wire transfer cannot be transmitted due to technical limitations, intermediary banks/institutions are required to keep a record in accordance with record keeping requirements under chapter 13, for at least five years, of all information received from the ordering bank/institution or another intermediary bank/financial institution.

c. Intermediary banks/institutions are required to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

d. Intermediary institutions are required to have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

7.5 Beneficiary Banks/Institutions (Banks/Institutions Conducting Inward Remittance)

7.5.1 Branches or concerned Head Office Divisions which are the beneficiary banks/Branches are required to ensure that the message or payment instruction for all cross- border wire transfers involving any amount are accompanied by the following information before disbursing the amount to beneficiaries:

a. Complete originator/applicant information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;

(iii) residential or mailing address;

b. Complete and accurate beneficiary information such as:

(i) name;

(ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction;
(iii) reason for transactions;
(iv) residential or mailing address;
(v) NID/Birth Registration/Any acceptable ID with Photo;
(vi) Phone/Active Mobile No;
(vii) Additional Documents related to Transaction (if required);

7.5.2 Cross-border wire transfers or fund transfers with inadequate originator/applicant information, Branches or concerned Head Office Divisions which are the beneficiary banks/Branches are required to contact the concerned parties for complete information or may collect complete information from any other reliable & acceptable sources.

7.5.3 Branches or concerned Head Office Divisions which are the beneficiary banks/Branches are required to collect the following beneficiary information at the time of payment of any inward cross-border wire transfer or fund transfer & preserve the same information for at least five years in accordance with record keeping requirements;

7.5.4 Branches or concerned Head Office Divisions are required to verify the information collected in accordance with paragraph 7.5.1 (b) to ascertain its' accuracy using reliable, independent source documents, data or information.

7.5.5 Beneficiary institutions are required to have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking the required originator or required beneficiary information; and (b) the appropriate follow-up action.

7.6 Money or Value Transfer Services (MVTS)

7.6.1 Money or Value Transfer Services Related Definitions

Money Value Transfer Service: Money or Value Transfer Services (MVTS) as defined by the FATF: "Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions."

MVTS provider/MSB: Any natural or legal person who is licensed or registered to provide MVTS as a business, by a competent authority, including through agents or a network of agents.

Agent: Any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.

7.6.2 Responsibilities of MVTS/MSB

Branches or concerned Head Office Divisions offering MVTS/MSB either directly or as an agent to MVTS operators or providers or sub-agent to an agent of MTVS operators or providers are required to comply with all of the relevant requirements under paragraph 7.2.1 to 7.5.5 of this chapter on Wire Transfer (Remittance) of this document in the countries in which they operate, directly or through their agents or sub-agents.

7.6.3 MVTS/MSB - Good Principal/ Agency practice:

Agent "on-boarding" - selecting and appointing an agent

- Sanction Screening test must be completed before appointing agent;
- Complete the CDD procedure according to the chapter 5(five);
- Access the honesty, integrity and reputation of the beneficial owner and managers of the agent;

Agent "Monitoring"

- Adopt and apply a written policy to assess the risk of potential agents;
- Document the assessment of each agent risk;
- Establish expected levels of transactions for each agent;
- Monitor the agent's transaction on regular basis;

Agent "Training"

- Train agents and all their staff who access the principal's systems, assessing agents and staff to ensure that training messages have been understood and applied to an appropriate standard;

System and IT security

- Operate a system to ensure that exclusive passwords are issued to and used by each agent and relevant staff on an individual basis.
- Ensure that access to network systems is only allowed during opening hours agreed with the principal.

Agent "De-listing"

Principal/ ABD should circulate the name of the de-listed agents in their web sites due AML & CFT non-compliance or KYC/CDD issues;

7.6.4 Where the Branches or concerned Head Office Divisions offering MVTS/MSB control both the ordering and the beneficiary side of a wire transfer, the Branches or concerned Head Office Divisions are required to:

a. all Authorized Subsidiaries/Agents must ensure the implementation of directives of BFIU, Bangladesh in connection with MLPA-2012 (including all amendments -2015) and ATA-2009 (including all amendments-2012 & 2013), due to any conflict with the operating country law, the respective should informed to the Principal according to BFIU-23 date January 31,2019;
b. taking into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and
c. file a suspicious transaction report (STR) when detected any suspicious wire transfer, and make relevant transaction information available to respective compliance division/department/CCC for ultimate submission to Local/oversees concern regulatory body (i.e. BFIU, FCA/HMRC/NCA, MAS, Hong Kong Customs Authority & other competent authority).

Chapter # 8

TRANSACTION MONITORING

Chapter # 8
Transaction Monitoring

8.1 Regulatory Directives

As per section 5 of the BFIU Circular# 26 of 16JUN2020, the regulator expects:

- All banks will regularly monitor their customers' transactions manually or automated process,
- The transactions that are -- complex, inconsistent to normal and apparently there is no economic & legal purpose – those need to be monitored with additional effort/ care to evaluate and detect suspicious elements from the transaction and initiate STR/SAR. It should be considered indicators of suspicious transaction / activity as stated in 'Guidance on Reporting Suspicious Transaction and also in Guidance on Trade based Money Laundering.
- Transacting Branch should be more alert on transaction monitoring to detect structuring as mentioned in MLP Act 2012 section 2 (Fa & EE);
- Consider transaction monitoring for all foreign trade & foreign currency related transactions and also all electronic/ online cross border transactions;
- Transactions in High-Risk Accounts and in A/Cs classified as high-risk identified in periodical Risk-Assessments –to be monitored with Enhanced Due Diligence.
- Transaction screening with local and UN Sanction list and also transactions with persons / entities of non-complied / low complied jurisdictions;

As per section 6.5 of the Money Laundering & Terrorist Financing Risk Management Guideline of BFIU (15 September 2015) - Banks should put in place various ways of transaction monitoring mechanism within their branches that includes but not limited to the followings:

- Transactions in local currency;
- Transactions in foreign currency;
- Transactions above the designated threshold determined by the branch;
- Cash transactions under CTR threshold to find out structuring;
- Transactions related with international trade;
- Transaction screening with local and UN Sanction list.

Banks needs to monitor the transactions of customer on a regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized during monitoring. An effective system has to be developed by the banks to review the risk by maintaining a specific time interval; and according to the review, Enhanced Due Diligence has to be maintained for accounts that are in high risk category.

Based on the above MMBPLC conducts Transaction Monitoring in the following manner:

8.2 Staff-awareness & Overall Semi-Automated Transaction Monitoring System

MMBPLC has a strategy to ensure transaction monitoring through staff's careful vigilance & awareness and executing them various semi-automated tools with sincere dedication. Thus, staff awareness is continuously nourished. On Automated part, MMBPLC uses Ultimus Software at all relevant stages to monitor all parties and transactions to ensure checking against all relevant official sanction-lists. Similarly, our in-house ICT Division has arranged a real-time checking of Transaction against local customer's declared Transaction Profile (TP) by customizing Ultimus Software. But for other exception transaction monitoring, we rely on some monthly/daily exception reports – that are designed & generated by our in-house ICT Division. All these are systematically followed-up through on-going Monitoring by the AML&CFT Division.

8.3 Monitoring methodology comprises two components such as:

a) Monitoring performed by staff who deals directly with customers or processes customers transactions
b) Regular reviews of past transactions to detect unusual activities

8.3.1 Monitoring by front-line Staff

Front line staffs are the persons who know most about the customers and their typical pattern of transaction activities. They are in the best position to trigger unusual transactions/transaction's activities & contribute to branch transaction monitoring system. All staffs are made aware of the **"Red-Flags"** *(as per **Annexure-3, 4 and also 14**)* in various refresher trainings. So, they are apt on identifying customer's any unusual activities – including lack of producing required documents like Photo-ID in case of transaction by non-customers, lack of explanation, positive pay verification, different pattern i.e. large or structured cash & behavior, etc. Staff are advised to keep annotation written by customer/ or his bearer or by staff himself on the overleaf of the Cheque or deposit /transfer voucher - the reason/source fund as appropriate during any TP limit breach or any apparently unusual transaction including any relatively large cash transaction. Besides on the day to day dynamic triggers i.e. vigilance by staff over-the-counter also leads monitoring. Staff raises issues to the BAMLCO and if required those transactions are further scrutinized by the AML&CFT Division.

8.3.2 Real-Time Monitoring of Transaction Profile (TP)

MMBPLC's real-time transaction monitoring against (TP) is another very important & successful monitoring tool that enables the operating staff to monitor a transaction that exceeds – customer's declared limit and the system does not allow proceeding until the explanation /document provided by the customer is not acceptable to the Supervisor/ BAMLCO. This sometimes warrants further review of additional documents &/or Revision of Transaction Profile or leading to SAR/STR.

All Branches and concerned Divisions will check alerts of Transaction Monitoring every day; review transaction activities and perform *following* 2 (two) tasks:

1. in case suspicious transaction(s), conduct CDD/EDD, decide whether to raise STR/SAR based on the gravity of CDD/EDD information/documentation(s) and do others formalities accordingly to initiate STR/SAR;
2. In case of normal transaction (matched with profession or normal activities), keep record for False Positive and close the alert.

8.3.3 Sanction Monitoring

As mandated under section 10 of the BFIU Master Circular 26, MMBPLC ensures through its Sanction Screening tool **"S3"** (from Leads Corporation) at all relevant stages that Parties and transactions have been checked against all relevant official sanction-lists. Therefore, decision page of checking in S3 with remarks to be retained even for false (negative) match – during Opening A/Cs, Cross-border Transactions, trade transactions, paying out to Walk-in customers, etc. with AOF or main vouchers, as appropriate. If it is an exact (positive) match i.e. fully matches, the A/C or Transaction to be stopped immediately and reported to BFIU via AML&CFT Division not later than next working. During analysis special care to be taken to cross check with-- Date and Place of Birth/ Registration, Identification/ Registration/Vessel Number, Nationality/Citizenship, probable links/news with our customer & the Hit-name, etc. For better management of critical trade transactions by preventing fraud, malpractice & /or any potential sanction related issues – reviewing due diligence report from open Source web / Google, as the is yet to subscribe any related query service automated platform). If required AML&CFT Division should be also consulted during such monitoring & screening. Such Sanction screening false/ positive – result must be retained for 5 years for regulatory audit, in general.

Sometimes there are Trade-embargo (though not straight sanction but restriction, like ours Israel, & USA's BIS or EAR (Export Administration Regulations); so for geo-political conflicts staff should be extra cautious during proceeding for any transactions among those jurisdictions for which later our bank or valued customer may face legal or financial loss. Similarly, no effort to be entertained which might be treated as 'Circumvention of Sanction Law', e.g. changing/ deleting name of sanctioned party, using jargons, changing route / bank/ currency to avoid sanction party in the transaction.

8.3.4 Adverse Media News Monitoring

As instructed by BFIU, MMBPLC monitors the Adverse media news daily (MMBPLC subscribed adverse news services from Hawkerbd.com from July 2020) – and search its customer database and lodge STR/SAR, if warrants. Particularly for Terrorist Financing (TF) related news- importance given on urgent review & immediate reporting to BFIU (not later that next working day). Once there is a potential link/ part or full match noticed – the respective branch conducts through review of the Customer's KYC docs including site visit, transactions roughly for 5 years, probable link with adverse news, conducts local intelligence review and raise STR to AML&CFT Division– if there is reasonable concern. We seek guidance from BFIU on whether to put Hold/ Restriction on such sensitive A/Cs to keep further enhanced monitoring. To make the adverse news screening more robust, MMBPLC is in the process of maintaining a Local private listing where sensitive individuals/entities with adverse media news &/or suspicious concerns are listed and to be screened using **"Sanction Screening Software- S3".**

8.3.5 Monitoring of Exception Reports

MMBPLC has implemented some internal Exception Reports designed & generated by its capable in-house ICT Division under guidance from the AML&CFT Division to monitor its customer's transactions also in post facto basis to allow more time & prudence to review the alerts and raise STR accordingly. The following are the Monthly & Daily Exception Reports that are designed in such a manner on Risk Based Approach that ideally covers the probable sensitive Transactions & patterns that have potential vulnerability on AML/CTF aspect. For easy reference & smooth operational process – MMBPLC has prepared some operational flow-charts for monitoring of exception reports. Branch officials should follow these flow-charts for escalating SAR/ STR to AML&CFT Division and/or document their work for any audit trail/ checking.

8.3.6 Transaction Profile (KYC) Exception Report

Respective Official of Branch as assigned by the BAMLCO/ Manager generates the Transaction (KYC) Exception Report. As customer needs to declare his probable monthly - number & volume of transactions in different channels on BFIU prescribed template in the AOF, MMBPLC captures same in the Ultimus during A/C opening. Accordingly, when a customer conducts a transaction the system in the back-end verifies the declared limits and alerts the Transaction-Operator if the said transaction breaches his declared TP limit. As stated above, the operator exercises due diligence with the customer, if explanation & supporting documents provided by the customer acceptable Supervisor/ BAMLCO document the same & allow the transaction; if not customer gives written declaration & commit to provide document. BAMLCO consulting AML&CFT Division may lodge STR immediately based on gravity of the issue or later - if the customer does not provide further docs or revise TP with supporting documents. Upon receipt of the Exception Report BAMLCO conducts almost same exercise on post & Risk-Based Approach (e.g. deviation in percentile, frequency, etc.). So if any particular customer's TP is frequently breached &/or with high volume transactions –that warrant EDD & STR as appropriate.

8.3.7 Cash Transaction Report (CTR):

As prescribed in section 6 of the BFIU Master Circular#26, Banks need to report on Monthly basis, cash transaction/s (either debit or credit) in an A/C that is equivalent or above BDT 1miilion in a day and also to review these high-value transactions to ascertain whether there is any unusual

transaction/pattern – thus this report is generated. AML&CFT Division collates the report & with help of IT assigns this monthly Report to the Branch Managers/ BAMLCOs' system's queue – who need to analyze them on Risk-Based Approach (e.g. volume, pattern, frequency, etc.).

MMBPLC Branches generates CTR error report on first day of every month which consists of accounts which has KYC deficiency in Ultimus. BAMLCOs must ensure CTR with KYC error free and also occupation details and bearer information are properly filled. AML&CFT Division has given directives on how to capture Bearer & Director Information in Ultimus.

In line with Section 6.4 of BFIU's Circular, AML&CFT Division instructed branches to review accounts reported in CTR and raise STR/SAR if any unusual/ suspicious transaction detected and after that confirm reviewing all CTR transactions to AML&CFTD. So, if any particular customer's cash-transactions frequently breaches CTR limit &/or with unusual pattern and with no justified grounds –that warrant EDD & STR as appropriate.

Branches have to preserve record of monthly CTR upon monitoring (if any Bank generate & preserve CTR in any module centrally, Branches should allow easy entry into the system.

As per BFIU section 6.6 of Master Circular, there is no requirement of cash deposit in collection account of school, college & Govt Utility (Gas, Electricity, Water) collection, but it should come in CTR the transaction of Cash withdrawal.

8.3.8 Monthly Exception Report on Structuring:

As BFIU advises Banks to detect Structuring & lodge STR accordingly, MMBPLC also designed & implemented an Exception Report on this. Customers frequent cash transactions intentionally or unintentionally if conducted just below the CTR limit – as if purported to avoid regulatory reporting; these indicate significant concern and thus warrant enhanced monitoring and reporting to Regulator as suspicious, through AML&CFT Division, as appropriate. Structuring i.e. the splitting up of a large cash deposit into a number of smaller deposits (i.e. below the CTR threshold/limit) to evade the suspicious activity reporting requirement of the Bank can be done by:

- Regular deposit of cash into accounts in amounts that fall below the reporting threshold;
- Regular use of cash to purchase "instruments" such as bank cheques and bank drafts, or to load into credit or stored value cards in amounts below the reporting threshold;
- Using multiple branches or agencies, often within a short timeframe, to avoid detection;
- Establishing accounts at multiple bank/branch;
- Using third parties to make deposits into a single account or multiple accounts.

8.3.9 Exception Report on Transaction in Student/ Housewife Account

As local industry has experienced some major cases of disguising &/or siphoning of illegal fund by the ultimate "Beneficial-Owner (BO)" s through their spouse or children's A/C; thus, MMBPLC has prudently designed & implemented this exception report. BAMLCOs need to verify the transactions that are above the internal limit, against the profile of the customer & his/ her 'BO's occupation, income & other circumstances and report if appear unusual to the AML&CFT Division. On Risk Based Approach (RBA) MMBPLC Branches (in cooperation of AML&CFTD & ICT) generates transactions for Tk.5.0 lac or above for Student/Housewife Accounts on every month end. BAMLCOs and also AML&CFT Division reviews transactions of these accounts for any suspicious transactions –that warrant EDD & STR as appropriate. For easy reference & smooth operational process – MMBPLC has prepared some operational flow-charts for monitoring of exception reports of Student/ Housewife Account. Branch officials should follow these flow-charts and document their work for any audit trail/ checking.

8.3.10 Deposit Movement Report

Branch Managers typically gets this report on daily basis in their system-queue and besides their concern of siphoning of large deposit from his branch- it is an excellent tool to alert his team & CAMLCO on any unusual large transaction that may have ML vulnerability. The report also includes cash transactions which ensure large cash transaction under radar. This report can be monitored on Daily & Monthly basis.

8.3.11 Remittance Monitoring Report

MMBPLC has in process to implement some internal Exception Reports designed & generated by its ICT Division under guidance from the AML&CFT Division to monitor incoming remittance transactions in post facto basis to allow more time & prudence to review the alerts and raise STR accordingly. On every month-end, reports are generated for incoming remittance transactions in high frequency, threshold based, same beneficiary and high-risk jurisdiction & customers on RBA. The exception reports are then reviewed by Foreign Remittance Division with respective Branches and AML&CFT Division for any unusual transactions that may have ML vulnerability.

8.3.12 Remittance Monitoring through Sanction screening Software S3.

Branch & International Division (ID) will monitor the inward outward remittances under transaction monitoring using software named "S3". If any suspicion arises about any activity in the account, SAR/STR is raised.

International Division (ID) of the bank centrally handles the Remittance services through SWIFT and they conduct their due diligence (or Name Check) and send the branch specific report to respective branches for follow-up. For inward remittance, that are collected by customer over-the-counter; Branch conducts screening in S3 & standard KYC and related screening result, KYC (short), supporting document, etc, are preserved with vouchers. Similarly, for, FCY Demand Draft or Dollar Endorsement related screening result, KYC (short), supporting document, etc., are preserved with vouchers in AD Branches.

8.3.13 Transaction Monitoring of High-Risk Accounts:

As stated above, regulator expects banks to conduct enhanced monitoring in High Risk Accounts, thus AML&CFT Division has designed a mechanism and MMBPLC's ICT Division is in the process of finalizing the same for implementation, where certain accounts will be marked in Ultimus as High-Risk A/Cs on Risk Based Approach. This will automatically enable Branch /respective unit to conduct enhanced monitoring at relevant stages. Currently Staffs are aware and typically putting more emphasis on accounts of PEP/IP/HoIO and those are equal & above of 14 (as per new circular, it will be 15) in KYC Risk Scoring (part of AOF CDD). In general staff will conduct enhanced monitoring on all such High-Risk A/Cs as stated above and lodge STR, if required. Recently concerns on "Shell-Banks" have emerged in the industry; hence we must ensure - no trade or remittance transaction is processed through any such shell-banks/companies. Similarly, during Writing-off any Loan – staff must critically review that, no fund has been siphoned outside or used in any unethical/ illegal ground.

