

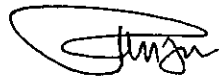
ANTI MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM POLICY GUIDELINE

November, 2019



Anti-Money Laundering & Combating Financing of Terrorism Division
The Premier Bank Limited
Head Office, Dhaka.

Reviewed and Updated By:



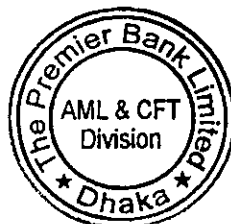
(Md. Ramjan Ali)
AVP, AML & CFT Division

Submitted By:



(Sami Karim)
DMD & CAMLCO

APPROVED BY BOARD OF DIRECTORS OF THE BOARD ON NOVEMBER 27, 2019

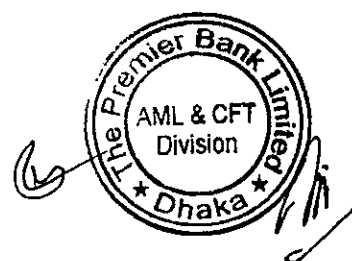


AML & CFT POLICY GUIDELINE**TABLE OF CONTENTS**

<u>Chapter No.</u>	<u>Chapter Name</u>	<u>Page</u>
Chapter : 1	Introduction	3
Chapter : 2	International and National Anti-Money Laundering Initiatives	10
Chapter : 3	Money Laundering Prevention Act	17
Chapter : 4	Institutional Policy	22
Chapter : 5	Requeirments of Anti-Money Laundering Policy	23
Chapter : 6	Organizational Structure and H.R Initiatives	25
Chapter : 7	Customer Due Dillgence	35
Chapter : 8	Recognition and Reporting of Suspicious Transactions/Suspicious Activities	48
Chapter : 9	Other Reports	57
Chapter : 10	Record Keeping	59
Chapter : 11	Awareness Programs	63
Chapter : 12	Correspondent Banking Relationship	67

CFT GUIDELINE

<u>Chapter No.</u>	<u>Chapter Name</u>	<u>Page</u>
Chapter : 1	Background	71
Chapter : 2	Terrorism and Terrorist Financing	74
Chapter : 3	The Anti Terrorism Act, 2009 (including amendments of 2012)	77
Chapter : 4	Institunal Policy	85
Chapter : 5	Compliance Requirements	88
Chapter : 6	CDD/KYC, Monitoring and Reporting	90
Chapter : 7	Misc.	94
Chapter : 8	Responsibilities of Bank Officials	97



CHAPTER 1**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 financiers 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.

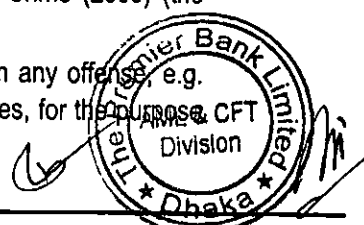
1.5 Keeping the above mandatory requirement in view, The Premier Bank Limited has prepared this handbook giving the title "Anti Money Laundering Policy (Revised)". This Book contains the fundamentals of the Guidance Notes of Focus Group as well as the recent changes and its implication procedures; we 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 from BFIU time to time and some important recent developments in AML/CFT regime.

1.7 It is expected that each and every employee of The Premier 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



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 Money Laundering 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;

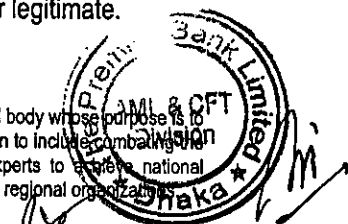
(viii) Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

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.

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.



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 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.

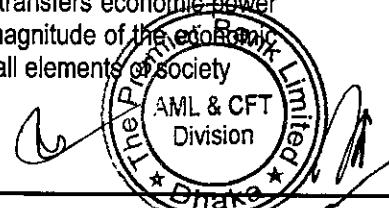
4.2 Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate. We also 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 lose 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:

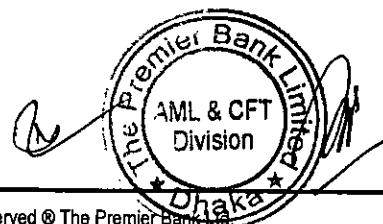
5.1 It is generally recognized that effective efforts to combat money laundering cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies. Accordingly, in order to address the concerns and obligations of these three parties,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

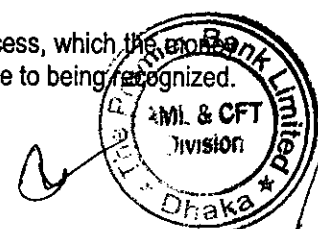
Placement stage	Layering stage	Integration stage
i) Cash paid into bank (sometimes with staff complicity or mixed with proceeds of legitimate business).	i) Sale or switch to other forms of investment.	i) Redemption of contract or switch to other forms of investment.
ii) Cash deported.	ii) Money transferred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

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.