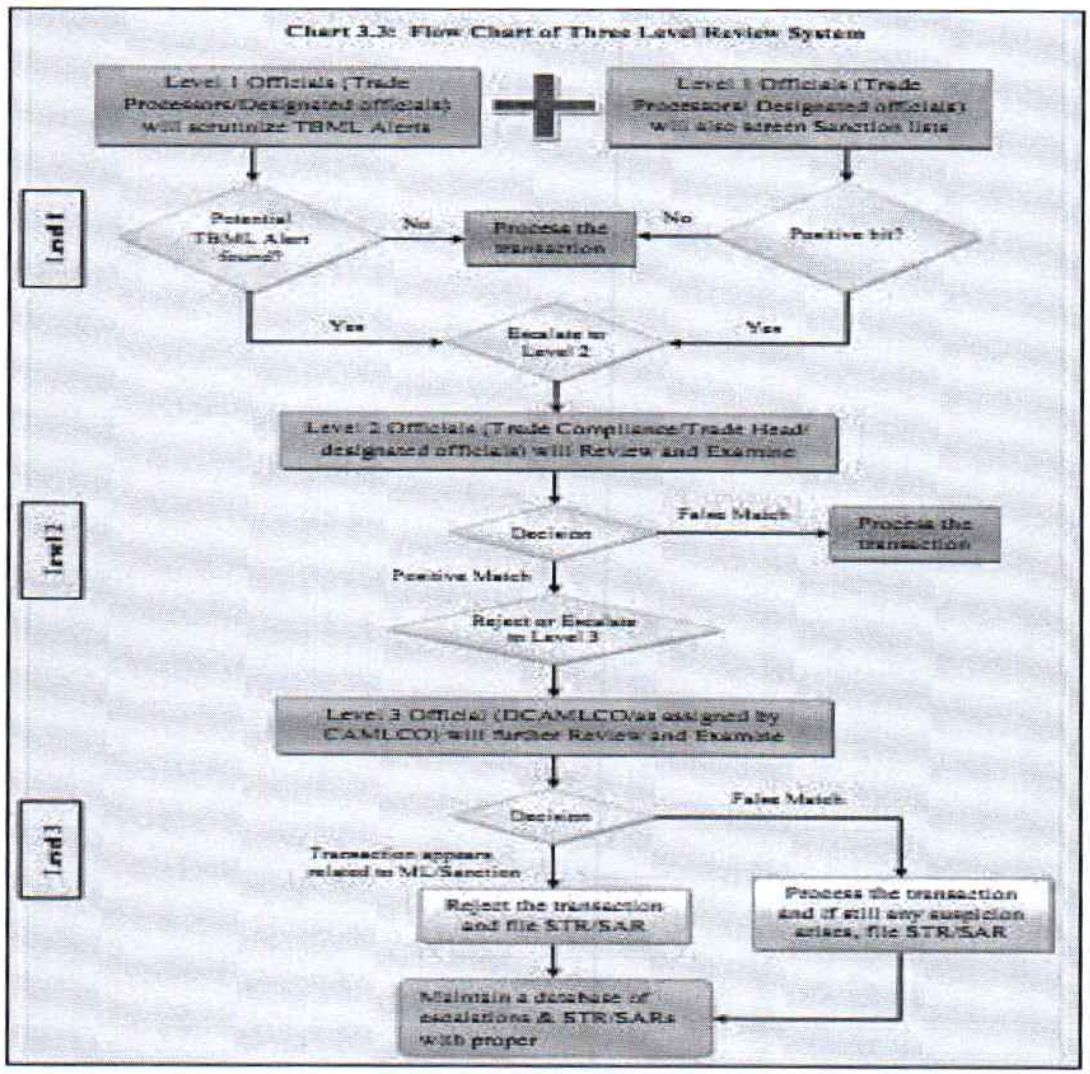
In connection to above & to assist branches performing Annual Review of High-Risk Accounts and Enhanced Due Diligence (EDD), AML&CFT Division has formulated a template and circulated through email.

8.3.14 Monitoring of Unusual Relationship/ Transaction in Virtual Currency/ Unauthorized Currency:

With new concern of Virtual Currency which has been made illegal by the Central Bank of Bangladesh and accordingly MMBPLC issued a related circular to make its staff aware not to get involved in such relationships and if detected to be reported to the regulator via AML&CFT Division. Any client conducting any dealing in any currency without the approval from Bangladesh Bank or not having 'Authorized Dealer (AD) License will be strongly prohibited, reported to regulator and will be exited. Similarly, any unusual transaction noticed in internet banking or in on–line banking or any on-line gaming, MLM or unauthorized activities, etc. are identified; instantly it has to be escalated to AML&CFT Division for further action.

8.4 Trade Base Money Laundering (TBML)-Alert Monitoring and Reporting Unusual Transaction/ Activity:

KYC process is the foundation on which the individual transaction will be evaluated/ examined for TBML Alerts. As part of risk-based approach Trade Officials of Level-1 will check for "TBML Alerts" regularly to identify, escalate and examine unusual/suspicious activities. The details procedures also covered under the Chapter-3 (Risk Based Approach and TBML Controls) of MMBPLC Guidelines for Prevention of Trade Based Money Laundering'. Mentionable that 1st Line of defense of Trade Service in Br/TSD in HO will evaluate the risk assessment considering Credit Report, line of business, involvement of shell companies, Tax haven jurisdiction, Price verification, level of sanction involvement of a particular legal person/ entity & determine risk level and if necessary, escalate issues to 2nd line of business. In case of suspicious issues, 2nd level of defense will escalate along with necessary findings & observation (in details) to 3rd line of defense for resolving particular issues. Besides, all concerned will report/ submit STR/SAR complying procedure shown in the following Chart:



Before submission of STR/SAR, D-CAMLCO (if not level 3) and CAMLCO shall only ensure compliance with instructions of relevant BFIU circular. Risk of tipping off should also be managed. Bank shall always file an STR/SAR when required to do so under MLPA, ATA and relevant BFIU circulars. In complex situations opinion may be seek from BFIU.

8.5 Credit Based Money Laundering (CBML)- Alert Monitoring & Reporting Unusual Transaction / Activity:

Bank will perform appropriate transaction monitoring to be able to detect any activity that is not consistent with the purpose of the services provided to the client or which is not in line with the usual or expected activities of the client. As part of transaction monitoring, bank official shall monitor flow of funds not directed to sanctioned entities and countries, to safeguard it from being used as a channel for financial crime. Transaction monitoring to be conducted for both AML and CFT purposes and bank staff will consider the scenarios, parameters and red flags used for the monitoring of the client's activities. At the initial stage or during the course of any trade finance transaction, if it becomes aware that the transaction presents higher financial crime risks or it is suspicious in nature, concerned branches/ divisions have to escalate the unusual issues to AML&CFTD timely for reporting to BFIU in this respect. BM/RM, CAD, CRM, LRD as appropriate, to regularly monitor end-use of provided loans and raise early-alerts to AML&CFTD. Besides Half-Yearly Self-Assessment Template requires some statistics in the following different format from Bank such as:

১৯.বাণিজ্যভিত্তিক মানিলন্ডারিং প্রতিরোধে গৃহীত ব্যবস্থাদি ঃ

রিপোর্টিং ষান্মাসিকে বিল অব এন্ট্রি ওভারডিউ থাকা কেওয়াইসি পর্যালোচনা কওে কোনো সন্দেহজনক লেনদেন চিহ্নিত করা হয়ে থাকলে তার সংখ্যা	রিপোর্টিং ষান্মাসিকে রপ্তানিমূল্য অপ্রত্যাশিত থাকা কেওয়াইসি পর্যালোচনা করে কোনো সন্দেহজনক লেনদেন চিহ্নিত করা হয়ে থাকলে তার সংখ্যা	রিপোর্টিং ষান্মাসিকে TBML এর উপর প্রশিক্ষণ পেয়েছে এরূপ কর্মকর্তার সংখ্যা

২০. শ্রেণিকৃত ঋণ হিসাব পর্যালোচনা ঃ

বিগত ষান্মাসিকে শ্রেণিকৃত ঋণের মোট পরিমান (লক্ষ টাকায়)	রিপোর্টিং ষান্মাসিকে শ্রেণিকৃত ঋণের মোট পরিমান (লক্ষ টাকায়)	শ্রেণিকৃত ঋণ হিসাব পর্যালোচনায় কোন এসটিআর/এসএআর করা হয়ে থাকলে তার সংখ্যা

২১.অবলোপনকৃত ঋণ হিসাব পর্যালোচনা ঃ

বিগত ষান্মাসিকে অবলোপনকৃত ঋণের মোট পরিমান	রিপোর্টিং ষান্মাসিকে অবলোপনকৃত ঋণের মোট পরিমান (লক্ষ টাকায়)	অবলোপনকৃত ঋণ হিসাব পর্যালোচনায় কোন এসটিআর/এসআর করা হয়ে থাকলে তার সংখ্যা

২২.রেমিট্যান্স পর্যালোচনা ঃ

রিপোর্টিং ষান্মাসিকে প্রেরিত রেমিট্যান্স পর্যালোচনায় কোনো এসটিআর/এসআর করা হয়ে থাকলে তার সংখ্যা	রিপোর্টিং ষান্মাসিকে আনীত রেমিট্যান্স পর্যালোচনায় কোনো এসটিআর/এসআর করা হয়ে থাকলে তার সংখ্যা

Mentionable that Regulatory rating of Bank including CAMELS rating depends a lot on the health of above indicators. Therefore, all the concerned Branch Managers/Divisional Heads will ensure the reviewing/ monitoring of CBML/TBML/Remittance alerts and raise STR/SAR in handsome numbers to safeguard Bank from AML/CFT risks as well as to contribute in development of Bank' Rating.

CHAPTER # 9

New Technologies: Credit Card, Debit Card, Prepaid Card, Internet Banking and Alternative Delivery Channels

CHAPTER # 9
New Technologies: Credit Card, Debit Card, Prepaid Card, Internet Banking and Alternative Delivery Channels

9.1 New Technology –

Technology-based innovations have radically changed the financial industry due to the emergence of new services and products, which has allowed the creation of opportunities for growth and efficiency, and at the same time, it improves the access and delivery of financial services and products to people, businesses and communities (customers/occasional customers) excluded or unattended from the current financial system, promoting financial Inclusion.

It is important to prevent the misuse of the financial system through the new services and products that technology-based innovations offer to the public such as new tools and vehicles for the commission of money laundering and terrorist financing (ML/TF).

FATE Recommendation 15	New Technologies: identify and **assess** ML/TF risks relating to the development of new products and new business practices and the use of new or developing technologies for both new and preexisting products.
Obligations under BFIU Circular-26 [section 3.16] dated: 16-06-2020	Every bank shall establish a procedure to identify and assess ML/TF risks relating to the development of new products and new business. Practices and the use of new or developing technologies and should have a mechanism to prevent ML/TF.

9.2 New Technology Related Definitions

Automated Teller Machine (ATM) - an automated teller machine (ATM) is an electronic banking outlet, which allows customers to complete basic transactions without **the** aid of a branch representative or teller.

Cash Deposit Machine (CDM) - the Cash Deposit Machine (CDM) is a self-service terminal that allows customers deposit cash & cheque directly in their account (MMBPLC is yet to introduce its own machine)

Credit Card- a Credit Card is a secured chip-based card issued as **a** payment instrument by a financial institution that allows its user to borrow pre-approved fund at the point of sale in order to complete a purchase or withdraw cash from ATM or counter of the financial institute.

Debit Card - a Debit Card is a secured chip-based card issued as a payment instrument by a financial institution that deducts money directly from **a** consumer's checking account **for** payment of **a** purchase or withdrawal of cash.

Internet Banking- Internet **Banking is a system** which **allows** customers to perform banking activities any time anywhere through the internet.

Mobile banking/arrangement with MFS Providers - Mobile Banking is a package of mobile financial services provided by a bank or other financial institution that allows its customers to conduct a range of financial transactions remotely using a mobile device such as a mobile phone **or** tablet, and using software, **usually** called an app, provided by the bank or financial institution for the purpose. Like MMBPLC has transaction arrangement with Bkash & UPAY.

Prepaid Card - a Prepaid Card is a secured chip-based card issued as a payment instrument by a financial institution that is preloaded with funds which can be used for payment of a purchase or withdrawal of cash. The nature of a prepaid card is somewhat opposite of a normal credit card because instead of buying something with borrowed funds (through credit), customers buy things with funds that have already been deposited (prepaid) in the card.

Point of Sales (POS) - the Point of Sale (POS) is the time and place where a retail transaction is completed. It is the point at which a customer makes a payment to the merchant in exchange for goods or after provision of a service. (MMBPLC is yet to introduce)

SMS Banking - Short Message Service (SMS) Banking is a service that allows customers to access their account information or make basic transactions via push-pull SMS services through mobile phones.

9.3 New Technology Related Products and Services & Their Vulnerabilities:

Credit cards are unlikely to be used in placement stage, but their use in the later stages of money laundering is unknown. Credit card accessed accounts in offshore banks create vulnerabilities to money laundering. Industry focus is on fraud and credit risk, not money laundering. Acquirers use fraud and credit risk policies and controls that they believe address money laundering among merchants. Major card processors use fraud focused policies and programs to support clients AML efforts. Regulatory oversight of issuing and acquiring banks credit card operations is focused less on AML requirements because of lower perceived risk. Associations and third-party processors have not been subject to AML related requirements or oversight.

9.4 Challenges facing in handling Card Payment Systems:

- ***Challenges from Customers:*** Being a force sale product card is given on fund/income particulars and it is difficult to access illegal source of fund if customer dose not disclose or willing to cooperate.
- **Technological *Challenges:*** CMS are well equipped with fraud monitoring tool and less focused on AML activities.
- **Management and *Operational Challenge:*** After placement and layering, it is difficult to find out suspicious activities from card payment system.
- **Others:** Lack of adequate training and course of actions.

9.5 The mitigation techniques to handle money laundering vulnerabilities in the Local, International Credit Card and other technology-based products:

Branches or concerned Head Office Divisions who introduced the customer for technology-based product of MMBPLC, the following KYC process should follow for non-account holder and account holder customers before providing technology-based services:

a. Non Account holders / Account holders:

(i) Complete sanction screen process and obtain report;
(ii) Legal agreement with customers for technology-based product/services;
(iii) Assess the money laundering risk;
(iv) Complete the CDD process
(v) Complete the EDD process based on risk profile of the customer
(vi) Obtain approval from senior management in case of PEPS/IPS;

9.6 Transaction/Customer Monitoring:

Once the card has been issued, Issuers/Bank must establish an effective transaction monitoring framework as part of ongoing due diligence. We should seek the opportunity to develop and, where appropriate, integrate our AML monitoring scenarios with other systems.

Transaction Monitoring:

- Frequent and unusual use of the card for withdrawing cash at ATM;
- Structuring payments/Overpayments: balances on cards may move into regular credit where card holders pay too much or where merchants give credits to an account.
- Unusual cash advance activity and large cash payments: the monitoring of incoming cash is critical, as excessive cash payments are often an attribute of money laundering.

- Transactions from High Risk jurisdiction or frequent transactions from offshore Tax Haven;
- Unusual purchase of goods or services in countries regarded by an institution as posing a heightened risk for money laundering;
- Purchases at merchant on personal cards which are significantly out of pattern with historical spending behavior;

Customer Monitoring

- Abnormal customer contact behavior (e.g., frequent changes of address).

Card Account Settlement:

- Multiple and frequent cash payment or money orders; large, cross-border wire transfer payments;
- Settlements/partial settlements from unrelated third parties;

9.7 Card Account Closure & STR/SAR reporting:

Based on the severity or Risk Appetite or frequency of suspicious activity, it **may be** appropriate, where legally permissible to exit a card relationship. MMBPLC shall report STR/SAR or exit card relationships after suspicious activity is detected and reported or **after** negative customer information is identified. MMBPLC shall not asked/notify customer further information to avoid the risks of "tipping off" the card holder. MMBPLC Card Division or ADC will proactively notify to AML&CFT Division for suspicious activity/transaction of Card holders.

CHAPTER # 10

RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS (STR)/ SUSPICIOUS ACTIVITIES (SAR)

CHAPTER # 10
RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS (STR)/ SUSPICIOUS ACTIVITIES (SAR)

RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ SUSPICIOUS ACTIVITIES

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk for bank. So, it is necessary for the safety and soundness of the bank. Guidance on Reporting Suspicious Transaction Report (STR) is annexed ***at Annex-9.***

10.1. DEFINITION OF STR/SAR

Generally, STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seeming to be usual manner. Such report is to be submitted by financial institutions to the competent authorities.

In the section (2)(z) of MLPA, 2012 "suspicious transaction" means such transactions which deviates from usual transactions; of which there is ground to suspect that,

(1) the property is the proceeds of an offence,

(2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;

(3) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh bank from time to time.

10.2 OBLIGATIONS OF SUCH REPORT

As per the Money Laundering Prevention Act, 2012, banks are obligated to submit STR/SAR to Bangladesh Bank. Such obligation also prevails for the banks in the Anti-Terrorism Act, 2009 (as amended in 2012). Other than the legislation, Bangladesh Bank has also instructed the banks to submit STR/SAR through AML&CFT Circulars issued by Bangladesh Bank time to time.

10.3 REASONS FOR REPORTING OF STR/SAR

As discussed above, STR/SAR is very crucial for the safety and soundness of the financial institutions. The financial institutions should submit STR/SAR considering the followings:

- It is a legal requirement in Bangladesh;
- It helps protect the reputation of banks
- It helps to protect banks from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

10.4 IDENTIFICATION AND EVALUATION STR/SAR

Identification of STR/SAR is very crucial for banks to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place by the banks. Such suspicion may not only at the time of transaction but also at the time of doing KYC and attempt to transaction.

10.4.1 Identification of STR/ SAR:

Identification of STR/SAR may be started identifying unusual transaction and activity. Such unusual transaction may be unusual in terms complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally, the detection of something unusual may be sourced as follows:

- Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable

explanation.

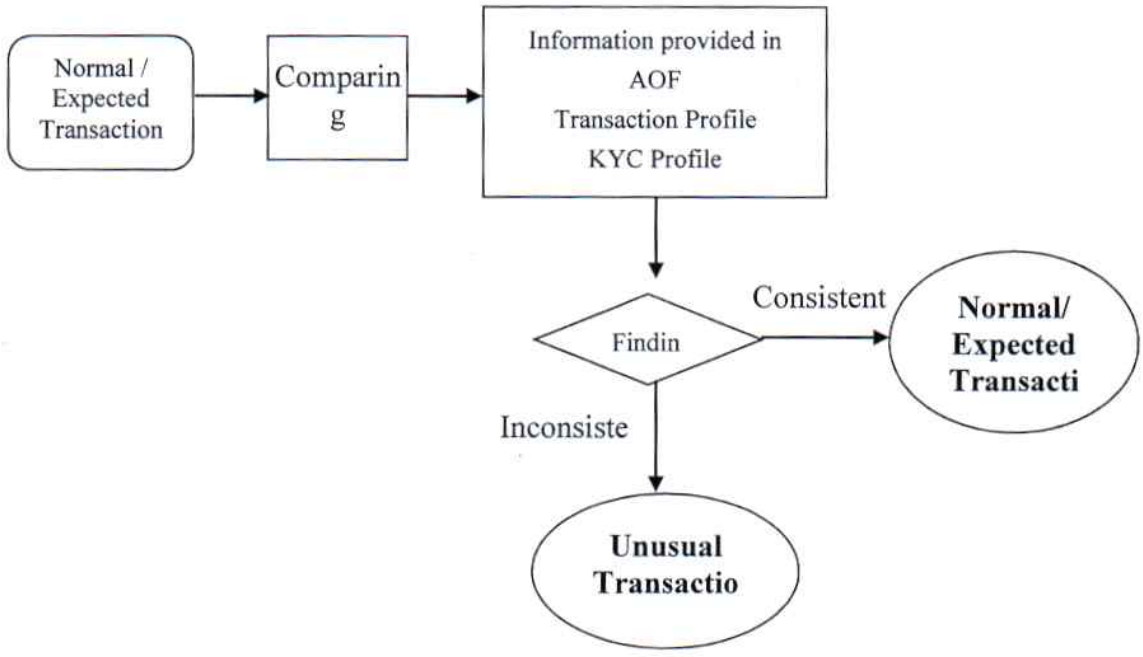
- By monitoring customer transactions.
- By using red flag indicator.

Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.

As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, FIs should conduct the following 3 stages:

a) Identification:

This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented managerial oversight and not be replaced the need for constant monitoring of activity of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution and supported by adequate information systems to alert management and other appropriate staff (e.g., the compliance officer) of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity. Considering the nature of business FIs must be vigilant in KYC and sources of funds of the customer to identify STR/SAR.



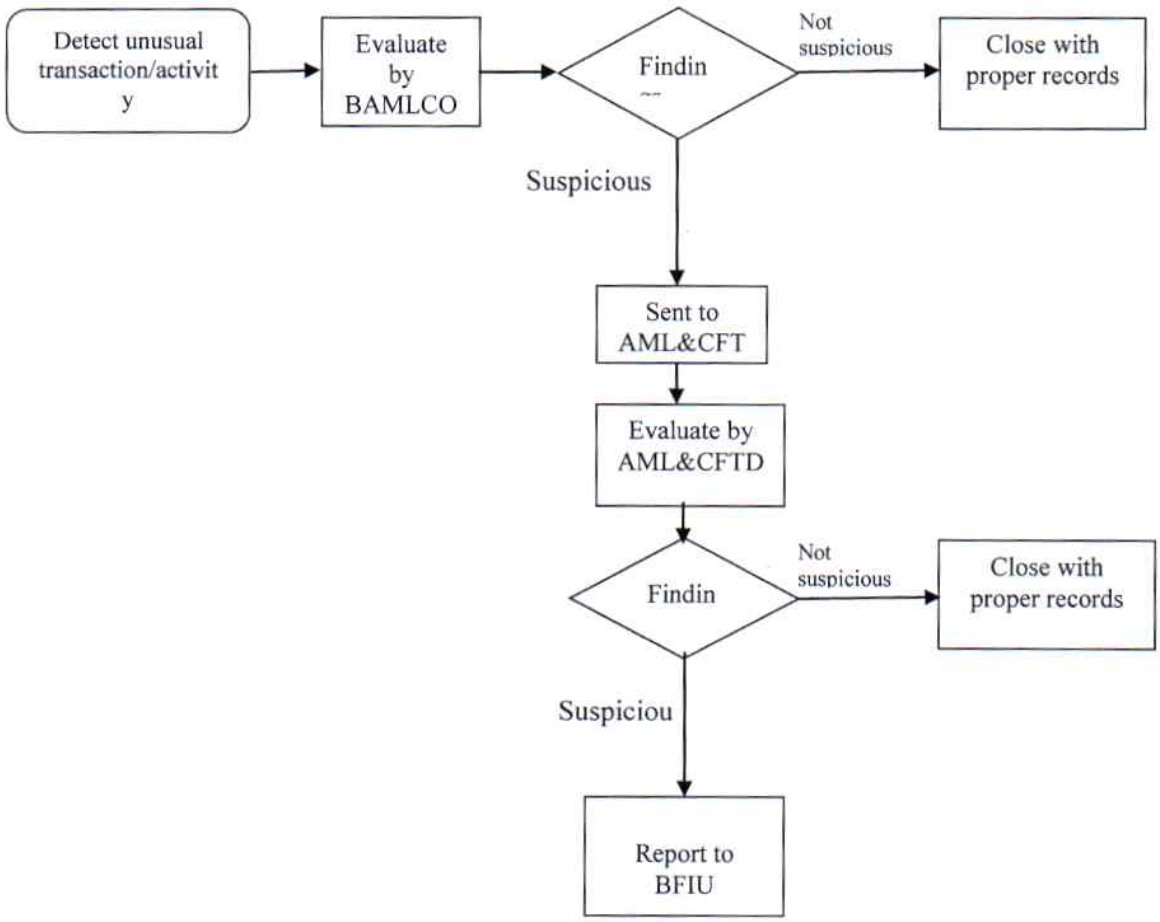
b) Evaluation:

These problems must be in place at branch level and Anti-Money Laundering Division (AML&CFTD). After identification of STR/SAR, at branch level BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BAMLCO must be tactful considering the tipping off provision of the acts. If BAMLCO is not satisfied, he should forward the report to AML&CFTD. After receiving report from branch, AML&CFTD should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stages of evaluation (whether reported to Bangladesh Bank or not) financial institutions should keep records with proper justification & manner.

c) Disclosure:

This is the final stage and FIs should submit STR/SAR to Bangladesh Bank if it is still suspicious.

For simplification the flow chart given below shows STR/SAR identification and reporting procedures:



10.5 RISK-BASED APPROACH

An integrated risk-based system depends mainly on a proper assessment of the relevant risk sectors, products, services, and clients and on the implementation of appropriate risk-focused due diligence and record-keeping. These in turn become the foundation for monitoring and compliance mechanisms that allow rigorous screening of high-risk areas and accounts. Without sufficient due diligence and risk profiling of a customer, adequate monitoring for suspicious activity would be impossible. According to the Wolfsburg Group guidelines, a risk-based monitoring system for financial institutions clients should:

- compare the client's account/transaction history to the client's specific profile information and a relevant peer group, and/or examine the clients account/transaction history against established money-laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies;
- establish a process to compare customer or transaction-specific data against risk-scoring models;
- be capable of recognizing patterns and of "learning" which transactions are normal for a client, rather than designating certain transactions as unusual (for example, not all large transaction is unusual and may easily be explained);

- issue alerts if unusual transactions are identified;
- track alerts in order to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required; and
- maintain an audit trail for inspection by the institution's audit function and by financial institutions supervisors.

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. It is more than the absence of certainty that someone is innocent. A person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition knows enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

Questions that a financial Institution must consider when determining whether an established customer's transaction must be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?

Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

10.6: Internal Reporting Procedures and Records:

1.1 Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the CAMLCO. This ensures speed, confidentiality and accessibility to the CAMLCO. However, in line with accepted practice, some financial sector businesses may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting to the CAMLCO or an appointed deputy through the branch/unit level AMLCO.

1.2 Supervisors should also be aware of their own legal obligations. An additional fact which the supervisor supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the supervisor. The supervisor then has a legal obligation to report to the BAMLCO.

1.3 All suspicions reported to the CAMLCO should be documented (in urgent cases this may follow an initial discussion by telephone). In some cases, it may be possible for the person with the suspicion to discuss it with the BAMLCO.

1.4 The CAMLCO should acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. "tipping off". All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed

1.5 On-going communication between the CAMLCO and the reporting person/department is important. The institution may wish to consider advising the reporting person, department or branch of the CAMLCO's decision, particularly if the report is believed to be invalid. Likewise, at the end of an investigation, consideration should be given to advising all members of staff concerned of the outcome. It is particularly important that the CAMLCO is informed of all communication between the investigating officer and the branch/unit concerned at all stages of the investigation.

1.6 Records of suspicions, which were raised internally with the CAMLCO but not disclosed to BFIU, should be retained for five years from the date of the transaction. Records of suspicions which the BFIU has advised are of no interest should be retained for a similar period. Records of suspicions that assist with investigations should be retained until the bank is informed by the BFIU that they are no longer needed.

Officers of the Bank will not divulge any information pertaining to STR submitted to BFIU in any circumstances to the customer or other for which investigation is hampered or impact adversely.

10.7: STR Reporting Procedures:

Institutions enlisted as per MLPA, 2012 and ATA, 2009 (as amended in 2012) are obligated to submit STR/SAR to BFIU, Bangladesh Bank. Such report must come to the BFIU from AML&CFTD of the bank by using specified format/instruction given by the BFIU.

2.1 Sufficient information should be disclosed on the suspicious transaction, including the reason for the suspicion, Suspicious Activity/ information and transaction detail with counter parties' detail to enable the investigating officer to conduct appropriate enquiries. If a particular offence is suspected, this should be stated so that the report may be passed to the appropriate investigation team with the minimum of delay. However, it is not necessary to complete all sections of the suspicious activity report form and its submission should not be delayed if particular details are not available.

2.2 Where additional relevant evidence is held which could be made available to the investigating officer, this should be noted on the form.

2.3 Following the submission of a suspicious activity report, bank is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a "tipping-off" offence. Close liaison with BFIU, Bangladesh Bank and the investigating officer is encouraged in such circumstances so that the interests of all parties may be fully considered.

10.8 TIPPING OFF

Section 6 of MLPA 2012 and FATF Recommendation 21 prohibits bank, its directors, officers and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the bank is seeking to perform its CDD obligation in those circumstances. If there is any chance of Tipping off while doing CDD for a suspicious client, STR should be reported without doing CDD of the same. The customer's awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.

10.9 Penalties of Tipping Off

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

10.10 "SAFE HARBOR" PROVISIONS FOR REPORTING

Safe harbor laws encourage bank to report all suspicious transactions by protecting banks, employees and its board of directors from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLPA, 2012 provides the safe harbor for reporting.

10.11 RED FLAGS OR INDICATORS OF STR

10.11.1 Moving Customers: A customers who moves every month, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal, could be suspicious.

10.11.2 Out of market windfalls: If you think a customer who just appeared at the bank sounds too good to be true, you might be right. Pay attention to one whose address is far from your branch, especially if there is no special reason why you were given the business. Isn't there any branch closer to home that could provide the service? If the customer is a business, the distance to its operations may be an attempt to prevent you from verifying there is no business after all. Don't be bullied by the sales personnel who follow the "no question asked" philosophy of taking in new business.

10.11.3 Suspicious Customer Behavior:

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses the record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be recorded.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- Customer who is a student uncharacteristically transfers/exchanges large sums of money.
- Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

10.11.4 Suspicious Customer Identification Circumstances:

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer's permanent address is outside the branch's service area.
- Customer asks many questions about how the bank disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.
- Customer is not interested to disclose any other bank account's information.

10.11.5 Suspicious Cash Transactions:

- Customer opens several accounts in one or more names, then makes several cash deposits under the reporting threshold.
- Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.
- Corporate account has deposits and withdrawals primarily in cash than cheques.

10.11.6 Suspicious Non-Cash Deposits:

- Customer deposits large numbers of consecutively numbered money orders or round figure amounts.
- Customer deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business.

- Funds out of the accounts are not consistent with normal business or personal items of the account holder
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

10.11.7 Suspicious Activity in Credit Transactions:

- A customer's financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.

10.11.8 Suspicious Commercial Account Activity:

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.
- TT or other remittances to or from the border areas without any reasonable ground.
- Remittances from any High Risk or drug producing/transit countries
- Under/Over invoicing in import or export business.
- Mis-declaration of goods in import or export business.
- Maintain different accounts in different names

10.11.9 Suspicious Employee Activity:

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee frequently is involved in unresolved exceptions or recurring exceptions on exception reports.
- Employee lives a lavish lifestyle that could not be supported by his/her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.

10.11.10 Suspicious Activity in a bank Setting:

- Request of early encashment. ,
- A DPS (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.

Chapter # 11

OTHER REPORTS

Chapter # 11
OTHER REPORTS

11.1 Legal Obligations:

The reporting organizations shall have to report any suspicious transaction (defined in Section 2(Z) of MLPA, 2012 and Section 2(16) of ATA, 2009) to the Bangladesh Bank (BFIU) immediately on its own accord. Under Section 25 of the MLPA, 2012 & MLP Rules, 2019 - every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to Bangladesh Bank without any delay or in due time. Besides they have to produce any documents that are sought by Bangladesh Bank (BFIU). BFIU used to collect Statement 2 on Transaction in Non-Resident A/C (if Tk.1crore or above in 6months) and Statement 3 on Summary of SAR/STR on Bi-Monthly basis. These 2 statements have been discontinued from 21 January 2018 as per instruction letter Ref. No. BFIU (CHIE)-03/2018-442-498.

11.2 General and Routine Reporting to BFIU

11.2.1 Monthly Cash Transaction Reporting (CTR)

As prescribed in section 6 of the BFIU Master Circular#26, Banks need to report on Monthly basis, cash transaction/s (either debit or credit) in an A/C that is equivalent or above BDT 1 miilion in a day. Cash deposits in Govt. A/Cs and Inter-Bank & Inter-branch cash transactions will not qualify for such reporting. Reporting is done centrally by 21st of the following month in "goAML" platform correctly in prescribed format.

Every branch prepares/download their respective monthly CTR and send it to AML&CFT Division in due time. If the branch has no such transaction, it should state AML&CFTD as 'There is no reportable CTR'. Simultaneously, branches need to identify whether there is any suspicious transaction reviewing the cash transactions. If any suspicious transaction is found, the branch will submit 'Suspicious Transaction Report (STR)' to the Division. If no such transaction is identified, it needs to inform to the AML&CFTD as 'No suspicious transaction has been found' while reporting the CTR. Besides, every branch needs to preserve its CTR in its own branch.

The AML&CFTD needs to prepare the accumulated CTR after checking all Branch CTRs. The AML&CFTD must ensure the accuracy and timeliness while reporting to BFIU. Moreover, it has to review all the cash transaction from the branches above the threshold and search for any suspicious transaction. After reporting CTR, AML&CFTD must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

11.2.2 Half-Yearly Self-Assessment

Branches need to assess their status on AML/CFT Compliance using BFIU prescribed template and send to AML&CFTD and IC&CD. Accordingly, AML&CFTD compiles a report, gets concurrence from MD&CEO and finally sends to the BFIU within 2 months of end of June & December. Detail procedure & importance has been illustrated in chapter 8 of this Policy manual.

11.2.3. Half Yearly Report to be submitted to the CEO/ BOARD

As per Bangladesh Bank directives in BFIU Circular No. 26 dated 16JUN2020, AML&CFTD will submit a report on Half- Yearly basis on the implementation status/steps taken to combating money laundering and other related AML&CFT issues to the CEO/Board on regular basis.

11.2.4: System of Independent Testing

Procedures

As per the format given in AML&CFT Circular No. 26 dated 16JUN2020, issued by BFIU an Independent Testing Procedures should be conducted for the branches by the ICCD. While conducting the same they should look into whether the policy and directives on AML&CFT issues are followed meticulously by the Branches and appraise the performance of the branch with grading and submit report to AML Division. On receiving the Independent Testing Procedure report, AML&CFTD will prepare a report on branch grading and marks on half yearly basis and that should be placed to the CEO for his review and comment. A copy should be forwarded to BFIU, Bangladesh Bank.

11.3 Queries & Compliance reply

BFIU sends a good number of letters on name searching, queries, freezing and inspection reports. Accordingly, Branch & Bank needs to report to BFIU on time after proper due diligence ensuring searching, freezing, documentation & compliance of audit recommendations, as appropriate.

Chapter # 12

Self-Assessment & Independent Audit Function

Chapter # 12
Self-Assessment & Independent Audit Function

12.1 Self-Assessment:

As per section 8 of BFIU Circular # 26, MMBPLC has established proper 'Self-Assessment (half yearly) and Independent Testing Procedures'. This ensures how effectively banks' AML/CTF program is working on an on-going basis. To establish an effective AML/CTF system in the Bank, it should be ensured that sufficient workforces are available to accomplish the work of evaluation of Self-Assessment reports of the branches and Independent Testing there against by the IC&CD. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations. The self-assessment should advise management whether the internal procedures and statutory obligations of the bank have been properly discharged. It is very difficult for the AML&CFTD or ICCD to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self-Assessment Reporting system for the branches that MMBPLC also follows.

As per Section 8.1 of the BFIU Circular #26, all BAMLCOs will conduct 'Self-Assessment' as per Annexure-'Kha' of the said circular **(Annex-6)**, following directives & templates sent from AML&CFTD for effective execution as per regulatory expectation. 'Self-Assessment' will be done on half-yearly basis (i.e. JAN-JUN & JUL-DEC cycle). The following are to be ensured during completion of the Assessment:

i. Before finalizing the 'Self-Assessment' report, the same to be tabled in the respective branch/ unit meeting and discussed with relevant staff;
ii. If the identified issues can be resolved at branch level it should be immediately done; necessary action plan and recommendations to be stated in the final report;
iii. The action plans to be tracked discussing the progress in subsequent quarterly meetings;
iv. The 'Self-Assessment' report with action plans and recommendations is to be submitted to the AML&CFT Division **(email: amlct@modhumotibankltd.com)** and Head of Internal Control & Compliance Division (IC&CD) within the 15th day, after end of each half-year (i.e. by 15JUL & 15JAN respectively).

In line with section 8.2 & 8.3 of the BFIU Circular No#26, the Internal Audit and AML&CFT Division will accomplish their responsibilities regarding this 'Self- Assessment' and table the same to the MD & CEO before submitting to BFIU. To harness maximum benefit from the half-Yearly Self-Assessment, AML&CFT Division will arrange to convey the further actionable – that are recommended from the MD & MANCOM along with if anything is advised from BFIU after submitting the Self-Assessment Report to them – to all Branches &/or relevant units, so that Branches can further execute & track them through **Quarterly Meetings** following the directives sent from the AML&CFTD.

This Self-Assessment must be treated as a dynamic document for continuous improvement of Branch's AML/CTF standard towards attaining "Satisfactory or Strong" rating in audit/ inspections. During the branch visit (randomly selected), AML&CFTD officials check the AML/CTF issues of branches based on the directives (Self-Assessment Template, Unique Quarterly Meeting Minutes Template, KYC review Form – High Rick A/C, etc.) to evaluate AML/CTF initiatives of branches. An active participation is also ensured from AML&CFT Division during or before system checks inspection conducted on branches by BFIU.