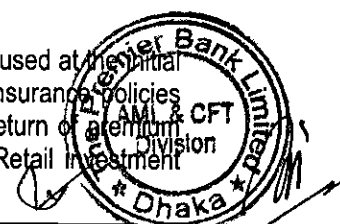
6.10 Some banks and non-banking financial institutions may additionally be susceptible to the attention of the more sophisticated criminal organizations and their "professional money launderers". Such organizations, possibly under the disguise of front companies and nominees, may create large scale but 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 direct 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 effected in favor of a cheque or gold bullion.

7. How PBL 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 PBL family must know the channels concerned for combating money launder.

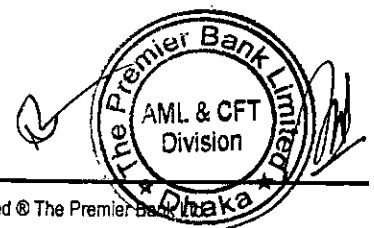
7.1 One of the best methods of preventing deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. **"Know Your Customer"** is the key-policy to know what our customers do, how much their transactions are legitimate, how much not. 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. The Premier 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****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.

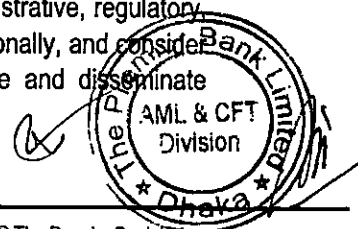
2.1 The Vienna Convention

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; and



- 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, its membership consists of 34 countries and territories and two regional organizations.

3.1 FATF 40+9 Recommendations

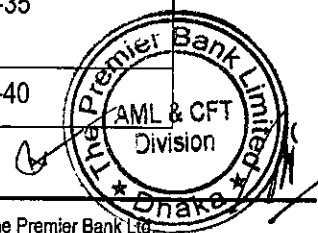
FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. Although not binding as law upon a country, the Forty Recommendations was widely 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 summary of new standards.

Table 1: Summary 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).

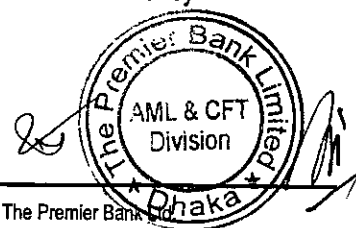
3.5 ICRG (International Co-operation review group)

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.

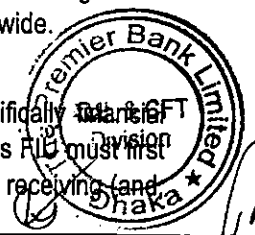
4.3 Customer Due Diligence

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 terrorist 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 40 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.

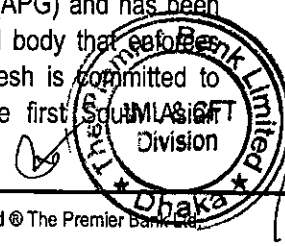
The APG also assists its members to establish coordinated domestic systems for reporting and investigating suspicious transaction reports and to develop effective capacities to investigate and prosecute money laundering and the financing of terrorism offences.

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:

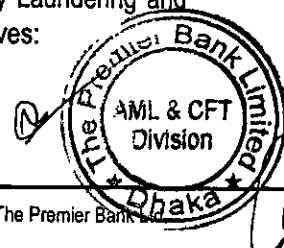
In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and terrorist financing, considering their severe effects on the country. Some important initiatives are shown below:

- 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 sets 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

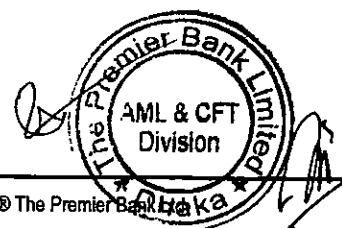


country, promulgated Money Laundering Prevention Act (MLPA), 2002 which came into force on 30 April, 2002. For exercising the power and shouldering the responsibilities, as stated in the MLPA, a separate department named Anti Money Laundering Department (AML) was established at Bangladesh Bank.

- 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 AMLD 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 its pursuit 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**Money Laundering Prevention Act****1. Requirements of the Money Laundering Prevention Acts**

The legislation specifically relating to money laundering is contained in the Money Laundering Prevention Act, 2012 (Act No. 5 of 2012) and Money Laundering Prevention (Amendment) Act, 2015 (Act No. 25 of 2015), the provisions of which supersedes whatever may contain in any other Act in force in Bangladesh.