12.2 Independent Testing Procedure:

The Internal Control & Compliance Division (IC&CD) that conducts audit is independent in MMBPLC in line with section 8.2 of the BFIU Circular No#26. Independent testing has to be done through a checklist that is prescribed by the BFIU as per *BFIU Circular No. # 26).* At the same time external auditors are appointed to review the adequacy of the program during their periodical Audit of the Bank.

12.2.1 IC&CD's Obligation on Self-Assessment & Independent Testing Procedures:

In line section 8.2 of the BFIU Circular no.#26, the IC&CD shall:

- assess the branch evaluation reports that are received from the branches typically by 15 July & 15 January and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the AML&CFTD along with any other observations on the

Self-assessments conducted by the Branches – preferably by 3rd week of July & January respectively;

- execute inspection/audit activities in various branches according to its own regular Annual Audit Plan, using the specified checklist assign rating and publish report as per standard internal protocol & follow-up compliance;
- execute inspection/audit of additional 10% of Branches, that are not covered in their Annual Audit Plan using the aforesaid checklist & issue report;
- execute inspection/audit of 10% of total Cash points/ Agents in a year to assess the compliance status of Mobile Financial Services & Agent Banking on the AML/CTF area;
- forward all the aforesaid Inspection / Audit Reports along with Ratings to the AML&CFT Division /CCC.

12.2.2 CCC's Obligation on Self-Assessment & Independent Testing Procedures:

Based on the received branch evaluation reports from the branches and submitted inspection/audit reports by the IC&CD, the AML&CFTD shall prepare an evaluation report on half-yearly basis. In that report, beside other topics, the following topics must be included:

(a) Total number of branch and number of self-assessment report received from the branches;
(b) The number of branches inspected/audited by the Internal Audit Department at the time of reporting and the status of the branches (branch wise achieved number);
(c) Same kinds of irregularities that have been seen in maximum number of branches according to the received self-assessment report and measures taken by the AML&CFTD to prevent those irregularities.
(d) The general and special irregularities mentioned in the report submitted by the Internal Audit Department and the measures taken by the AML&CFTD / CCC to prevent those irregularities; and
(e) Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'unsatisfactory' and 'marginal' in the assessment/ audit reports.

Besides, after evaluation if any issue of sensitive /high-risk is noticed in any Branch, then immediately that branch need to be inspected by the IC&CD and the matter to be notified to the competent authority.

12.2.3 Regulatory System-based Inspection:

To assess the compliance status of any branch of a Bank the Department of Banking Inspection or BFIU or their authorized unit may conduct System-based Inspection using their standard template. The core focuses on branch assessment areas are:

Sl#	Points	Remarks	Key Areas of Supervision/Evaluation	Score
	90^{+} - 100	Strong	Evaluation of Branch Compliance Officer	06
	70^{+} - 90	Satisfactory	KYC procedure	26
	55^{+} - 70	Fair	Transaction Monitoring	23
	40^{+} - 55	Marginal	Suspicious Transactions & Cash Transaction Reporting (STR &CTR)	20
	40 & Below	Unsatisfactory	Report submission to CCC / AML&CFTD	03
			Self-Assessment process	05
			Knowledge & Awareness of Staff on AML/CTF	04
			Record Retention	05
			Status of Audit, Inspection & others	08
			Total	**100**

Considering all these critical issues, the AML&CFT Division has reviewed all the Check-lists and prepared a comprehensive Self-Assessment template with guidelines for Branches.

12.2.4: External Auditor:

External auditor also plays an important role in reviewing the adequacy of AML & CTF controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External auditor would be risk-focus while developing their audit programs and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits in its audit report. In MMBPLC the External Auditor also makes valuable observation in the Bank's Management Report.

12.2.5 Role of Audit

As stated in the section 5.5 of the ML & TF Risk Management Guidelines of BFIU, Internal Audit or Internal Control and Compliance (ICC) of a bank has an important role for ensuring proper implementation of bank's AML & CTF Compliance Program. Every bank needs to ensure that ICC is equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICC has to oversee the implementation of the AML & CTF compliance program of the bank and has to review the 'Self-Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

In line with BFIU prescription, to ensure the effectiveness of the AML&CTF compliance program, MMBPLC assesses the program regularly and look for new risk factors. FATF recommendation 18 suggests that-

> *'Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML&CTF purposes. Financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML&CTF measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing'.*

An institution's internal auditors should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable.

The internal audit must-

- understand ML & TF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML/CTF Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML&CTF Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;
- communicate the findings to the board and/or senior management in a timely manner;
- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU or BB;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
    - the importance of the board and the senior management place on ongoing education, training and compliance,
    - employee accountability for ensuring AML&CTF compliance,
    - comprehensiveness of training, in view of specific risks of individual business lines, **o** training of personnel from all applicable areas of the bank,
    - frequency of training,
    - coverage of bank policies, procedures, processes and new rules and regulations,
    - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
    - Penalties for noncompliance and regulatory requirements.

The IC&CD of MMBPLC also strives its best to accomplish their independent responsibilities as stated above to alert MMBPLC on any potential ML&TF risk that may diminish its reputation.

12.2.6 Value Adding Review & Management Information (MIS) from AML&CFT Division

In addition to the statutory requirements on 'Self-Assessment & Independent Testing' &/or reporting, the MMBPLC AML&CFT Division accomplishes the following:

- Compliance Review: On RBA & on random basis the AML&CFT Division conducts short Compliance Review physically visiting the branch, where key AML/CTF Risk Indicators and contemporary issues are checked to assess the Branch status. A refresher Training is also conducted with all Branch staff along with Q/A session that helps the Branch immensely to enhance their awareness.

- Monthly Dash-Board: The AML-Head sends a monthly dash-board to all key stake-holders on the high-level numbers of the entire AML/CTF related tasks conducted by the AML&CFT Division, which is a mechanism of self-accountability with focusing the trend of core-tasks.

- Monthly Reporting to Management: On certain Key Risk Indicators (KRI)s, - like STR analysis/trend, CTR submission and any major regulatory or risk concerns etc, AML&CFT Division provides report on regular basis to the MMBPLC, CCC for the monthly meeting & discussion.

- Quarterly Report on AML/CTF to the MD & CEO: Though not mandated by the BFIU, but MMBPLC Senior Management to remain updated on the Regulatory & MMBPLC status on AML/CTF compliance has introduced a Quarterly/half yearly Reporting to the CEO from the AML&CFT Division– summarizing all key tasks covering all the regulatory circulars/ letters issued in that month and their respective compliance status. This gives a full picture to the MD &CEO at a glance – his Bank's governance & control status in the area of AML/CTF compliance.

- Updates in CCC/MANCOM: The CAMLCO being the member of the MANCOM, has the opportunity to update the senior most committee of the Bank, on the crucial issues on AML/ CFT – and the requirement of cooperation from them, if necessary, on monthly basis. Additionally, in certain MANCOM meetings the Half-yearly Self-assessment & Annual AML reports are also discussed.

- Follow-up of Branches on the Audit Reports of IC&CD and BFIU/DBI: Similarly, though mot mandated by the BFIU, to ensure proper compliance; the AML&CFT Division formally pursues & assists the respective branches on which IC&CD, BFIU or DBI has issued reports, so that they can comply with the recommendations.

Chapter # 13

Record Retention

CHAPTER # 13

RECORD RETENTION

13.1 Statutory Requirements

As the matter related to investigation, review & prosecution – hence retention of relevant records is very crucial at every stage of AML/CTF governance & controls. Let's see the statutory requirements, below:

Obligations under MLPA, 2012	The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to Bangladesh Bank.

Obligations under the bank shall maintain all necessary records of all transactions, both domestic MLP Rules, 2019 and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:

1) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;
2) The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;
3) The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.

Obligations under BFIU Circular-26 dated 16/06/2020

13) All necessary information/documents of customer's domestic and foreign transactions have to be preserved for at least 5(five) years after closing the account.

2) All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5(five) years after closing the account.
3) All necessary information/documents of a walk-in Customer's transactions have to be preserved for at least 5 (five) years from the date of transaction.
4) Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.
5) Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU.

13.2 Records to be kept

The records should cover, at least in broad headline:

- Customer information
- Transactions
- Internal and external suspicious reports
- Report from CCC/CAMLCO/IC&CD/BFIU/DBI, etc.
- Compliance monitoring & transaction monitoring
- Training Records (detail information along with effectiveness of training)
- Various reporting to BFIU (CTR, Self-Assessment, Freezing, etc.)
- Sanction & Adverse media news screening (particularly linked to potential TF)
- Related records that have potential to become evidence for any trial/prosecution, etc.
- Agent Banking (AB) Records
- High Risk Account Assessment/Review documents

13.2.1 Customer Information

For the evidence of a customer's identity, banks must keep a copy of or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where a bank has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. A bank may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date when the relationship with the customer ends is the date:

- an occasional transaction, or the last in a series of linked transactions, is carried out; or
- the business relationship ended, i.e. the closing of the account or accounts.

Records relating to CDD & verification of identity will generally comprise:

- Verified copy of legal Photo-ID (e.g. NID, Passport) including NEC Verification result sheet
- Verified/attested copy of legal document (e.g. Trade License, Certificate of Incorporation)
- Verified copy of Birth registration Certificate (with attestation of photo & certificate)
- Relevant Identification & Registration document for various types of A/Cs as stated in Annexure B of the ML&TF Risk Management Guidelines of BFIU-SEP15 (**Annexure# 2**)
- Documents evidencing Source of Fund &/or Occupation
- Supporting Documents evidencing verification of present address
- Properly filled-in A/C opening form and Photograph of Customer/s & Nominee (if any)
- Related important document crucial for CDD (e.g. Board Resolution, PEP Assessment & Approval)

All these Account Opening related documents must be kept in core banking at-least for 5years from closing the Account.

13.2.2 Transactions

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the bank's records. Routine Transaction for Core banking A/Cs -records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips; cheques, vouchers, photo-ID of depositor/withdrawer (if non-customer), Justification letter-if TP breaches, Swift message, trade documents, PO/DD/Remittance Application, Wire-Transfer records, etc. should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records to be kept at-least for 5 years from closing the A/C.

For Walk-in Customer: completed simplified KYC document & Photo-ID to be kept for at least 5(five) years from the date of such transaction.

13.2.3 Internal and External Suspicious Reports:

A bank should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material, concerning possible money laundering but has not made a report to BFIU, a record of the other material that was considered.
- All internal initial suspicions made not be validated to qualify for external SAR/STR- after thorough analysis (**4Ds- Dates, Details, Doubts & Decision),** hence documents of this exercise and the decision of BAMLCO for closing the initial SAR to be retained in Branch AML file. Similarly, if AML&CFT Division after final review seems a SAR a not a quality one /does not have merit or other obvious grounds have proven the justification for not treating issue as suspicious – that needs to be documented in AML&CFT Division file as well as communicated to respective Branch.
  Records of all internal and external reports must be retained for five years from the date the report was made, in general. However, copies of all SAR/STRs made to the BFIU should be retained for more than five years, if the investigation is not concluded or if the issue is under legal prosecution stages. Therefore, no external STR records be destroyed without CAMLCO's approval.

13.2.4 Report from CCC/CAMLCO/IC&CD/BFIU/DBI, etc.

Various Investigation, Inspection, Audit, Compliance Review are done by respective controlling authorities where crucial concerns &/or recommendations related to AML/CTF are embedded in the reports and similarly respective Branch/ Audited-unit also gives written confirmation in compliance-reply of those important recommendations – all these forms vital legal document for any potential regulatory examination or prosecution – hence, these documents to be kept for 5 years, from the date of closing of related audit file.

13.2.5 Compliance monitoring & transaction monitoring

Branches/ Units to ensure on-going compliance monitoring – conduct Quarterly Meeting, Half-yearly Self-Assessment exercise & meeting, and also various daily & monthly Transaction Monitoring exercise. During material transaction monitoring Branch also analyze & collect further documents to ascertain whether that particular transaction is suspicious or not. Hence, the meeting minutes, material transaction monitoring exercise documents to be kept for 5years from the date of meeting /transaction analysis.

13.2.6 Training Records

Bank shall maintain records which include the following, so that the Bank can demonstrate that they have complied with the regulations concerning staff training: -

(i) Details of the content of the training programs provided;
(ii) The names of staff who have received the training;
(iii) The date on which the training was delivered;
(iv) The results of any testing carried out to measure staff understanding of the money laundering requirements; and
(v) An on-going training plans

13.2.7 Various reporting to BFIU (CTR, Self-Assessment, Freezing, etc.)

All regulatory routine Reports as mentioned under section 6.2 of this Manual (i.e. CTR, Bi-monthly statements, Self-Assessment, Annual AB report, etc.) to be kept for 5 years. Similarly documents related to Hold/ Freezing instructions and searches where A/C found &/or sensitive (TF) searches' documents (even if not found) to be kept for 5years. Key correspondence documents with BFIU/ Regulator to be retained by AML&CFT Division.

13.2.8 Sanction & Adverse media news screening (particularly linked to potential TF)

As stated above in chapter 6, under section 5.3 – all such Sanction screening false/ positive –result must be retained for 5 years for regulatory audit, in general. For cases where exact match found and regulatory review under process &/or potential dispute underway – those documents cannot be destroyed even after 5years i.e. till the issue has not been resolved.

Similarly, as stated above in chapter 5, under section 5.4 – all such searching & reporting documents are to be retained for 5years.

13.2.9 Related records that have potential to become evidence for any trial/prosecution, etc

These documents may be related to any ad-hoc regulatory inspection on any Predicate-Offence or related to any Vigilance Investigation on Control-lapses but the materiality is high or sensitive or where money/ MMBPLC account is also involved – these issues can turned to be at certain stage very crucial leading to legal prosecution including charges under MPLA/ ATA (though initially it was not)! With prudence such records also should be retained for 5 years.

13.2.10 Agent Banking Records

The requirement contained in Prudential Guidelines for Agent Banking Operation in Bangladesh of September 18, 2017; it stated that "the agent shall at all times ensure safe-keeping of all relevant records, data, documents or files or alternately, such records, data, documents or files shall be shifted to the bank at regular pre-specified intervals for bank's safe-keeping".

13.3 Formats and Retrieval of Records

To meet the requirements of the law and to fulfill the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of a bank. However, the primary requirement is on the bank itself and the responsibility is thus on the bank to ensure that the third party (yet to be engaged) is willing and able to retain and, if asked to, produce copies of the records required.

However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

As timely retrieval & timely submission of records to Regulator as per their requirement has a legal obligation, hence MMBPLC Branches & units should keep the records in such an orderly manner in Registers (A/C closing register, voucher control register, archiving register, etc.), that they can retrieve them promptly.

13.4 Sharing of record/information

In general, as per related section of the Bankers' Books Evidence Act (BBEA) 2021 and as per section 94(1) of the Code of Criminal Procedure (CrPC), 1898 – Bank cannot disclose customer information without customer's consent or without court-order or written instruction from the competent authority authorized under respective sections of Laws or provide only to the authorities as mentioned in BBEA 2021. . Generally, Under Section (u/s) 26A, of the Customs Act 1969, (u/s) 24, of VAT Act 1991 & (u/s) 113 of the Income Tax Ordinance, 1984 (ITO,84), and (u/s) 19 of the Anti-Corruption Commission Act, 2004– competent authority can call for documents. Under section (u/s) 116A of ITO,84 – they can restrict withdrawal/transfer; u/s 117- they have power of Search & Seizure and u/s 143 of ITO,84 they can ask Bank to debit customer A/C & pay the Govt. So, it is a mandatory duty for bankers to ensure confidentiality of Customer Information. In this regard a guidance mail was sent from MLTFPD to all concerned.

In case of issues, accounts, SAR/STR, investigation, cases, etc. under the Money Laundering Prevention Act 2012, and Anti-Terrorism Act, 2009, MMBPLC will only share account related information with competent authority of BFIU or its authorized investigating agency's competent Investigation Officer or upon instruction from competent court.

If anyone divulge information u/s 6 of the MLPA, 2012 – he/she shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both. Point to note that, it is very important to carefully check the documents before submitting to any regulatory authority on time and similarly important to systematically preserve the documents that are provided to them, until the investigation or trial is not closed. Orderly archiving will ensure timely retrieval of documents and production to authority / court. No records under investigation can be destroyed without clearance from the AML&CFT Division.

Chapter # 14

AML TRAINING & AWARENESS PROGRAMS

CHAPTER # 14
AML TRAINING & AWARENESS PROGRAMS

14.1. Training and Awareness

FATF recommendation 18 suggests that a formal AML/CFT compliance program should include an ongoing employee training program. The importance of a successful training and awareness program cannot be overstated. Employees in different business functions need to understand how the bank's policy, procedures, and controls affect them in their day to day activities. As per BFIU circular, each bank shall arrange suitable training for their officials to ensure proper compliance of money laundering and terrorist financing prevention activities.

14.2. The need for Employees Awareness:

The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the serious nature of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

It is, therefore, important that bank introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

14.3. Education and Training programs:

All relevant staff should be educated in the process of the "know your customer" requirements for money laundering and terrorist financing prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the bank itself. Some sorts of high-level general awareness raising training are, therefore, also suggested by the Central Bank.

14.4. General Training

A general training program of the bank should include the following:

- General information on the risks of money laundering schemes, methodologies, and typologies;
- Legal framework, how AML related laws apply to the bank and its employees;
- Bank's policies and systems with regard to customer identification and verification, due diligence, monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training should present real life money laundering schemes, preferably

cases that have occurred at the bank or at similar institutions, including, where applicable, how the pattern of activity was first detected and its ultimate impact on the institution.

14.5. Job Specific Training

The nature of responsibilities/activities performed by the staff of the bank is different from one another. So their training on AML&CFT issues should also be different for each category. Job specific AML trainings are discussed below:

14.5.1 New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the bank, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

14.5.2 Customer Service/Relationship Managers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are vital to the organization's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

It is vital that 'front-line' staffs are made aware of the bank's policy for dealing with non-regular (walk in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

14.5.3 Processing (Back Office) Staff

The staffs, who receive completed Account Opening, FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the bank's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML&CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

14.5.4 Credit Officers:

Training should reflect an understanding of the credit function. Judgments about collateral and credit all require awareness and vigilance toward possible money laundering activities. Indirect lending programs and lease financing also call for KYC efforts and sensitivity to laundering risks.

14.5.5 Audit and compliance staff

These are the people charged with overseeing, monitoring and testing AML controls, and they should be trained about changes in regulation, money laundering methods and enforcement, and their impact on the bank.

14.5.6 Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering prevention procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and

terrorist financers; internal reporting procedures and the requirements for verification of identity and the retention of records.

14.5.7 Senior Management and Board of Directors

Money Laundering issues and dangers should be regularly and thoroughly communicated to the board. It is important that the compliance department has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering poses to the bank.

14.5.8 AML & CFT Compliance Officer

The AML&CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering Prevention Legislation, Bangladesh Bank directives and internal policies.
In addition, the AML&CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity. Also to improve the efficiency of the CAMLCO & D-CAMLCO or any other concerned official, Bank shall arrange proper training and/or professional certification program for the same.

14.6. Training Procedures

The trainers (internal or external) will take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning (may be in Zoom/ other e-Platform) can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or exams, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee personnel file.

14.7. Refresher Training

In addition to the above relatively standard requirements, training may have to be tailored to the needs of specialized areas of the bank's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least once in every two years to ensure that staff does not forget their responsibilities. Bank will provide such training once in every two years; sometimes may choose a shorter or longer period or take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

Training should be ongoing, incorporating trends and developments in the bank's business risk profile, as well as changes in the legislation. Training on new money laundering schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

14.8. In-house discussion:

Branch will arrange in house discussion on regular basis to update the employees of the branch on AML laws and regulation and circulars issued from Bangladesh Bank and Head office from time to time.

14.9. Education and Training of Customer:

As instructed by Bangladesh Bank vide BFIU circular 26 issued dated 16JUN2020, Bank shall respond to customers on different matters including KYC and TP attached to the account opening form with proper rational. Bank shall time to time distribute leaflets among the customers to make them aware about money laundering and terrorist financing and also to arrange to stick poster in every branch at a visible place. Every Bank has to arrange public awareness programs like advertisements through Billboard, poster, leaflet etc.

The Bank will continue to devote considerable resource to establish and maintain employee's awareness of the risk of money laundering and their competence to identify and report relevant suspicions in this area. . The Bank is dedicated to a continuous program of increasing awareness and training of employees at all appropriate levels in relation to their knowledge and understanding of AML&CFT issue, their respective responsibilities and the various control and procedures introduced by the bank to deter money laundering and terrorist financing.

Chapter # 15

Agent Banking Policy and Procedures for Anti-Money Laundering & Combating Financing of Terrorism

Chapter # 15
Agent Banking Policy and Procedures for AML&CFT

A. **Preface:**

Banking is the inevitable part of an economy and plays a major contribution towards socio-economic development of a country. The sector is considered as life blood of the economy as well. An efficient and stable banking system is the prerequisite for overall development of the country. But still more than 70% of the people of the country are out of banking umbrella; still people are relying in cash transaction. Bangladesh Bank and Bangladesh Government believe that *financial inclusion* is a key enabler to reducing poverty and boosting prosperity.

For financial Inclusion and Banking for all motto of the Government, Agent Banking will ensure the inclusive financing is the delivery of financial services at affordable costs to sections of disadvantaged and low-income segments of society. Through Agent Banking, underprivileged people across the country will get limited Scale of banking other than Bank Branches via Agent/Sub-agents. Modhumoti Bank always align with Bangladesh Bank initiatives for socio-economic develop of the country and in this road map, Modhumoti Bank will certainly uplift the motto "Banking for all" and it will help people to grow their savings habit and as well as will increase the foot print of banking channel by setting control following Anti-Money laundering and combating Terrorist financing guidelines of Central Bank.

B. Scope of this Document:

This Policy should be integral part/ individual Chapter of MMBPLC AML & CFT Policy Guidelines as all MMBPLC customers can enjoy all Branch Banking facilities as it uploaded in CBS instantly/ in real time. This document will set a control on Agent Banking activities both Financial and non-financial under the Anti-Money laundering and combating Terrorist financing guidelines of the bank. This document will be reviewed every year to ensure service excellence and standard control. This document must not be disclosed to persons working outside Modhumoti Bank Limited and Agent Banking Division will ensure safekeeping of MMBPLC Agent Banking Policy and Procedures for Anti-Money Laundering & Combating Financing of Terrorism. It is mentionable that approved AML & CFT Guidelines of the Bank will be that key element and this document will be added as an addendum of the guidelines to set more control on Agent Banking activities. Money Laundering (ML) and Terrorist financing (TF) can potentially damage and pose serious threats to the integrity and stability of a financial system. To protect the Banking industry from these threats, the Bank Authority has been working in partnership with financial institutions and BFIU, government departments and other key stakeholders to put in place an effective regime to fight against these crimes.

The Board of Directors and Senior Management of Modhumoti Bank Limited are firmly committed to comply with their roles and responsibilities vested under Money Laundering Prevention Act of 2012 (Amendment-2015) & Anti-Terrorism Act of 2009 (Amendment-2012 & 2013). Money laundering Prevention is viewed as an integral part of Agent Banking activities and Risk Management strategy.

C. **The Benefits of an Effective AML/CFT Framework:**

A strong AML/CFT institutional framework that includes a broad scope of predicate offenses for money laundering helps to fight against crime and corruption. An effective AML/CFT regime is deterrent to criminal activities related to capital market (e.g. Insider Trading, Market Manipulation, Securities Fraud etc.).In this regard, confiscation and forfeiture of money laundering proceeds impedes to earn profits from criminal activities, thereby reducing the incentive to commit criminal acts. In addition, an effective AML/CFT regime reduces the possibilities of losses to the institutions originating from fraudulent activities. Proper Client identification procedures and determination of beneficial ownership provide specific due diligence for higher risk policies and ensure monitoring for suspicious activities. Such prudential internal controls play a vital role for the safe and sound operation of a financial institution. This enhances public confidence and permits investments in the capital market to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.

D. Types of Services that will be offered through Agent Banking and AML & CFT Controls:

Non-Financial Transaction:

I. Agent/Sub Agent On-Boarding.
II. Agent/Sub Agent Data Capture & ID Creation.
III. Account Opening, Mini KYC fill out & Form Collection.
IV. FDR Opening Mini KYC fill out & Form Collection.
V. Monthly savings Scheme Opening Mini KYC fill out & Form Collection.
VI. Balance Query & Mini-Statement Request.
VII. Loan Application Sourcing & Form Collection.
VIII. Credit Card/Debit Card Issuance Form Collection.
IX. Cheque Book Requisition Collection.
X. E-Channel Registration Request Collection.
XI. Customer Complaint Receiving.

AML & CFT Controls: All the Non-financial transaction especially on-boarding Agent /Sub-agent and acquisition of New Account through Agent/Sub-agent will be monitored Customer Due Diligence (CDD) procedure, AML & CFT Prevention measures, KYC Procedures, Reporting, Record keeping, Awareness program etc. by Chief Anti-Money Laundering Compliance Officer (CAMLCO) office with the assistance of Agent Baking Division.

We have Agent selection criteria where Bank will select entities as Agent/Sub-agent who has following eligibility criteria which will also help us to prevent AML & CFT beside KYC & CDD policy of the bank:

- The entity must have sound financial capacity while appointing sub agents for operating agent banking activities of bank(s),
- The entity must have strong IT and electronic communication infrastructure for recording of transactions at bank level on real time basis and uninterrupted manner. The structure must be compatible for integrating Point of Sale (POS) with biometric features capturing and reading facilities, card reader, mobile phone, barcode scanner, Personal Identification Number (PIN) pads and similar technologies.
- Agent shall open current account(s) with the bank and deposit such amounts as agreed between bank and agent. Initial limits should not be less than BDT 2.00 lakh per agent banking outlet. Such limits shall be revised based on demand and transaction profile of the agent.

E. Types of Financial transaction that will be offered through Agent Banking and AML & CFT controls:

Financial Transaction:

I. Cash Deposit (Cash In)
II. Cash Withdrawal (Cash Out)
III. Fund Transfer (P2P)
IV. Fund Transfer (G2P)
V. Utility Payment (Govt & Semi Govt or Pvt.)
VI. Mobile Top Up
VII. MRP & MRV Fees Payment
VIII. Life Style product Payment and Insurance premium collection

AML & CFT Controls: All the Non-financial transaction at Agent/Sub-agent point will be monitored by Suspicious Transaction monitoring AML & CFT Prevention measures, KYC Procedures, Reporting, Record keeping, Awareness program etc. by CAMLCO office with the assistance of Agent Baking Division.

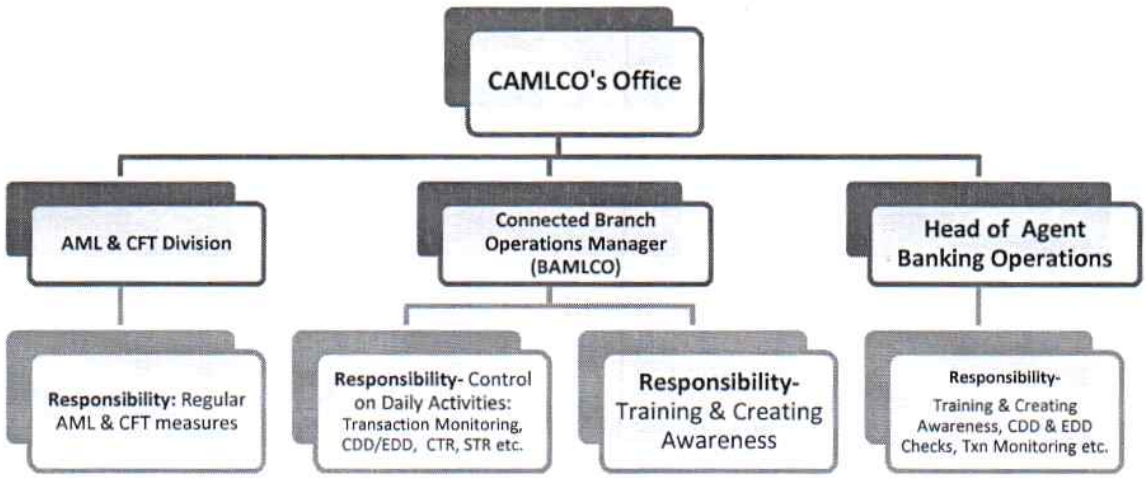
Beside regular AML & CFT measures by AML & CFT Division and Agent Banking Division; Agent Banking System and guideline will work as shield and safeguard of AML & CFT. After proper Customer validation via Bio-metric or PIN; one Customer will be able to perform transaction as per Daily Limit of Central Bank using Agent Banking Channel. As Bangladesh Bank already put strong control through Daily & Transaction Thresh

Hold, Customer Authentication via PIN or Biometric, these will certainly set more control AML & CFT besides regular reporting, transaction monitoring by Central Compliance Unit.

F. Documentation/Archival of Agent Banking:

There will be an audit trail for all transactions for both financial and non-financial transactions in Agent Banking Channel. Account Opening, KYC or Sensitive Documents will be archived for perpetual and Non-Sensitive documents will be stored for 6 year but system reflection should be perpetual as guided by AML & CFT Guidelines of central bank.

G. AML & CFT Frame Work for Agent Banking:



H. Monitoring and Supervision:

The Central Compliance Committee headed by a Chief Anti Money Laundering Compliance Officer (CAMLCO) at Head Office has been prepared the Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) policies and procedures for agent banking for prevention of money laundering. It will also from time to time review the implementation of the guidelines, policies and strategies by the branches/agents of the Bank. MMBPLC and its partners shall have to comply with the prevailing Anti Money Laundering (AML)/Combating the Financing of Terrorism (CFT) related laws, regulations and guidelines issued by Bangladesh Bank from time to time. Banks shall have to follow KYC format issued by Bangladesh Financial Intelligence Unit (BFIU) of Bangladesh Bank for the agents and customers. Banks will be responsible for authenticity of the KYC of all the customers and agents. Banks shall ensure that suspected transactions can be isolated for subsequent investigation. Banks shall develop an IT based automated system to identify suspicious activity/transaction report (STR/SAR) before introducing the services. Officers shall immediately report to AML & CFT Division of Head to escalate it to BFIU of Bangladesh Bank regarding any suspicious, unusual or doubtful transactions likely to be related to money laundering or terrorist financing activities.

To ensure compliance with Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) standards set by AML/CFT rules, regulations, guidelines and instructions issued by Bangladesh Bank, every Agent is responsible for

- Obtaining and maintain KYC information properly and updating the same time to time;
- Ensuring Risk Classification of Customers and proper review of transactions made in the customers' accounts;
- Ensure proper filing and handover of accounts related documents to their respective branch;
- Monitoring and checking information of the walk-in customers, on-line customers and ware transfer;
- Ensuring awareness of Agent's staffs on the rules and regulations of AML & TF, Bangladesh Bank Circulars, Internal policies of the Bank on AML and the changes made in the AML regulations;
- Participate at periodical review meeting of Branch Compliance Unit on AML;

- Providing necessary cooperation to the Internal Audit, External Audit, AML visits and BFIU,AML Inspection Team;
- Providing necessary cooperation for preparation and submission of Cash Transactions Report (CTR) and Suspicious Transactions Report (STR) and other reports by Branch;
- Arrangement of Internal training for staffs in every year on AML and maintenance of training register through Branch and Agent Banking;
- Ensure education and training for customers. Every Agent shall respond to customers on different matters including KYC and TP attached to the account opening form with proper rationale, shall time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and also arrange to stick posters in every Agent Point at a visible place;
- Providing necessary cooperation for timely and duly compliance report on Bangladesh Bank Inspection report, Independent Testing & other report of Internal Audit related to AML and on the report/requirement of inspections conducted by Branch and Head Office team;
- Ensure other activities as described in this Policy;
- Ensure other related works may be assigned time to time.

I. Declaration of employees:

All Modhumoti Bank employees are required to declare that the contents of this Policy and Procedures has been read and understood and confirm strict compliance of the instructions. The Branch Anti Money Laundering Compliance Officer (BAMLCO) should preserve this declaration.
Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions. It is, therefore, important that financial institutions introduce comprehensive measures to ensure that all staffs and appointed agents are fully aware of their responsibilities.

J. Customer Due Diligence:

Modhumoti Bank shall carry out Customer Due Diligence to ensure that requirements of AML/CFT are not compromised. The Know Your Customer (KYC) requirements, transactional limits and minimum technological security requirements that are applicable to each level of account will be subject of the review process by Bangladesh Bank at the time of seeking;

- Know Your Customer (KYC) or E-KYC requirements.
- Transactional limits per day, month and year limits commensurate with customer's profile.
- Maximum balance limits on debit and credit.
- Minimum technological security requirements.
- Two factor authentication per customer per transaction.

MMBPLC shall comply with all applicable Anti-Money Laundering/Combating Financing of Terrorism AML/CFT laws and requirements.

K. Electronic Know Your Customer (e-KYC):

The traditional KYC process requires to be filled in the KYC form and collect photo ID and signature of the customers along with required documents. All the way it's a manual process. However, e-KYC is a digital process where financial institutions can open a customer account by filling up a digital form, taking photograph on the spot, and authenticate the customer's identification data (ID No. biometric information, address proof) immediately. The customer onboarding process may undertake via followings means:

a) **Assisted customer onboarding**: Where a financial institution or its nominated agent or third-party visit customer or customer visit financial institution or its nominated agent or third party's premises

and open account with the direct assistance of financial institution or its nominated agent or third party; and

b) **Self-check-in (Self Registration):** Where customer can on board at his own by using kiosk, smart phone, computer or other digital means abiding by the norms of this e-KYC Guideline. Self-check in shall be allowed for face matching model only as described in the Agent Banking Customer Onboarding of this Guideline.

Deployment of e-KYC will certainly help us set more control on AML & CFT during customer onboarding by Agents which ensure all customer physical presence at Agent outlets for availing Agent Banking Services using Finger print and Face recognition.

L. Agent Due Diligence:

Efficient and thorough Agent Due Diligence (ADD) procedures shall be put in place to mitigate risks. MMBPLC shall be responsible for having clear, well documented Agent Due Diligence policies and procedures. The Agent Due Diligence procedures shall at a minimum contain methods of identifying potential agents, initial due diligence and regular due diligence checks to be performed at specified intervals and a list of early warning signals and corrective actions to ensure proactive agent management. The Agent Due Diligence procedures shall clearly specify the roles and responsibilities of various functions with regard to agent management.
The minimum agent selection criteria shall be defined. MMBPLC shall ensure that agents are well established, enjoying good reputation and have the confidence of the populace in their areas of operation. MMBPLC shall ensure that proper AML/CFT monitoring processes exist for agent banking. The necessary actions to be taken by agents in this regard should be communicated to the agents and the agents' compliance monitored.

M. Operational/transactional limits and related issues:

MMBPLC shall establish limits for the provision of services agreed upon with the agents. The limits must be prudent and bear a relation to the volume of cash moved by the agent and the risks associated with the agent's locality for the conducting agent banking business. MMBPLC shall set limits for each agent and where applicable, for each type of transaction. In general, the maximum number and volume of transactions for client at Agent Banking outlet should not exceed the limits specified in the following table:

Amount in Lakh BDT

Daily Number of Transactions and Amount Limit						
Nature of Accounts	Cash Deposit		Cash Withdrawal		Transfer/BEFTN/ Inter-bank/Intra-bank	
	No. of transactions	Total Volume	No. of transactions	Total Volume	No. of transactions	Total Volume
Current Account	4	6.00	2	5.00	4	15.00
Savings Account	2	4.00	2	3.00	2	5.00
Special Notice Deposit (SND)	4	6.00	2	3.00	4	10.00

Note: Operational/transactional limits shall be changed based on Central Bank Guidelines.

Transactions beyond the established limits may also be carried but this shall require at least 1 (one) working day prior notice to the bank through the agent.
In special cases, when a client has need for regular banking transactions exceeding the limits, banks may set an increased limit for that client with due approval from the Managing Director. The increase must be prudent, rational and must accord the merit of the account and client and transaction category based on customer due diligence, client needs and associated risks. Within 30 (thirty) days of such increase of transaction limit, the bank shall inform FID of Bangladesh Bank in writing along with the rationale of such increase with related information of client transactions of at least last 1 (one) month.

Modhumoti Bank engaged in agent banking shall ensure that its transaction processing system is capable of

- imposing limits to avoid any breach;

- sending alerts to the users if they are close to the limit;
- identifying irregular or suspicious transactions and generate reports;
- handling real time transactions; and
- communicating transaction confirmation to the clients in a suitable manner.

N. Training on AML & CFT for Agent Banking:

Agent Banking Division with the assistance of AML Division and Training Academy of the Bank will arrange regular training for the staffs who will work for Modhumoti Bank Banking and at the same times will arrange awareness program on AML & CFT for Agent/Unit-agents. Refresher training for the staffs and periodic awareness program for the Agents/Sub-agent will be conducted to socialize the AML & CFT issues.

Strategies for providing Training:

There are two main strategic approaches for AML/CFT Training and Awareness:

a) First, new employees and Agent should receive basic training before they interact with the customers or handle transactions, so that they do not expose the organization to increased risk. This training may need to be more detailed or specific depending on the business function in which the new entrant is employed.

b) Second, all relevant staffs and Agents should receive refresher training on a regular basis. The timing of this training can vary from very frequent (monthly or quarterly specific reminders in high-risk areas) to a more generic content that is delivered on a regular basis (once every year or two years to all other staff). Again, this is an area where a risk-based approach can be adopted. The content and timing of any AML/CFT training or awareness program is one area where a bank or other financial institution can adopt a risk-based approach. Those business areas considered at greatest threat from suspicious activity should receive more frequent training.