So far as financial service providers are concerned, the Acts:

- defines the circumstances, which constitute the offence of money laundering [Section 2(Pha)],
- provides penalties for the commencement of the offences [Sections 4, 5, 6, 7, 8 and 27],
- defines the powers and responsibilities of Bangladesh Financial Intelligence Unit (BFIU) for the purpose of prevention of money laundering [Section 23]
- defines the responsibilities of reporting organizations for the purpose of prevention of money laundering [Section 25]

Reporting Organizations have been defined in Section 2(Ba) of the Act as follows:

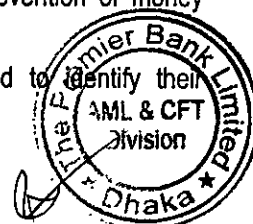
"Reporting Organizations" mean:

- (i) Banks;
- (ii) Financial institutions;
- (iii) Insurers;
- (iv) Money changers;
- (v) Any company or institution that remits or transfers money or monetary value;
- (vi) Any other business institution licensed by Bangladesh Bank;
- (vii) (1) Stock dealer and stock broker,
(2) Portfolio manager and merchant Banker,
(3) Security custodian,
(4) Asset manager;
- (viii) (1) Non-profit organization/institution (NPO),
(2) Non-government organization (NGO),
(3) Cooperative society;
- (ix) Real estate developer;
- (x) Traders of precious metals and stones;
- (xi) Trust and company service providers;
- (xii) Lawyers, Notary, other law professionals and accountants;
- (xiii) Such other institutions as Bangladesh Bank, with approval of the Government, may notify from time to time.

2. Responsibilities of the Reporting Organizations under the MLP Acts

The Act defines the responsibilities of reporting organizations for the purpose of prevention of money laundering in Section 25(1) as follows:

- (i) **KYC Requirement**: To retain complete and accurate information used to identify their customers [Section 25(1)(Ka)];



- (ii) **Record Keeping**: To retain records of the account and transaction of account at least for 5 (Five) years after termination of relationships with the customers [Section 25(1)(Kha)];
- (iii) **Providing Information on Demand**: To provide customer identification, account and account transaction records to Bangladesh Financial Intelligence Unit (BFIU) on demand from time to time [Section 25(1)(Ga)]; and
- (iv) **STR Reporting**: To send a Suspicious Transaction Report (STR) to the Bangladesh Financial Intelligence Unit (BFIU) where they observe any suspicious transaction or attempt for such transaction [Section 25(1)(Gha)].

3. **Penalties for Non-Compliance to the Responsibilities of Reporting Organizations**

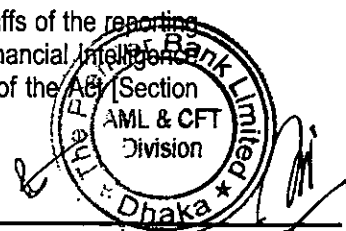
The Acts also provides penalties in Section 25(2) for non-compliance to the above responsibilities of the reporting organizations as follows:

- (i) **Penalty**: If any reporting organization fails to comply with its above-mentioned responsibilities defined under Section 25(1) of the Acts, then Bangladesh Financial Intelligence Unit (BFIU) may impose penalty of minimum Tk. 50 (Fifty) thousand up to maximum Tk. 25 (Twenty Five) lac upon that reporting organization [Section 25(2)(Ka)];
- (ii) **Cancellation of Permission or License**: In addition to the above-mentioned penalty, Bangladesh Financial Intelligence Unit (BFIU) may cancel permission or license of that reporting organization or any of its branch, service center, booth or agent's business, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Section 25(2)(Kha)].

4. **Powers and Responsibilities of BFIU under the MLP Acts**

The Acts give Bangladesh Financial Intelligence Unit (BFIU) broad responsibility for prevention of money laundering and wide-ranging powers to take adequate measures to prevent money laundering, facilitate its detection, monitor its incidence and enforce rules under the Acts. The powers and responsibilities of BFIU are, in summary [Section 23]:

- (i) Analyse cash transaction and suspicious transaction information received from reporting organizations and received information through any other source(s), or collect any additional information from reporting organizations for the purpose of further analysis and maintain database of the same, and where appropriate, provide such information to the concerned law enforcement agency for taking necessary proceedings [Section 23(1)(Ka)].
- (ii) Notwithstanding anything contained in any other Law, collect any information or report from reporting organizations [Section 23(1)(Kha)].
- (iii) Issue an order to any reporting organization to suspend or freeze transactions of an account for a period not exceeding 30 (Thirty) days where there are reasonable grounds to suspect that proceed or property acquired through commencement of a crime have been deposited into that account or proceeds of any account used for the purpose of commencement of a crime or may be used.
Provided that the order so passed for additional periods of 30 (Thirty) days each up to maximum 7 (Seven) times for the purpose of further investigation [Section 23(1)(Ga)].
- (iv) Issue, from time to time, necessary instructions to the reporting organizations for the purpose of prevention of money laundering [Section 23(1)(Gha)].
- (v) Where necessary, carry out on-side inspections of the reporting organizations [Section 23(1)(Uma)].
- (vi) Provide training and arrange meeting, seminar etc. for the officers and staffs of the reporting organizations or any other organizations or institutions as Bangladesh Financial Intelligence Unit may consider appropriate for the purpose of proper implementation of the Act [Section 23(1)(Cha)].



- (vii) Carry out any other functions in attaining the objectives of the Acts including inspection of reporting organization [Section 23(1)(Chha)].

Investigation agency has been defined in Section 2(Tha) of the Act as follows:

"Investigation Agency" means if not differ anything in any section in these acts

- (i) Investigation Agency as empowered by respective act for investigation the 'Predicate Offence' as defined in Section 2(Sha);

Provided that, Criminal Investigation Department of Bangladesh Police shall investigate the predicate offence which is investigable by the Bangladesh Police.