AML & CFT Training Process Summary:

- Account Opening and Know Your Customer (KYC) and e-KYC Procedures
- Risk Categorization- Based on Activity, KYC and Transaction Profile.
- Transaction Monitoring Process and due diligence
- Suspicious Activity Reporting Process
- Self-Assessment Process
- System of Independent Testing /Audit
- AML periodical Reporting and Reporting Line
- Preservation of Customer information (at least 5 years)
- Duties, responsibilities of Central Compliance Unit (CCU) and Branch Compliance Unit (BCU)
- Arrangement of Training for Bank Officers.

O. Review of the Policy & Procedure:

This document be reviewed and necessary approval from Board of Directors based on Business, Operations and Compliance requirement. The Managing Director and CEO will have the ultimate authority to amend or modify any part of the manual based on Business, operations and compliance demand; however, the changes will be placed to the Board for notification.

COMBATING FINANCING OF TERRORISM GUIDELINE

Revised Edition December 2025

Modhumoti Bank PLC.
Your Access to Success

AML & CFT Division
Modhumoti Bank Limited
Head Office, Dhaka.

CHAPTER # 1

BACKGROUND

Introduction

1.1 This 'Combating Financing of Terrorism Policy for Modhumoti Bank Limited has been prepared in line with the existing Anti-Terrorism Act, 2009 (including amendments of 2012), Circulars issued by Bangladesh Financial Intelligence Unit (BFIU), the revised Financial Action Task Force (FATF) Standards and the international best practices. *Guidance Notes for Prevention of Terrorist Financing & Financing of Proliferation of Weapon of Mass Destruction is annexed at* ***Annex-10.***

1.2 To ensure compliance with the laws and other regulatory requirements and to develop, administer, and maintain bank's own CFT policy and to comply with the requirements of section16 (2) of Anti-Terrorism Act, 2009 (including amendments of 2012) this Policy Guidelines has been approved by the board of directors, and noted as such in the board meeting minutes

1.3 This Policy Guideline is designed to assist Modhumoti Bank Limited officials to comply with the Bangladesh combating financing of terrorism regulations and to assess the adequacy of the internal controls, policies and procedures to combat terrorist financing of the bank subject to its supervision.

1.4 It is expected that all branches in home and abroad, offices, subsidiaries, offshore banking unit of the bank and all officials of Modhumoti Bank Limited pay proper attention to this Guidelines while conducting relevant financial business and also be vigilant for practicing suitable combating financing of terrorism procedures while discharge their duties. If anyone mentioned in this Para appears not doing so, then it arises various risks for the bank including financial sanctions from BFIU.

1.5 It is also expected that all branches in home and abroad, offices, subsidiaries, off-shore banking unit of the bank and all officials of Modhumoti Bank Limited, should keep in mind combating financing of terrorism is not simply a stand-alone requirement that is being imposed by the legislation. It is a part of Modhumoti Bank Limited risk management policies and procedures.

1.6 This policy guideline should be followed by all branches in home and abroad, offices, subsidiaries, Off-shore banking unit of the bank and all officials of Modhumoti Bank Limited in conjunction with the 'Anti Money Laundering Policy ' for Modhumoti Bank Limited.

International Initiatives:

2.1 International Convention for the Suppression of the Financing of Terrorism

The financing of terrorism was an international concern prior to the attacks on the United States on September 11, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002, with 132 countries signing the convention and 112 countries ratifying it.

The convention requires ratifying states to criminalize terrorism, terrorist organizations and terrorist acts. Under the convention, it is unlawful for any person to provide or collect funds with the (1) intent that the funds be used for, or (2) knowledge that the funds be used to, carry out any of the acts of terrorism defined in the other specified conventions that are annexed to this convention.

2.2 Security Council Resolution 1267 and Successors

2.2.1 The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the listed individuals and entities, and entities owned or controlled by them, as designated by the "Sanctions Committee" (now called the 1267 Committee). The initial Resolution 1267 (1999) dealt with the Taliban and was followed by 1333 of December 19, 2000, on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusions (1452 of December 20, 2002), and measures to improve implementation (1455 of January 17, 2003).

2.2.2 The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee.

2.3 Security Council Resolution 1373

Unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to:

- deny all forms of support for terrorist groups;
- suppress the provision of safe haven or support for terrorist, including freeing funds or assets of persons, organizations or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorists; and
- cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.

2.4 The Counter-Terrorism Committee

2.4.1 As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism.

2.4.2 Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution's measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373.

2.5 THE FINANCIAL ACTION TASK FORCE

The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 36 countries and territories and two regional organizations.

2.6 FATF 9 SPECIAL RECOMMENDATIONS

FATF adopted a set of 40 recommendations to prevent money laundering. To accomplish its expanded mission of combating financing of terrorism FATF adopted nine Special Recommendations in 2001.

2.7 FATF NEW STANDARDS

FATF Plenary has revised its recommendations in February 2012. The previous 40+9 Recommendations has been accumulated into 40 (forty) recommendations called the FATF Standards. Proliferation financing has been included in the new standards. There is no special recommendation to address the financing of terrorism. All special recommendations have been merged with the 40 recommendations. Domestic Initiatives: In line with international efforts, Bangladesh has also taken many initiatives to combat terrorist financing, considering their severe effects on the country and other jurisdictions. To meet the international standards Bangladesh enacted Anti-Terrorism Ordinance (ATO) in 2008 which was replaced by ATA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), some provisions of ATA 2009 have been amended through enactment of Anti-Terrorism (Amendment) Act 2012. BFIU has issued Circulars and circulars letters in relation to Anti-Terrorism Act and UNSCRs. Bangladesh Govt. has proscribed some terrorist groups for their involvements with terrorist activities.

CHAPTER # 2

TERRORISM AND TERRORIST FINANCING

1. WHAT IS TERRORISM OR TERRORIST ACTIVITIES?

1.1 Terrorism can be defined as the unlawful use of the force against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in the furtherance of political or social objectives. Terrorist acts are criminal in nature and constitute a serious threat to the individuals" lives and freedom. (Ref. Xpress Money CFT policy)

1.2 According to the section 6(1) of the Anti-Terrorism Act, 2009 (including amendment of 2012), Terrorist Activities' has been defined as follows:

6 (1) (A): If any person or entity for the purpose of endangering the unity, integration, public security or sovereignty of Bangladesh, and with the aim of compelling the government or any entity or any other person to do something or preventing them from doing something by creating panic in the public or a section of the public

a) Kills, injures seriously, puts confinement or kidnaps any person or abets to do the same, or damages any property belonging to any person or entity or the State or abets to do the same

b) Instigates any person to kill, injure seriously, puts in confinement or kidnap any person, or to instigate any person to damage any property belonging to any person or entity or the State; or

c) Uses or keeps in one"s possession any explosive substance, inflammable substance and arm with the aim of fulfilling the purpose of subsection (a) and (b);

B) If any person or entity from Bangladesh organizes or takes initiative to commit or instigates or abets someone to commit an offence with a purpose to impede the security of any other state or if any person or entity has any financial involvement to damage any property belonging to any other state or commits or attempts to commit or instigates or abets such offence;

C) If any person or entity knowingly uses/enjoys or possesses any property or money/fund derived from terrorist activities or uses/enjoys or keeps possession of property given by any terrorist or terrorist group;

D) If any foreign national commits an offence under sub section (a), (b) or (c) he or she shall commit the offence of organizing "terrorist activities".

2.0 DEFINING TERRORIST FINANCING

2.0 Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

'If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or

b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

2.1 For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b)'.

2.2 According to the section 7 of the Anti-Terrorism Act, 2009 (including amendment of 2012) of Bangladesh, 'financing to terrorist Activities' has been defined as follows:

7 (1): If any person or entity knowingly provides or expresses the intention to provide money, services, material support or any other property to another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person, entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

2.3 If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full of partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

2.4 If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

2.5 If any person or entity knowingly instigates another person or entity to provide or receive or make arrangement for money, services, material support or any other property in such a manner where there are reasonable grounds to believe that the same have been used or may be used in full or partially by a terrorist person or entity or group or organization for any purpose, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

3. WHY WE MUST COMBAT FINANCING OF TERRORISM?

3.1 Financing of Terrorism was criminalized under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999. To reinforce the 1999 convention, United Nations adopted UNSC Resolutions 1373 and 1390 directing member states to criminalize Financing of Terrorism and adopt regulatory regimes to detect, deter and freeze terrorists" assets. The resolutions oblige all states to deny financing, support and safe harbor for terrorists.

3.2 Bangladesh has actively involved in multinational and international institutions. Its international relationship and business, banking business in particular are regulated by some domestic and international regulations. So it is mandatory to abide by those regulations. Financial Action Task Force (FATF), the international standard setter, adopted Special Nine Recommendations on Terrorist Financing which have been merged with the revised FATF Standards. So we must be involved in international effort to combat Financing of Terrorism.

3.3 It is increasingly evident that terrorists and their organizations need to raise significant amounts of cash for a wide variety of purposes for recruitment, training, travel and materials as well as often payment for safe heaven protection. So to root up terrorism, we must stop the flow of funds that keep them in business.

3.4 The consequences of allowing the financial system to facilitate the movement of terrorist money are so horrendous that every effort must be made to prevent this from happening. So combating money laundering and financing of terrorism are not only the regulatory requirement but also an act of self-interest.

4.0 THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

4.1 The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

4.2 As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as

foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

5.0 HOW MODHUMOTI BANK LIMITED CAN HELP IN COMBATING TERRORIST FINANCING

5.1 The prevention of terrorist financing has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of preventing and deterring terrorist financing is a sound knowledge of a customer's business and pattern of financial transactions and commitments associates. The adoption of procedures by which Banks and other Financial Institutions "know their customer" is not only a principle of good business but is also an essential tool to avoid involvement in terrorist financing.

5.2 Thus efforts to combat terrorist financing largely focus on those points in the process where the terrorist's activities are more susceptible to recognition and have therefore to a large extent concentrated on the deposit taking procedures of banks i.e. the placement stage.

5.3 The Bank must keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

5.4 In complying with the requirements of the Act and in following these Guidance Notes, Modhumoti Bank Limited should at all times pay particular attention to the fundamental principle of good business practice - 'know your customer'. Having a sound knowledge of a customer's business and pattern of financial transactions and commitments is one of the best methods by which Modhumoti Bank Limited and their staff will recognize attempts at terrorist financing. It will also be dealt with in staff training programs which are a fundamental part of the procedures designed to recognize and combat Money Laundering and Terrorist Financing.

CHAPTER # 3

The Anti-Terrorism Act, 2009 (including amendments of 2012)

(Some related Important Sections)

Definitions –

Unless there is anything contrary to the subject matter, in this Act "Bank" means a bank company as defined under section 5(o) of the Bank Companies Act, 1991 (Act No. 14 of 1991) and will include any institution established as a bank under any other Act or Ordinance;+

"Suspicious Transaction" means such transactions –

i) That deviates from usual transactions;

ii) With regards to any transaction there is ground to suspect that (1) the property is the proceeds of an offence, (2) the financing of terrorist activities, a terrorist group or an individual terrorist'

iii) Any transaction or attempted transaction that are delineated in the instructions issued by Bangladesh Bank from time to time for the purpose of this Act.

"Reporting Organization" means –

1) Bank;
2) Financial institution;
3) Insurer;
4) Money changer;
5) Any company or institution which remits or transfers money or money value;
6) Any other institution carrying out its business with the approval of Bangladesh Bank;
7) Stock dealer and stock broker,
8) Portfolio manager and merchant banker,
9) Security Custodian;
10) Asset Manager;
11) Non-profit organization
12) Non-Governmental Organization
13) Cooperative Society
14) Real estate Developer;
15) Dealer in precious metals and/or stones;
16) Trust and Company Service Provider;
17) Lawyer, notary, other legal professionals and accountant;
18) Any other institution which Bangladesh Bank, with the approval of the Government, may notify from time to time.

Bangladesh Financial Intelligence Unit" means the Financial Intelligence Unit as established under section 24(1) of the Money Laundering Prevention Act 2012.

Applicability of other words and expressions –

(1) Those words and expressions that have been used in this Act but have not been defined in this Act, such words and expressions shall carry the meanings used to define them in the Code of Criminal Procedure, the Money Laundering Prevention Act, or in certain circumstances, the Penal Code.

(2) The general provisions of the Penal Code relating to offences and responsibilities with regard to sentence shall apply to the offences under this Act, as far as possible, so far as they are not contradictory to the other provisions of this Act.

Supremacy of the Act –

Notwithstanding anything contained in the Code of Criminal Procedure or any other laws for the time being in force, the provisions of this Act shall have effect.

Extra-territorial Application –

(1) If any person or entity organizes an offence within Bangladesh from outside of Bangladesh, which would be punishable under this Act if organized from Bangladesh by the said person or entity, then said office would be treated as the offence committed in Bangladesh and the provisions of this Act shall apply to the said person and offence.

2) If any person or entity from Bangladesh organizes an offence outside of Bangladesh which if organized within Bangladesh by the said person or entity would be punishable under this Act, then said office would be treated as the offence committed in Bangladesh, and the provisions of this Act shall apply to that person or entity and that offence.

Offence and Penalty for Terrorist Activities –

1. A) If any person or entity for the purpose of endangering the unity, integration, public security or sovereignty of Bangladesh, and with the aim of compelling the government or any entity or any other person to do something or preventing them from doing something by creating panic in the public or a section of the public –

a) Kills, injures seriously, puts confinement or kidnaps any person or abets to do the same, or damages any property belonging to any person or entity or the State or abets to do the same

b) Instigates any person to kill, injure seriously, puts in confinement or kidnap any person, or to instigate any person to damage any property belonging to any person or entity or the State; or

c) Uses or keeps in one's possession any explosive substance, inflammable substance and arm with the aim of fulfilling the purpose of subsection (a) and (b);

1. B) If any person or entity from Bangladesh organizes or takes initiative to commit or instigates or abets someone to commit an offence with a purpose to impede the security of any other state or if any person or entity has any financial involvement to damage any property belonging to any other state or commits or attempts to commit or instigates or abets such offence;

1. C) If any person or entity knowingly uses/enjoys or possesses any property or money/fund derived from terrorist activities or uses/enjoys or keeps possession of property given by any terrorist or terrorist group;

1. D) If any foreign national commits an offence under sub section (a), (b) or (c) he or she shall commit the offence of organizing "terrorist activities".

2) If any person or entity organizes terrorist activities, he or any person/ persons related to the person or entity whatever they may be called shall be sentenced to death, imprisonment for life or to any term of rigorous imprisonment up to a maximum term of twenty years and a minimum term of four years, and in addition to that a fine may be imposed.

3) Offences relating to financing of terrorist activities –

3.1) If any person or entity knowingly provides or expresses the intention to supply money, service, material support or any other property to another person or entity willfully and where there are reasonable grounds to believe that the full or partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity shall be treated as committing the offence of financing of terrorist activities.

3.2) If any person or entity directly or indirectly receives money, services, material support or any other property from another person or entity willfully and where there are reasonable grounds to believe that full or partial amount of the same has been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization, then he or she or the said entity shall be treated as committing the offence of financing for terrorist activities.

3.3) If any person or entity arranges or collects money, services, material support or any other property for another person or entity willfully and where there are reasonable grounds to believe that the full or the partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity will be treated as committing the offence of financing of terrorist activities.

3.4) If any person or entity instigate in such a manner, another person or entity to provide, receive, arrange or collect money, services, material support or any other property willfully and where there are reasonable grounds to believe that the full or the partial amount of the same have been used or may be used for any purpose by an individual terrorist, terrorist entity or terrorist group or terrorist organization then he or she or the said entity shall be treated as committing the offence of financing of terrorist activities.

3.5) If any person is found guilty of any of the offences set out in sub-sections (1) to (4), that person shall be sentenced to imprisonment for a term between a maximum of twenty and a minimum of four years, and in addition to this a fine may be imposed not less than the greater of twice the value of the property involved with the offence or taka 10(ten) lac.

3.6) (a) If any entity is found guilty of any of the offences set out in sub-sections (1) to (4), steps may be taken under section 18 and in addition to this a fine may be imposed not less than the greater of thrice the value of the property involved with the offence or taka 50(fifty) lac ; and

(b) The head of such entity, Chairman, Managing Director, Chief Executive Officer whatever may be called by shall be punished with an imprisonment of a term up to maximum of 20 years and a minimum of 4 years and in addition to this a fine may be imposed the greater of twice the value of the property involved with the offence or taka 20(twenty) lac unless he is able to prove that the said offence was committed without his knowledge or he had tried utmost to prevent the commission of the said offence.

3.7) Membership of a Prohibited Organization – If any person is or claims to be a member of an organization which has been prohibited under section 18, then he or she will commit an offence and shall be sentenced to imprisonment for a term not exceeding six months, or to a fine, or both.

3.8) Support of a Prohibited Organization –

(a) If any person requests or invites anyone for the purpose of supporting an organization prohibited under section 18, or arranges, directs or assists in the direction of a meeting, or makes a speech, with the aim of supporting a prohibited organization or to expedite or encourage its activities, then he or she shall commit an offence.

(b) If any person makes a speech at any meeting or on the radio or television or disseminates any information through any print or electronic medium, asking for support of any prohibited organization or with the aim of facilitating its activities, then he or she shall commit an offence.

(c) If any person is found guilty of any of the offences set out in sub-sections (1) or (2), then he or she shall be sentenced to imprisonment for a term between a maximum of seven and a minimum of two years, and an additional fine may also be imposed.

3.9) Punishment for Criminal Conspiracy – If any person conspires to commit an offence under this Act, then he or she shall be sentenced to imprisonment for a term up to two thirds of the maximum sentence prescribed for that offence, or to a fine, or both; and if the prescribed sentence for that offence is death, then the sentence for the offence shall be imprisonment for life or imprisonment not exceeding fourteen years, but it shall not be below five years" imprisonment.

3.10) Punishment for Attempt to Commit an Offence – If any person attempts to commit an offence under this Act, then he or she shall be sentenced to imprisonment for a term up to two thirds of the maximum sentence prescribed for that offence, or to a fine, or both; and if the prescribed sentence for that offence is death, then the sentence for the offence shall be imprisonment for life or imprisonment not exceeding fourteen years, but it shall not be below five years" imprisonment.

3.11) Punishment for Abetment of an Offence – If any person abets in the commission of any offence punishable under this Act, then he shall be sentenced to the prescribed sentence for that offence.

3.12) Punishment for Instigation of Terrorist Activities – If any person through doing or taking part in activities, prepares or distributes any document, or through transmission of any information through any print or electronic medium, or through any other medium, apparatus, assistance, technology or training to any person or organization, knowing that the said document, apparatus, assistance or technology or training shall be used in the commission of any offence under this Act, or the said person or organization shall use the same for their commission of such offences, then he or she shall be deemed to have instigated terrorist activities; and he or she shall be sentenced to imprisonment for a term up to two thirds of the maximum sentence prescribed for the constituted offence, or to a fine, or both; and if the prescribed sentence for that offence is death, then the sentence for the offence shall be imprisonment for life or imprisonment not exceeding fourteen years, but it shall not be below five years" imprisonment.

3.13) Sheltering an Offender –

(a.1) If any person, knowing that another person has committed an offence under this Act or having reasonable grounds for believing that person to be an offender, shelters or hides that person with the intention of protecting him/her from the sentence then –

(a.2) If the punishment of that offence is death then he or she shall be sentenced to imprisonment for a maximum of five years and a fine may be imposed in addition to this; or

(a.3) If the punishment of that offence is life imprisonment or imprisonment of any other term then, shall be liable for imprisonment for at least three years and a fine may be imposed in addition to this;

(b) The provisions of this section shall not apply if the offence of sheltering or hiding set out in sub-section (1) is committed by husband, wife, son, daughter, father or mother.

Powers of Bangladesh Bank

(1) Bangladesh Bank may take the necessary steps to prevent and identify any transactions carried out through any reporting organization for the purpose of committing any offence under this Act, and for this purpose, it will have the following powers and authority –

- Call for a report relating to any suspicious transactions from any reporting organization,
- Provide the reports received under sub-section (a) to the respective law enforcement agencies for taking necessary steps or, where applicable, provide it to the foreign law enforcement agencies upon their request or, exchange information relating to the report with the foreign law enforcement agencies.
- Collect and preserve of all statistics and records;
- Create and maintain a database containing the reports of all suspicious transactions;
- Analyze reports relating to suspicious transactions;
- If there are reasonable grounds to suspect that any transaction is connected to terrorist activities issue an written order to the respective reporting organization to suspend or freeze transactions in the relevant account for a period not exceeding 30(thirty) days. Such order may be extended for additional periods of 30 (thirty) days each up to a maximum of 6 (six) months, if it appears necessary to uncover correct information relating to transactions of the account;
- Monitor and supervise the activities of reporting organizations;
- Give directions to reporting organizations to take preventive steps to combat the financing of terrorist activities;
- Inspect reporting organizations for the purpose of identification of suspicious transactions connected with financing of terrorist activities; and
- Provide training to officers and employees of reporting organizations for the purpose of identification and prevention of suspicious transactions connected with financing of terrorist activities.

(2) Bangladesh Bank, on identification of a reporting organization or its customer as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the relevant law enforcement agency and provide all necessary cooperation to the said law enforcement agency to facilitate their inquiries and investigations into the matter.

(3) In case of offences organized in other countries under trial, Bangladesh Bank shall take steps to seize the accounts of any person or entity pursuant to any international, regional or bilateral agreement, UN conventions ratified by the Government of Bangladesh or respective resolutions of UN Security Council.

(4) The fund seized under subsection (3) shall be subject to disposal by the respective court pursuant to the respective agreements, conventions or respective resolutions of UN Security Council.

(5) In order to perform the responsibilities set out in subsections (1) to (3), governmental, semi-governmental, autonomous bodies shall provide requested information or in certain cases spontaneously provide information to the Bangladesh Financial Intelligence Unit.

(6) The Bangladesh Financial Intelligence Unit on demand or in certain cases spontaneously shall provide information relating to terrorist activities or the financing of terrorist activities to the Financial Intelligence Units of other countries.

(7) For the purpose of investigation relating to financing of terrorism law enforcement agencies shall have the right to access any document or file of any bank as per the following conditions:

a) with an order from an appropriate court or tribunal;

b) with the approval of Bangladesh Bank.

Duties of Reporting Organizations –

(1) Each reporting organization shall take necessary measures, exercising appropriate caution and responsibility, to prevent and identify financial transactions through them connected to any offence committed under this act and if any suspicious transaction is identified, shall spontaneously report it to the Bangladesh Bank without any delay.

(2) The Board of Directors, or in the absence of the Board of Directors the Chief Executive Officer or whatever may be called by, of each reporting organization shall approve and issue directions regarding the duties of its officers, and will ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting organizations, have been complied with.

(3) If any reporting organization fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provide any wrong information or false information or statement, the said reporting organization shall be liable to pay a fine determined and directed by Bangladesh Bank, not exceeding Taka 10 (ten) lakh and Bangladesh Bank may suspend the registration or license with a purpose to close the operation of the said agency/organization or any branch, service centre, booth or agent of that organization within Bangladesh or where applicable, shall inform the registration/licensing authority about the subject matter to take appropriate action against the organization.

(4) If any Reporting Organization fails to pay any fine imposed by Bangladesh Bank under sub sections 3 of this Act, Bangladesh Bank may recover the amount from the reporting organizations by debiting their accounts maintained in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized Bangladesh Bank may make an application before the relevant court for recovery.

Terrorist Organizations

Organizations Involved in Terrorist Activities – For the purpose of fulfilling the aims of this Act, an organization will be deemed to be involved in terrorist activities if –

- It commits terrorist activities or takes part in such activities;
- It makes preparations for terrorist activities;
- It assists in or encourages the commission of terrorist activities;
- It supports and abets any organization involved in terrorist activities;
- It is included under United Nations Resolution 1267 or 1373 and other resolutions ratified by Bangladesh; or
- It is involved in terrorist activities in any other ways.

Prohibition of Organizations –

(1) For the purpose of this Act, having reasonable grounds to believe that an organization is involved in terrorist activities, the government may prohibit it, through an order enlisting it in the Schedule.

(2) The government may by an order include any organization in the Schedule, or remove any organization from the Schedule, or amend the Schedule in any other manner.

Review –

(1) An organization aggrieved by an order of the government under section 18 , may within thirty days of the date of issuance of the order, make a written application with grounds to the government for review, and the government, considering the rules promulgated under this Act, shall dispose of the application within ninety days of receipt.

(2) If the application for review under sub-section (1) is refused, the said aggrieved organization, within thirty days of such refusal, may prefer an appeal before the High Court Division.

(3) The government shall constitute a three member Review Committee for disposal of the review applications filed under sub-section (1). by notification in the Bangladesh Gazette.

Taking Steps against Prohibited Organizations –

(1) If any organization is prohibited the government, in addition to the other steps set out in this Act, considering the rules promulgated under this Act, shall take the following steps :-

- ∇ Shall shut the offices of the organization, if any;
- ∇ Shall freeze its bank and other accounts, if any and shall seize all property;
- ∇ Shall confiscate all types of pamphlets, posters, banners or other print, electronic digital or other material; and
- ∇ Shall prohibit the publication, printing or circulation of press statements, press conferences or the giving of speeches by the prohibited organization, or its favor or support.

(2) The prohibited organization shall present accounts of its income and expenditure and shall disclose the sources of all its income to the relevant authority nominated for this purpose by the government.

(3) If it appears that the funds and assets of the prohibited organization have been earned in an illegal manner or have been used in the commission of an offence under this Act, then the said funds and assets shall be confiscated in favor of the State.

Mutual Legal Co-operation-

(1) When a terrorist activity is carried out in such a way or the carrying out of such activity is assisted, attempted, conspired or financed in such a way that it involves land of a foreign state, or when a terrorist activity is carried out or the carrying out of such activity is assisted, attempted, conspired or financed from a foreign state in Bangladesh or in a foreign state from Bangladesh and if that state requests the Bangladesh Government, then Bangladesh government, upon receiving request from the foreign state shall, if satisfied, provide legal cooperation to that foreign state as per any agreement in respect of criminal investigation, trial or extradition related necessary matters subject to the remaining provisions of this section.

- ❖ The terms and conditions of the legal cooperation shall be decided vide a formal agreement or by exchanging views in writing between the requesting state and the request receiver state by mutual exchange of views.
- ❖ In absence of mutual understanding between countries no Bangladeshi citizen shall be handed over to a foreign state for trail of offence friable under this Act; however, the handover of any Bangladeshi citizen shall not be executed if the person is under trial in any court in Bangladesh for the same offence.
- ❖ Any Bangladeshi citizen may be handed over to a foreign state, with his permission, to provide assistance as a witness to assist in the relevant criminal case or investigation for the purpose of mutual legal cooperation under this Act.
- ❖ If the Government has sufficient reasons to believe that a foreign country has requested legal cooperation for trial or providing punishment purely on the basis of the ethnicity, religion, or nationality or political belief, then it may refuse the request of extradition or mutual legal cooperation in the specific case as the receiver state requested.

General Provisions

Cognizance of offence and bail requirements –

(1) All offences under this Act shall be cognizable.
(2) All offences under this Act shall be non-bail able.

Necessity of prior approval in relation to investigation and trial of such cases –

(1) Without the prior approval of the District Magistrate, no police officer shall be able to investigate a case under this Act.
(2) Without the prior sanction by the government, no court shall take an offence into cognizance for trial.

Special Tribunal and transfer of cases from Special Tribunal –

Government, at any stage of the trial before the completion of taking of evidence, may transfer a case or any number of cases under this Act from a Sessions Court to a Tribunal or from a Tribunal to a Sessions Court for reasonable grounds.

Power to amend Schedule –
Government may amend the schedule of this Act by issuing notification it in Bangladesh gazette.

Power to make rules –
Government may, by notification in the Bangladesh gazette, make rules for carrying out the purposes of this Act.

Original text and English text – The original text of this Act shall be in Bangla and there shall be a reliable English translation.

Provided that, in case of any contradiction between Bangla and English version, the Bangla version shall take precedence.

Repeal and savings –

(1) The Anti-Terrorism Ordinance 2008 (Ordinance No. III of 2012) is hereby repealed.
(2) Notwithstanding such repeal, the provision of the enactments under the repealed ordinance shall be treated as having been enacted under this Act.

CHAPTER # 4

Institutional Policy

1. Purpose and contents:

1.1 Both money laundering and financing of terrorism have been identified as major threat to the financial services community especially to Banks. Modhumoti Bank Limited has recognized and believes that prevention of money laundering and combating financing of terrorism is a team effort. This section outlines policies, procedures and measures to be taken for combating financing of terrorism. All employees of Modhumoti Bank Limited must comply with the terms of this policy meticulously.

1.2 Managers, employees and technical personnel must modify system configurations and procedures, if necessary to comply with this policy immediately.

2. Policy Statement:

2.1 Pursuant to the recently enacted Anti-Terrorism Act, 2009 (including amendments of 2012) and BFIU circular No. 26 dated 16JUN2020 issued by BFIU, guided to have defined responsibilities of Banks to combat financing of terrorism. Modhumoti Bank Limited acknowledges and supports the increasing need for a partnership between the governments, regulators, law enforcement authorities, banks and the general public to work together to combat terrorist financing. We are determined to play our role in this partnership.

2.2 We are committed to sustaining high standard of identification and Know Your Customer (KYC) information across our entire customer base and also to guard against undertaking any transaction that is or may be connected with or may facilitate terrorism or terrorist financing.

2.3 We strongly believe that on- going monitoring of transactions is equally as important as KYC procedure. We also consider that building up awareness amongst the staff is also important to prevent damage to the bank's reputation and ensuring compliance with the respective legislation and regulations. Accordingly, Modhumoti Bank Limited is committed to implement the provisions of the Anti-Terrorism Act, 2009 (including amendments of 2012) and also the guidelines and instructions of Bangladesh Bank issued from time to time in respect of transaction monitoring systems and operational processes.

2.4 We are strongly committed to assist and cooperate with the relevant law enforcement authorities in Bangladesh whenever possible and to the fullest extent possible. Furthermore, Modhumoti Bank Limited also renew it's commitments to:

- Train all of the employees;
- Work closely with the respective law enforcement authorities;
- Meet all of the legal and regulatory obligations;
- Work with industry bodies to promote the highest standards of AML/CFT controls across the financial services industry.

2.5 This is the policy of the Bank to adhere to all of the provisions of Anti-Terrorism Act, 2009 (including amendments of 2012) and other regulations by implementing this policy and subsequent procedures.

3. Enforcement:

3.1 Changes to this policy require approval to the Board of Directors. The Changes in operating procedures, standards, guidelines and technologies, provided they are consistent with this policy, may be authorized by the DMD & Chief Anti-Money Laundering Compliance Officer (CAMLCO), Head of Credit, Head of Business, Head of General Banking Operations and Head of Internal Control and Compliance.

3.2 The Board of Director is the appropriate authority to approve this policy and any amendments thereafter. Senior Management of the bank is responsible for ensuring the directives are implemented and administered in compliance with the approved policy.

3.3 The AML policy of the Bank should be followed by all concerns for ensuring the regulatory requirements in relation to all procedural issues.

3.4 Any conflict in interpretation of this policy should be submitted immediately to the CAMLCO or Head of internal Control and Compliance for ruling.

4. Exceptions to policy:

Request for exceptions to this policy must be very specific may only be granted on specific items, rather than to entire sections. Bank personnel with exceptions are to communicate their request to CAMLCO directly.

5. Procedure:

5.1 Modhumoti Bank Limited is committed to combat financing of terrorism and the bank already has a separate internal procedure to prevent money laundering and combat terrorist financing. The bank has also formed a separate & independent division as per BFIU instructions namely Anti-Money Laundering Division (AML&CFTD). The AML&CFTD is responsible for overall supervision & implementation of AML/CFT policy in the Bank in compliance with BFIU, Bangladesh Bank's instructions.

5.2 Modhumoti Bank believes that strict adherence to our existing CFT policies provides basic TF controls which also serves as primary controls for detection and prevention of terrorist financing. Therefore, in addition to the existing CFT policy the following extra due diligence and vigilance must be exercised to detect and prevent financing of terrorism.

6. Features of CFT Policy

6.1 The CFT policy of Modhumoti Bank Limited is written, approved by the Board of Directors, and noted as such in the board meeting minutes.

6.2 The CFT compliance policy establishes clear responsibilities and accountabilities within the bank to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using its facilities for the financing of terrorist activities, thus ensuring that it comply with its obligations under the law and regulations

6.3 The Policies are based upon assessment of the Terrorist financing risks, taking into account of the Bank's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to terrorist financing.

6.4 The Policies include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures addresses it's Know Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness.

6.5 The Bank includes a description of the roles the Anti-Money Laundering Compliance Officers(s)/division and other appropriate personnel will play in monitoring compliance with and effectiveness of CFT policies and procedures.

6.6 The CFT policies will be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing CFT rules and regulations or business.

6.7 In addition the policy emphasizes the responsibility of every employee to protect the bank from exploitation by financer to the terrorist activities, and should set forth the consequences of non-compliance with the applicable laws and the bank's policy, including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any association with terrorist financing activity.

7. Senior Management Commitment

7.1 The senior management of the Bank including the Chief Executive Officer / Managing Director and the Board of Directors are committed to ensure the compliances with their obligations under the law, which is most important element of a successful CFT program.

7.2 Senior management is aware about that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of bank's CFT policy bank will communicate clearly to all employees on an annual basis through a statement from Managing Director that clearly sets forth its policy against terrorist financing and any activity which facilitates terrorist financing. Such a statement will be the evidence of the strong commitment of the bank and its senior management to comply with all laws and regulations designed to combat terrorist financing. The statements may be circulated in conjunction with the AML Policy statements.

CHAPTER 5

COMPLIANCE REQUIREMENTS

1. Policies for Prevention Combating Terrorist Financing

In pursuance of section 16(2) of Anti-terrorism (Amendment) Act, 2012, and Anti Money Laundering Department's letter dated 04.07.2006, all banks must have their own policy manual approved by their Board of Directors/top most committee to combat terrorist financing. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh. Banks shall from time to time review and confirm the meticulous compliance of the circulars issued by Bangladesh Bank.

2. According to Anti-Terrorism Act, 2009 (including amendments of 2012) the responsibility of the reporting Agency is:

a) All the reporting Agency in view to combat and detect monetary transaction involved with crime shall take necessary action with due care and responsibility and if suspicious transaction is detected should be reported to BFIU, Bangladesh Bank proactively without delay.

b) The Board of directors of every reporting agency or the CEO in absence of the Board will approve and issue instructions regarding the responsibility of the officers to combat Terrorist financing and will ensure the implementation in the Bank.

3. AML&CFT Circular

According to the AML&CFT Circular 26 banks shall perform the following activities as per requirements under the Anti-Terrorism Act, 2009 (including amendments of 2012):

a) Anti-Money Laundering Division of the Head office and the officer nominated at the branch level shall perform the duty of compliance and internal monitoring of the instructions Anti-Terrorism Act, 2009 (including amendments of 2012) and the relevant instructions issued by the Bangladesh Bank.

b) Bank shall develop a system to detect and prevent transactions related to terrorist financing through banking channel.

c) If there is any reasonable ground to suspect that a transaction or an attempt of transaction has connection to financing terrorist activities as Anti-Terrorism Act, 2009 (including amendments of 2012) shall have to be reported the same day with comments of the branch compliance officer to the AML&CFTD of the bank. AML&CFTD will examine and review the received report and will send to the Operational; Head & General Manager of Bangladesh Financial Intelligence Unit, Bangladesh Bank with Confidentiality. In case of sending the report to Bangladesh Bank, the AML&CFTD shall not in any way, delay for more than three working days from the date of the receipt of the report from the branches.

d) Board of Directors of the bank shall approve and circulate relevant instructions to be followed by the bank officials and shall send a copy these instructions to BFIU, and shall also ensure the compliance of the instructions circulated by BFIU.

e) While reporting Suspicious/unusual Transaction Report under Anti-Terrorism Act, 2009 (including amendments of 2012) Annexed Form Ka of AML&CFT Circular 26 shall have to be used to report the STRs related to terrorist financing.

4. AML&CFT Circular Letter in Relation to UN Sanctions List

As a member of the United Nations, Bangladesh is obliged to comply with the instructions of the resolutions adopted by the Security Council under Chapter-VII of UN Charter. Besides, instructions are effective to comply with the United Nations Security Council Resolution 1267 and its successor resolutions and other resolutions to freeze without delay any account/transaction operated in the name of the person(s) or institution(s) listed in those resolutions or institution(s) owned or controlled directly or indirectly by them under sections 15(3) and 17(e) of Anti-Terrorism Act, 2009 (including amendment of 2012).

The following instructions have been issued by Bangladesh Financial Intelligence Unit (BFIU) as per power conferred in section 15(1)(h) of Anti-Terrorism Act, 2009 (including amendment of 2012) for compliance by the Bank:

A. The instructions contained in the United Nations Security Council Resolution 1267(1999) and its successor resolutions and other resolutions have to be complied and if any account/transaction operated in the name of the person(s) or institution(s) listed in those resolutions or in the name of institution(s) owned or controlled directly or indirectly by them; the account(s) have to be frozen without delay and the same have to be reported to BFIU.

B. Any account/transaction operated in the name of the person(s) or institution(s) listed by the Government of the People's Republic of Bangladesh on the basis of the Resolution 1373(2001) adopted by the United Nations Security Council, or institution(s) owned or controlled directly or indirectly by them; the account(s) have to be frozen without delay and the same have to be reported to BFIU.