- (ii) Consultation with the government, Bangladesh Financial Intelligence Unit may empower one or more Investigation Agency as mentioned in Section 2(Sha).

5. **Penalties for Non-Compliance to the Directives of BFIU**

The Act also provides penalties in Sections 23(3), 23(4), 23(5), 23(6), 23(7) and 23(8) for failure to provide information on demand, for providing erroneous/false information, or for failure to comply with Bangladesh Financial Intelligence Unit instructions as follows:

- (i) **Failure to Submit Information within Deadline:** If any reporting organization fails to submit within deadline information sought by Bangladesh Financial Intelligence Unit under Section 23(1) of the Act, then Bangladesh Financial Intelligence Unit may impose penalty of Tk. 10 (Ten) thousand per day up to maximum Tk. 5 (Five) lac upon that reporting organization [Section 23(3)]; and

if any reporting organization faces penalty for more than 03 (Three) times in a financial year, then Bangladesh Financial Intelligence Unit may withhold registration or license of that reporting organization or any of its branch, service center, booth or agent's business in Bangladesh, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Section 23(3)].

- (ii) **Submitting Erroneous or False Information or Statement:** If any reporting organization submits erroneous or false information or statement on any subject sought by Bangladesh Financial Intelligence Unit under Section 23(1) of the Acts, then Bangladesh Financial Intelligence Unit may impose penalty of minimum Tk. 20 (Twenty) thousand up to maximum Tk. 5 (Five) lac upon that reporting organization [Section 23(4)]; and

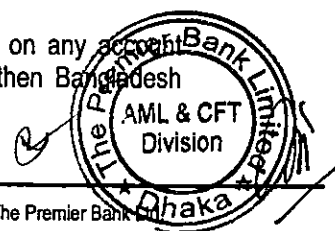
if any reporting organization faces penalty for more than 3 (Three) times in a financial year, then Bangladesh Financial Intelligence Unit may withhold registration or license of that reporting organization or any of its branches, service center, booth or agent's business in Bangladesh, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Section 23(4)].

- (iii) **Failure to Comply with any Instruction of Bangladesh Financial Intelligence:** If any reporting organization fails to comply with any instruction issued by Bangladesh Financial Intelligence under the Act, then Bangladesh Financial Intelligence may impose penalty of Tk. 10 (Ten) thousand per day up to maximum Tk. 5 (Five) lac for each non-compliance issue upon that reporting organization [Section 23(5)]; and

if any reporting organization faces penalty for more than 03 (Three) times in a financial year, then Bangladesh Financial Intelligence may withhold registration or license of that reporting organization or any of its branch, service center, booth or agent's business in Bangladesh, or where appropriate, shall request the registrar or licensing authority to take proper action against such reporting organization [Section 23(5)].

- (iv) **Failure to Comply with Account Freezing or Suspension Order of Bangladesh Financial Intelligence :**

If any reporting organization fails to comply with the freezing or suspension order on any account issued by Bangladesh Financial Intelligence under Clause 23(1)(Ga) of the Acts, then Bangladesh



Financial Intelligence may impose penalty equal to the balance of that account as a minimum, which will not be more than twice of the balance of that account on the order date [Section 23(6)].

- (v) **Realization of Penalty by Bangladesh Bank:** If any person or entity or reporting organization fails to pay the amount of penalty imposed by Bangladesh Financial Intelligence under Sections 23 and 25 of the Acts, then Bangladesh Financial Intelligence inform Bangladesh Bank and Bangladesh Bank may realize the same by debiting the account maintained in the name of that person or entity or reporting organization with any Bank or financial institution or with Bangladesh Financial Intelligence. If any portion of the penalty amount still remains unpaid, then Bangladesh Bank may appear before the Court for realizing the same and the Court shall pass order as it seems appropriate [Section 23(7)].

To investigate and enquiry of the offence described in the Acts, the investigation Agency may collect customer's account documents and information from the Bank or financial institution by the appropriate court order or through Bangladesh Financial Intelligence Unit [Section 23(7) Ka].

- (vi) **Additional Penalty for Responsible Owner(s), Director(s), Employee(s) or Contractual(s):** If any penalty is imposed upon any reporting organization under above-mentioned Sections 23(3), 23(4), 23(5) and 23(6) of the Acts, then Bangladesh Financial Intelligence Unit may impose cash penalty of minimum Tk. 10 (Ten) thousand up to maximum Tk. 5 (Five) lac upon the responsible owner(s), directors(s), employee(s) or contractual employee(s) of that reporting organization, and if necessary, may instruct the reporting organization for necessary disciplinary action [Section 23(8)].

6. Money Laundering Offences

Offence of Money Laundering: The acts of money laundering will be treated as an offence [Section 4(1)].

Offence Committed by an Entity: If any offence under the Acts have been committed by an entity, then every owner, director, manager, secretary or any other employee or representative of that entity who had direct involvement with the offence shall be deemed to be guilty for such offence. However, it is a defense for any person as aforesaid can prove that such offence was committed without his/her knowledge or it has occurred despite his/her best efforts to prevent it [Section 27].

Offence of Violation of Freeze or Attachment Order: It is an offence for any person to violate any freeze or attachment order passed under the Acts [Section 5].

Offence of Disclosure, Publish or Using of Information: It is an offence for a person:

- to disclose any information related to an investigation or any other information to any person, organization or news media for any ill motive [Section 6(1)], or
- to use or disclose information for any purpose other than the purpose of the Acts, which was collected, received, retrieved and known by any person, organization or agent authorized under the Act during the period of his/her employment or appointment period or after completion of his/her employment or appointment contract [Section 6(2)].

Offence of Obstructing or Refusing to Assist an Investigation or Refusing to Submit Reports: It is an offence under the Acts for any person:

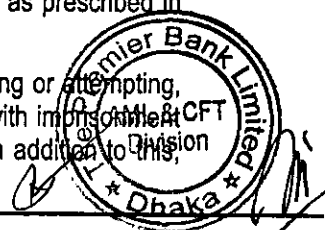
- to obstruct or refuse to assist the investigating officer in an investigation [Section 7(1)(Ka)], or
- to refuse to submit any report or supply information without any reasonable ground [Section 7(1)(Kha)].

Offence of Providing False Information: It is an offence for any person to provide false information knowingly about the sources of funds, or own identity, or the identity of an account holder or about the beneficial owner or nominee of an account [Section 8(1)].

7. Penalties for Money Laundering Offences

All offences under the Acts are cognizable, non-compoundable and non-bailable [Section 11]. All penalties for commencement of the offences have prison terms and/or penalties as prescribed in the Acts as follows:

Penalty for the Offence of Money Laundering: Any person engaged in money laundering or attempting, aiding or conspiring in the commencement of such offence shall be punishable with imprisonment for a term of minimum 4 (Four) years up to maximum 12 (Twelve) years, and in addition to this,



shall be fined with twice the value of the property involved with the offence or Tk. 10 (Ten) lac, whichever is higher [Section 4(2)].

Provided that if failed to payment of financial penalty within stipulated time set by the court, considering unpaid amount of financial penalty, the court may order for additional imprisonment.

In addition to the above, the Court may order to forfeit the property involved directly or indirectly

Penalty for the Offence Committed by an Entity: As per rules under Sub-Section 2 of Section 27, if any entity has committed any offence or try to commit offence, abets or conspires then penalty of twice the value of the property involved with the offence or Tk. 20 (Twenty) lac, whichever is higher may be imposed and registration of that entity shall be liable for cancellation [Section 4(4)].

Provided that if the entity failed to payment of financial penalty within stipulated time set by the court, considering unpaid amount of financial penalty, the court may order for imprisonment to the owner of the entity, chairman or director nevertheless any name.

Penalty for the Offence of Violation of Freeze or Attachment Order: If any person violates a freeze order or an attachment order, then he/she will be punishable with an imprisonment for a term of maximum 3 (Three) years or with a penalty equal to the value of the property under freeze or attachment order, or both [Section 5].

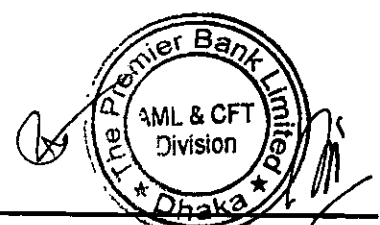
Penalty for the Offence of Disclosure, Publish or Using of Information: If any person discloses any information related to an investigation or any other information to any person, organization or news media for any ill motive, or discloses information for any purpose other than the purpose of the Acts, then he/she will be punishable with an imprisonment for a term of maximum 2 (Two) years or a penalty of maximum Tk. 50 (Fifty) thousand, or both [Section 6(3)].

Penalty for the Offence of Obstructing or Refusing to Assist an Investigation or Refusing to Submit Reports: If any person obstructs or refuses to assist the investigating officer in an investigation, or refuses to submit any report or supply information without any reasonable ground, then he/she will be punishable with an imprisonment for a term of maximum 1 (One) year or a penalty of maximum Tk. 25 (Twenty Five) thousand, or both [Section 7(2)].

Penalty for the Offence of Providing False Information: If any person provides false information knowingly about the sources of funds, or own identity, or the identity of an account holder or about the beneficial owner or nominee of an account, he/she will be punishable with an imprisonment for a term of maximum 3 (Three) year or a penalty of maximum Tk. 50 (Fifty) thousand, or both [Section 8(2)].

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

- 4.8.1 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.
- 4.8.2 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.
- 4.8.3 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.



CHAPTER 4**INSTITUTIONAL POLICY**

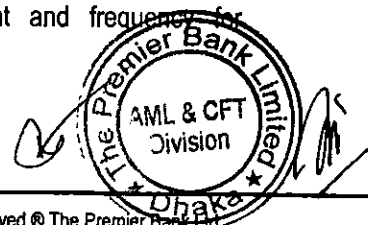
To ensure compliance with the laws and other regulatory requirements and to develop, administer, and maintain bank's own AML policy, this Policy Guidelines has been approved by the board of directors, and noted as such in the board meeting minutes.