C. Any account/transaction operated in the name of the person(s) or institution(s) listed in Resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing, adopted by the Security Council under Chapter VII of the United Nations Charter, or in the name of institution(s) owned or controlled directly or indirectly by them; the account(s) have to be frozen without delay and the same have to be reported to BFIU.

D. Necessary measures have to be taken by collecting the list prepared under those resolutions proactively from the UN website (http://www.un.org/sc/committees/index.shtml)

Bank has been instructed to provide necessary directions to all concerned to ensure proper compliance of the aforesaid instructions.

CHAPTER # 6

CDD/KYC, Monitoring and Reporting

1. General procedures for Customer due Diligence (CDD)/ know your Customer (KYC):

1.1) The uniform account opening form provided by BFIU including Transaction profile (TP) and CCD/ KYC profile is the integral part of establishing account relationship. It is mandatory and a vital reference point to all account relationship.

1.2) With regard to CCD/KYC, Transaction Profile, Customer risk assessment, record keeping and suspicious transaction reporting, the branch will follow the procedure of AML policy and Guidelines of the Bank.

1.3) While CDD/KYC is an important component of the AML/CFT process, the ongoing monitoring of individual transactions on customer account is critical to improving our ability to detect criminal activity.

1.4) The IT Division is responsible to develop automated systems and processing for classifying customers on the basis of the risk matrix provided by Bangladesh Bank, monitoring transactions with the transaction profile provided by the customers. This new systems will improve our ability to detect unusual transactions, help authorities to identify and respond to new terrorist financing techniques. Modhumoti Bank Ltd has incorporated AML into our Core Banking software to be able to improve our ability to detect unusual transactions and which will help us to identify and respond to new money laundering and terrorist financing technique including auto CTR reporting to our regulators. Furthermore it will enhance our ability to monitor account activities and report to our regulators new and more sophisticated trend and techniques adopted by the criminals.

1.6) Branch Manager-Operations /Branch Anti Money Laundering Compliance Officers (BAMLCO) will monitor customers transaction regularly in order to identify suspicious transaction/activities relates terrorist financing. He will also oversee the day to day activities at the branch and confirm compliance of the instructions of concerned authority.

2. Correspondent Banking Relationship

Correspondent banking relationships sometimes creates a risk that the other Bank's customer may be using that Bank for financing terrorism. It is not necessarily possible to conduct due diligence on that Bank's customer base and as such, these relationships require additional care and attention to guard against becoming unwilling participants in this activity. The following control should be implemented for establishing corresponding banking relationship (Reference: Bangladesh Bank AML&CFT Circular # 24 dated March 03, 2010):

2.1) Bank before providing correspondent banking service, senior management's approval must be obtained. On being satisfied about the nature of the business of the respondent bank through collection of information (KYC on AML Questionnaire) as per annexure attached with the circular.

2.2) Bank should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority.

2.3) Bank should not establish or continue a correspondent banking relationship with SHELL BANK or Bank's which maintain relationship with SHELL Bank (here Shell Bank refers to such banks as are incorporated in a jurisdiction where it has no branches / physical presence in the country in which it is incorporated and licensed and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. physical presence means meaningful mind and management located within the country). The existence simply of a local agent or low level staff does not constitute physical presence.

2.4) Correspondent Banking relationship shall not be established or continued with those responded bank that established correspondent banking relationship or maintain account with a shell bank.

2.5) Bank should pay particular attention when maintaining a correspondent banking relationship with bank incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries & territories enlisted in FATF's non cooperative countries

and Territories list). Enhanced due diligence shall be required in such case. Detail information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.

2.6) No payment –through account which extended payment facilities to the customers of other institutions, often foreign banks should normally be allowed unless verifying the identity of and have performed on –going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data to the Modhumoti Bank Limited upon request.

2.7) The Bank will review correspondent banking relationship as and when required.

2.8) Before establishing relation Bank will be satisfied with the respondent institution's Anti money laundering and Anti-Terrorism control.

3. Non-Profit Organization (NPO) and Non-Government Organization (NGO)

3.1) Account of Charities, NGO & NPO to be treated as high risk account. No account shall open without the registration from the appropriate Government authorities i.e. NGO Affairs Bureau, Directorate of Co-operative Society, and Director of Social Welfare where applicable.

3.2) Enhancement of Due Diligence (EDD) will be performed for opening and operating such account to prevent money laundering & terrorist financing. As per foreign donation regulations (voluntary Activities) ordinance, 1978 and foreign contribution (Regulation), 1982 no person or organization can accept or expense the foreign fund/donation for voluntary activities without the prior permission of the Government. The Bank shall release the fund after ensuring that necessary approval of the NGO Affairs Bureau (Government Entity) has been obtained. Periodical monitoring of transaction is a must to observe the nature of transaction. Account of such organization should be treated as high risk account and transaction in the account should be monitored regularly.

Simplified CDD will be done for low risk accounts like Student Accounts, Farmer's Accounts and other No-Frill accounts.

4. Cross Border Wire transfer:

4.1) All cross-border wire transfer must be accompanied by accurate and meaningful originator information.

4.2) Information accompanying cross boarder wire transfer must contain the name and address of the originator and where an account exists, the number of that account, in the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

4.3) Where several individual transfer from a single originator are bundled in a batch file for transmission to beneficiaries in another countries, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at 4.2 above.

5. Domestic Wire Transfer:

Information accompanying all domestic wire transfers of BDT 25,000.00 and above must include complete originator information i.e. name, father and mother's name, address , account number, identification number, date of birth etc., unless full originator information can be made available to the beneficiary bank by other means.

6. Alternative remittance:

Bank should take measures to ensure that persons or legal entities, including agents that provide a service for the transmission of money or value including transmission through an informal money or value transfer system of network should be licensed or registered and subject to all the FATF recommendations that apply to banks and non bank financial institutions. Bank should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanction. In this regard it should be considered that 'Hundi' business is prohibited in Bangladesh.

7. Transaction Monitoring Process

7.1) Bank should have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for bank to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the customer. Possible areas to monitor could be: -

a. transaction type
b. frequency
c. unusually large amounts
d. geographical origin/destination
e. changes in account signatories

It may not be feasible for specific branches of the bank having very large number of customers to track every single account against the TP where a risk based approach should be taken for monitoring transactions based on use of "Customer Categories" and "Transaction Limits" (individual and aggregate) established within the branch. The Customer Category is assigned at account inception - and may be periodically revised - and is documented on the Transaction Profile. Transaction Limits are established by the business subject to agreement by BAMLCO. The Customer Categories and Transaction Limits are maintained in the manual ledgers or computer systems

8. Suspicious Transaction Report:

When there is suspicion that funds are linked to terrorist financing, staff members are required to submit STRs to their respective Branch Anti Money laundering officer (BAMLCO). BAMLCO must send (if justified) STR to AML&CFTD on the same day as per format provided by Bangladesh Bank in BFIU Circular No. 26/2020. The STR must be reported to BFIU, Bangladesh Bank within three working days from the day of detection, if it is considered to be reported to Bangladesh Bank. Reporting procedures should be followed as per Policy.

9. Indicators of STR / Suspicious Transactions Activity:

- Customer is evasive or unwilling to provide document & information as & when requested.
- Customer using different identification for different transaction.
- Customers frequently visit high risk countries.
- Customer exchanging small denomination notes into large denomination notes, in large quality.
- Customer having relations with persons working abroad in an illegal job.
- Customer giving false information.
- Persons directly or indirectly involved in smuggling.
- Information given in KYC is inconsistent with his income and business.
- Person's Transaction is not consistent with his income and business.
- Source of fund does not cover his transaction profile.
- Deposits of funds with a request for their immediate transfer elsewhere;
- Unwarranted and unexplained international transfers.
- The payment of commissions or fees that appears excessive in relation to those normally payable.
- Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type of transaction or particular method of transacting.
- Transactions do not appear to be in keeping with normal industry practices.
- Purchase of commodities at prices significantly above or below market price.
- Unnecessarily complex transactions;/structuring of transactions to avoid CTR.
- Buying or selling securities with no apparent concern for making a profit or avoiding a loss.
- The transaction in which there is reason to believe that the proceeds came from illegal / criminal activities.
- Large cash deposit through online.
- Change of transaction pattern i.e. maximum number transaction than previous.

- Remittance received from different places which are not consistent with the clients business or income.
- Frequent transaction with Border areas branches.
- Huge transaction in deposit/withdrawal but less available balance.
- Sudden huge cash deposit/ transfer deposit.
- Customer withdrawing large sum of money in cash immediately after receipt of credit
- Branch request to customer to contact us which customer avoided or did not respond.
- Customer reluctance or refusal to disclose other banking relationships.
- Large number of individuals making payment in to the same account without an adequate explanation.
- Customer who repay problem/default/classified loans unexpected.

CHAPTER # 7

MISCELLANEOUS

1. Tipping off Customer:

The term "tipping off" the customer simply refers disclosure of filing of suspicious transaction/activity report to the customer. Bank must ensure the confidentiality of STR / SAR.

2. Training and Awareness of the Employees:

Modhumoti Bank Limited will continue to devote considerable resources to establish and maintain our employees' awareness of the risks terrorist financing and their competence to identify and report relevant suspicious in this area. We are dedicated to a continuous training program of increasing awareness and training of employees' at all appropriate levels in relation to their knowledge and understanding of CFT issues, their respective responsibilities and the various controls and procedures introduced by the bank to deter financing of terrorism. An element of this continuous program will reflect information and feedback received from the regulators and law enforcement authorities on CFT practices and the effectiveness of our efforts.

3. Self-Assessment:

CFT policy requires that appropriate and timely self-assessment, test audits and evaluations be conducted to ensure the bank is in compliance with the regulators. Each and every branch must assess their performance half yearly according to BFIU circular No. 26 issued by BFIU. The short comings identified must be overcome and complied with in next quarter.

It is mentionable that compliance of CFT is the responsibility of each employee of the Bank. Therefore, all guidelines related to CFT are regularly updated and circulated and ensure that all staff members are aware of the Anti-Terrorism Laws, internal guidelines and other policies and procedures.

4. Customer Acceptance policy

Customer is vitally important for banking business. Increasing competition is forcing banks to pay much more attention to satisfy customers. Our motto is to extend best services to the customers. We are also aware that sometimes pose the risk of financing of terrorism to the financial institutions particularly the banks. So the inadequacy or absence of KYC standards can result in serious customer and counterparty risks, especially reputation, operational, legal and compliance risks.

Collecting sufficient information about our customers is the most effective defense against being used as the medium to finance the terrorist activities through bank account. As per section 25 of MLP Act, 2012, each bank requires to keep satisfactory evidence of the identity of those it deals with and also require making necessary arrangement to prevent any transaction related to crimes as described in Anti-Terrorism Act-2012 (including amendments of 2012). It is also the responsibility of each bank to identify suspicious transactions of their customers with due care and diligence. Pursuant to above legal bindings, Section 5.3 of Guidance Notes on Prevention of Money laundering issued by Bangladesh Bank and apropos to international standard the management of the bank has developed the Customer Acceptance policy as under:

Bangladesh FIU recommended in their Guidance Notes on Prevention on Money Laundering to develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Guidelines for Customer Acceptance Policy for the Bank are given below:

1) No account shall be opened in anonymous or fictitious/ name(s) entity/entities
2) No numbered account shall be opened
3) Account opening Form, KYC profile Form and Transaction Profile Form should be properly filled in.
4) Customer risk must be assessed as per parameters of risk perception as clearly defined in KYC profile Form.
5) No account would be opened or existing account would be closed if bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and or obtain documents required as per the risk categorization due to non-cooperation of the customers or non-reliability of the data or information furnished to the bank. While carrying out due diligence it would be ensured that there is no harassment to the customer. The decision to close an account would be

taken by the branch Manager after giving due notice to the customer, explaining the reasons for such a decision.

6) While carrying out due diligence, it shall be ensured that the procedure adopted shall not become too restrictive and must not result in denial of banking services to general public, specially to those, who are financially or socially disadvantage.
7) Before opening a new account, necessary checks shall be conducted so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorist or terrorist organizations/financer etc. No account will open or conducted as per UN Sanction, OFAC Sanction and directed by Bangladesh Bank or any other sanction list.
8) Account will not be opened through Online. In case of foreign resident account may be opened through Bangladesh Mission or own bank branch if available or legal representative obtaining KYC, ETP, source of income and completing risk grading.
9) Customer for whom reports of unusual or suspicious transaction are repeatedly submitted to the BFIU, if it is known, account of such person /entity should not be opened & not to be opened in Sl. No.7-9.
10) Customer for whom the collection of information for assessing their overall profile is impossible.
11) Customer whose activities or transaction are not consistent with the information available on them, their professional activity, their risk profile and the origin of the fund.
12) Customer failing to provide all information required for the identification and verification of their identity.
13) Enhanced due diligence will be exercise for opening accounts of politically exposed person (PEPS) in line with the BFIU Circular No. 26 issued dated 16/06/2020 and revised FATF Standards-2012. PEPS account to be opened with the consent of Head office and Foreign Exchange Regulation Act, 1947 and Guidelines for Foreign Exchange Manual. The account activities of the PEPS's will be monitored so that any changes may be detected and consideration can be given as to whether such change suggests corruption or misuse of public assets. This includes close scrutiny of receipts of large sums not consistent with the occupation or business of the PEPS
14) No account will be opened without name, address, signature etc.
15) Customer due diligence: Bank is required to know true identity of the person wanting to open an account. Each new customer is accepted for banking relationship after application of customer due diligence (CDD) measures such as verification of identity, address, nature and location of business activities/profession, purpose of intended bank account, social and financial status, source of funds etc. The Bank will apply Customer Due Diligence measures when it:

- establishes a business relationship
- carries out an occasional transaction
- Suspect money laundering or terrorist financing or
- Doubt the veracity of documents, data or information previously obtained for the purpose of identification or verification.

16) SHELL BANK: Bank will not establish correspondent relationship with Shell Bank and the bank is maintaining relationship with Shell bank.
17) Trust/ Nominee or Executors, Administrator's Account: Branch should determine whether customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so branch may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain detail of the nature of the trust or other arrangement in place. While opening an account for a trust should take reasonable precautions to verify the identity of the trustees and the settlers of trust, guarantors, protectors, beneficiaries and signatories.
18) Beneficial owners: Beneficiaries should be identified when they are defined. In the case of a "Foundation", Branches should take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Source of fund, income or wealth and complete information on the actual or beneficial owners of the accounts holding

controlling/ownership interest share of the account must be obtained at the time of opening of any account.

19) Correspondent Banking relationship: Bank can maintain correspondent Banking relationship following the terms and condition as laid down in BFIU Circular No. 26 dated 16/06/2020.
20) Non- resident Bangladeshi and Foreign national: Bank is allowed to open and conduct both type of account maintaining Foreign Exchange Regulation Act, 1947 and Guidelines for Foreign Exchange Transaction. To be confirmed the source of income, KYC, TP and risk grading.
21) NGO, NPO, and Club, society, charitable organization: Bank can open the account in the mentioned name. All information in line with AML/CFT policy to be fulfilled and transaction should be monitored regularly.
22) The Branches where locker service facilities exist will follow the identification procedures for their customers. No locker should be opened without maintaining account properly.
23) The Branch shall verify the identity of the customer using reliable sources, document etc. but it must retain copies of all references, documents used to verify the identity of the customer.
24) The customer address should be verified as per AML/CFT policies as well as MMBPLC policy.
25) Circumstances, in which a customer is permitted to act on behalf of another person/entity should be strictly followed so as to avoid occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity

5. Record Keeping

Bank should retain the correct and full records of customers' identification and transactions while operating an account of a customer, and to retain the records of customers' identification and transactions at least for five years after closing of relationships with the customers are essential constituents of the audit trail that the law seeks to establish.

FATF also recommended that financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

As per FATF revised standard 2012, records of occasional transaction also to be preserved up to 5 (five) years. Besides, Financial institutions need to preserve any sorts of analysis regarding the customer.

If the bank has submitted a report of suspicious transaction to BFIU or where it is known that a customer or transaction is under investigation, it should not destroy any records related to the customer or transaction without the agreement of the BFIU or conclusion of the case even though the five-year limit may have been reached.

SHARING OF RECORD/ INFORMATION OF CUSTOMER TO LAW ENFORCING AGENCY

Under the provisions of Anti-Terrorism Act-2012 (sec.15 sub. sec.7) , Bank shall not share account related information & document to the law enforcing agencies to investigate financing of terrorism cases without having approval from the appropriate court or tribunal or prior approval from Bangladesh Bank.

CHAPTER # 8

RESPONSIBILITIES OF BANK OFFICIALS

To comply with AML&CFT Circulars issued by Bangladesh Bank, the responsibilities of Bank officials are mentioned below:

A. Every Bank official will take necessary measures / apply due diligence and try to prevent and detect monetary transactions through banking channel involved in any terrorist activities.
B. Providing necessary statement to Bangladesh bank and shall preserve statement/ reports maintaining due confidentiality as per AML/ CFT Act.
C. Stop /freeze activity of any account as per instruction of BFIU, Bangladesh Bank. Strictly follow every instruction issued from Bangladesh Bank & Head office with regard to the Anti- Terrorism Act-2012.
D. Assist Bangladesh Bank Inspection team in their work. And also assist "Law Enforcing Agencies" authorized by the appropriate court or Bangladesh Bank.
E. Suspicious transaction also requires to be reported under the Law ATA 2012. BAMLCO has a vital role to submit STR.
F. Compliance of rules and regulations of Anti-Terrorism Act is the responsibility of each and every officer in Modhumoti Bank in the normal course of their assignment. It is the responsibility of the officer to become familiar with the rules and regulations that relate to his/her respective area, ignorance of the rules and regulations is no excuse for non-compliance. Employee will be held accountable for carrying out their responsibilities pertaining to compliance.
G. If an employee knows or suspect that customer is a terrorist, a member of an organized crime organization or a politically exposed person (PEPS) who is being investigated for a crime, the employee must immediately notify the BAMLCO, the compliance officer. The BAMLCO should immediately report the STR to the AML&CFTD proactively. The employee who violate the policy and the business related procedures may be subject to disciplinary action even termination of employment. Such violation could jeopardize or damage the institutional reputation and management. If an institution is convicted of the crime of money laundering or terrorist financing, resulting in fine and other serious punishment which may result in cancellation of business license and imprisonment of its officials.
H. Bank officials shall not disclose any information of STR, information regarding investigation with ill motive to the customer, organization or news media which is punishable act as per AML Act 2012.We must ensure the confidentiality of STR/SAR or investigation report.

I. Under the Law if any officer fails to comply with the instruction or provide false information willingly or provide false information or statement to BFIU or Law enforcing agencies, it is punishable act under this Law.
J. To detect suspicions transaction, monitoring of transaction matching with the TP/ actual income or business transaction should be reviewed. It is the responsibility of every official.
K. It is the responsibilities of every official to retain correct & full record of customers" including occasional customer information and transaction at least 5 (Five) years both domestic and international after retirement of relationship with the customer as to provide evidence for prosecution for terrorist financing behavior.

11.12.2025 11/12/2025

--- THE END ---