The following statements in this Policy Guidelines should be followed as the institutional commitments:

- All employees are required to comply with applicable laws and regulations and corporate ethical standards.
- All activities carried on by the bank must comply with applicable governing laws and regulations.
- Each individual in the bank is responsible to comply the rules and regulations in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations is no excuse for non-compliance.
- Staffs are directed to consult with a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- Employees will be held accountable for carrying out their compliance responsibilities.

In order to protect Bank's reputation and to meet its legal and regulatory obligations , it is essential that Bank should minimize the risk of being used by Money Launderers. With that view it will be an obligatory responsibility for all Bank official, customer and management of the Bank to realize and combat the situation on this critical risk issues. Considering all these bank will ensure the following issues as the institutional policy:

- a) Establish clear lines of internal accountability, responsibility and reporting. Primary responsibility for the prevention of money laundering rest with the nature of business which must ensure that appropriate control are in place and operating effectively and bank officers are adequately trained.
- b) Given its importance in reputation and regulatory terms, the effectiveness of the money laundering prevention regime across all business should form part of the governance oversight responsibilities of all Branch Compliance officer.
- c) Document , implement and maintain, procedures and controls which interest bank's policy and Bank's standard for each business in the context of applicable laws and regulations and corporate ethical standards. Compliance with such procedures and controls and with Bank policy and Bank standards will be effectively monitored.
- d) Establish an effective 'Know your customer' policy for the Branch which will contain a clear statement of management's overall expectation matching with local regulations and establishing specific line of responsibilities. Detail guideline on know your customer(KYC) are given of this guidelines.
- e) Cooperate with any lawful request for information made by government agencies during their investigation in to money laundering support government, law enforcing agencies and Bangladesh Bank in their efforts to combat the use of the financial system for the laundering of the proceeds of crime or the movement of fund for financial purposes.
- f) Report money laundering issue to AMLD, Head office on a regular basis. The BAMLCO is responsible to combat money laundering shall determine and communicate the content and frequency for management reporting.



CHAPTER 5**REQUIREMENTS OF ANTI MONEY LAUNDERING POLICY****1. Senior Management Commitment**

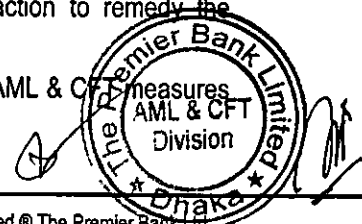
The most important element of a successful anti-money laundering program is the commitment of Senior Management. Senior Management of PBL is highly committed to the development and enforcement of the Anti Money Laundering, Anti Terrorist Financing and Proliferation Financing objectives which can deter 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. For the purpose of this policy, Senior Management means the Managing Director & CEO and the Board of Directors of the Bank.

2. Board of Directors shall (Role of Senior Management):

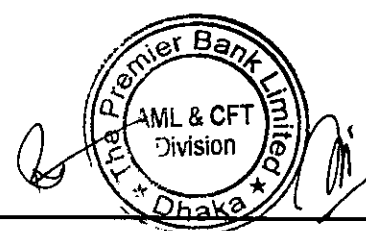
- Approve AML & CFT compliance program and ensure its implementation;
- Issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- Take reasonable measures through analyzing self assessment report and independent testing report summary;
- Understand ML & 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.

3. 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. 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.

5. 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.**6. 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.****7. Senior Management should adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the Bank.**

8. 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.
9. **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.
 - The Board of Directors shall develop, administer, and maintain an Anti Money Laundering Policy that ensures and monitors compliance with Anti Money Laundering legislation, including record keeping and reporting requirements. Such a compliance policy shall be written, approved by the Board of Directors, and noted as such in the Board meeting minutes.
 - The written Anti Money Laundering Policy at a minimum should establish clear responsibilities and accountabilities within the Bank to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using the Bank for money laundering and the financing of terrorist activities, thus ensuring that we comply with our obligations under the legislation.
 - In addition, the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and should set forth the consequence of non-compliance with the applicable laws and the institution's policy including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any Bank with money laundering and terrorist financing activity.



CHAPTER 6**ORGANIZATIONAL STRUCTURE AND H.R. INITIATIVES****6.1 Central Compliance Committee (CCC)**

- 6.1.1 Central Compliance Committee (CCC) is a cross departmental committee to facilitate the Anti-Money Laundering initiatives of the Bank. The Committee shall be formed under the leadership of an Executive who will be called as "Chief Anti Money Laundering Compliance Officer (CAMLCO)" and it shall report directly to the Managing Director of the Bank. The Bank shall designate an Executive in the rank of maximum two grades below the Managing Director & CEO as its CAMLCO². CCC will consist of atleast 7 members where the CAMLCO & D-CAMLCO and the Heads/ Executives of different divisions (i.e. HRD, Credit Division, Retail & Corporate Banking Division, FED, OPD, Card Division, ITD etc.) will be the member of the said committee. However no official from ICCD can be a member of the said committee.³

CCC will arrange at least 4 meetings yearly where, by reviewing the overall status of the Bank regarding AML & CFT issues, necessary decisions shall be made and necessary instruction shall be given by the committee.⁴

6.2 Formation of CCC

- 6.2.1 CCC (previously named CCU Committee) was first formed in July 16, 2015 with officials from concerned departments/divisions of Head Office which has been restructured upon the instructions given in the latest BFIU Master Circular (Circular No. 19) and formed a new committee with more members and better involvement of other departments/divisions of the Bank. The new committee consists of sixteen (16) senior members from different departments/divisions (AML Division, Retail Banking Division, Credit Risk Management Division, Corporate Banking Division, SME Division, International Division, Finance & Accounts Division, IT Division, HR Division, Operations Division, Remittance Division) to ensure proper involvement of those in complying with AML&CFT issues.

6.3 Responsibilities of CCC

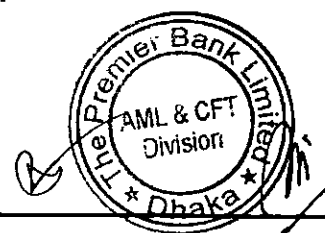
- 6.3.1 The committee shall have the following responsibilities:

- 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.

² Ref.: Section 1.3.1 Ka of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).

³ Ref.: Section 1.3.1 Cha of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).

⁴ Ref.: Section 1.3.1 Chha of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).



- 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.

6.4 Anti-Money Laundering Division (AML)

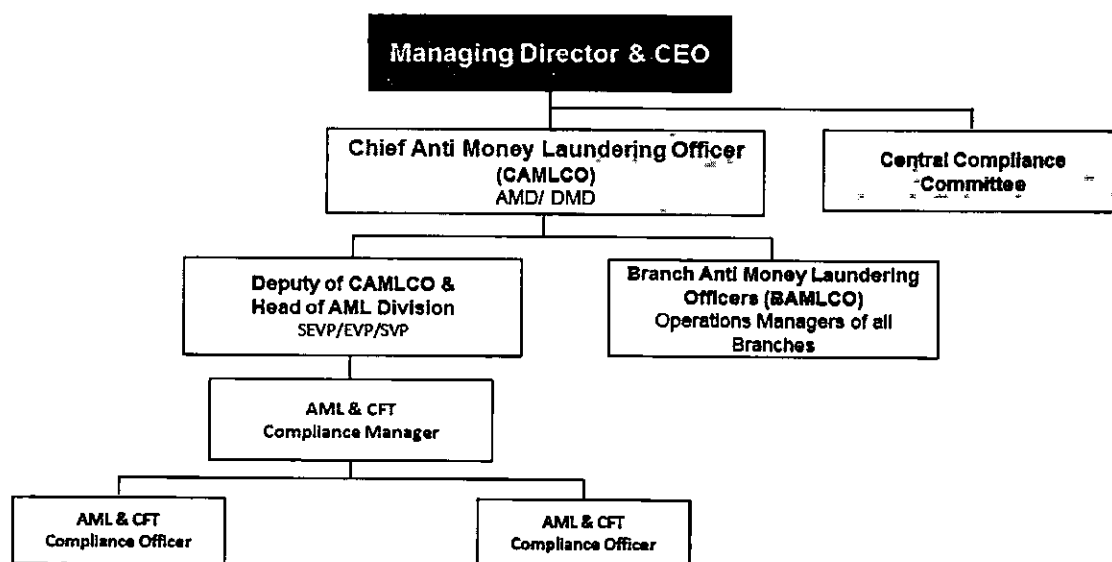
- 6.4.1 The Bank shall constitute an Anti-Money Laundering Division at its Head Office.
- 6.4.2 The Bank shall appoint Chief Anti Money Laundering Compliance Officer (CAMLCO).
- 6.4.3 The Bank shall appoint Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO) & Head of AML Division.
- 6.4.4 The Bank shall appoint Branch Anti Money Laundering Compliance Officer (BAMLCO).

6.5 Formation of Anti-Money Laundering Division

- 6.5.1 The Bank shall constitute an Anti-Money Laundering Division at its Head Office or any suitable place as a permanent set-up with specific organogram like other department or division of a Bank. AMLD shall implement and enforce corporate-wide Anti Money Laundering Policies, Procedures and Measures to the Bank and will report directly to the Managing Director & CEO through the CAMLCO.

6.6 The Premier Bank Ltd. Anti-Money Laundering Division (AML) Organogram Chart

- 6.6.1 The Premier Bank Ltd. has already been established a separate Anti-Money Laundering Division at its Head Office. Organogram of the AMLD of The Premier Bank is given below:



6.7 Manpower for Anti-Money Laundering Division

- 6.7.1 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 AMLD must have enough knowledge on AML & CFT measures of Bangladesh including MLPA, ATA and rules and instructions issued by BFIU or Bangladesh Bank.

6.8 Separation of AMLD from Internal Control & Compliance (ICC)

- 6.8.1 To ensure the independent audit function in the Bank AMLD should be completely separated from internal audit or compliance and control (ICC). In this regard ICC also examines the performance of AMLD and the Bank's AML & CFT compliance program. To ensure this autonomy there shall not be any member from ICC to AMLD and vice-a-vice; but there should be enough co-ordination and co-operation in performing their responsibility and information exchange. There should not be any

impediment to transfer employee from ICC to AMLD and vis-à-vis but no one should be posted in these 2 (two) departments/units at the same time. Also no official from ICCD can be a member of the CCC. Both AMLD and ICCD will independently perform their respective jobs regarding AML & CFT issues.⁵

6.9 Responsibilities of AMLD

6.9.1 AMLD is the prime mover of the Bank for ensuring the compliance of AML & CFT measures. Main responsibilities of AMLD are to:

- develop Banks policy, procedure and strategies in preventing ML, TF & PF;
- coordinate Banks AML & CFT compliance initiatives;
- coordinate the ML & TF Risk Assessment of the Bank and review thereon;
- present the compliance status with recommendations before the CEO or MD on half yearly basis;
- forward STR/SAR and CTR to BFIU in time and in proper manner;
- report summary of Self Assessment and Independent Testing Procedure to BFIU in time and in proper manner;
- impart training, workshop, seminar related to AML & CFT for the employee of the Bank;
- take required measures to submit information, report or documents in time.
- ensure the implementation of the AML & CFT program on Yearly Basis.⁶

6.10 Authorities of AMLD

6.10.1 To perform the responsibilities, the AMLD has the following authorities:

- assign BAMLCO their specific job responsibilities;
- appointment of BAMLCO and assign their specific job responsibilities;
- requisition of human resources and logistic supports for AMLD;
- make suggestion or administrative sanction for non-compliance by the employees.

6.11 Chief Anti Money Laundering Compliance Officer (CAMLCO)

6.11.1 The Bank shall designate an Executive in the rank of maximum two grades below the Managing Director & CEO⁷ as its Chief Anti Money Laundering Compliance Officer (CAMLCO). If the CAMLCO is changed, it should be informed to BFIU without delay. Before assigning the CAMLCO to other duties of the Bank, the management has to ensure that the AML & CFT activities of the Bank will not be hampered.

6.11.2 The Premier Bank Ltd. has designated a Chief Anti Money Laundering Compliance Officer (CAMLCO) at Head Office with sufficient authority to implement and enforce corporate wide AML & CFT policies, procedures and measures and who is reporting to MD & CEO.

6.11.3 CAMLCO is the Central Point of Contact (CPC) for communicating with the regulatory agencies regarding the Bank's Anti Money Laundering programs. All staff engaged in the Bank at all levels must be made aware of the identity of the CAMLCO.

6.11.4 CAMLCO is the chairman of the Central Compliance Committee (CCC). The committee shall look after the overall compliance of AML & CFT under the supervision of the CAMLCO.

6.12 Authorities and Responsibilities of CAMLCO

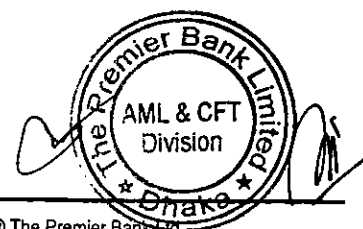
6.12.1 The CAMLCO has the following Authorities:

- CAMLCO is able to act on his own Authority;

⁵ Ref.: Section 1.3.1 Cha of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).

⁶ Ref.: Section 1.3.1 Ga of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).

⁷ Ref.: Section 1.3.1 Ka of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).



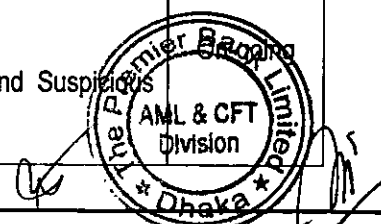
- Without taking any prior permission from /with MD or CEO , CAMLCO can submit of STR/SAR and any document or information to BFIU;
- He/She shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He/She must have access to any information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

6.12.2 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.

6.12.3 **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 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,	



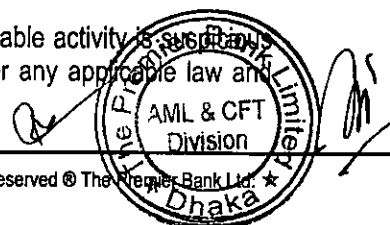
- are accompanied by documentation of the branch's decision to retain or terminate the account as required under the Policy, - are advised to other branches of the Bank who are known to have a relationship with the customer, - are reported to the Managing Director & CEO and/or the Board of Directors 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.	
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, Bi-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 & Correspondant Relatiolshion Banking Department at Head Office.	On-going
16. Prepare/Complete KYC Questionnaires of PBL for correspondents.	As required
17. Arrange AML 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

6.12.4 The Chief Anti Money Laundering Compliance Officer (CAMLCO) should **possess**:

- Proven leadership and organizational skills and ability to exert managerial control.
- Excellent communication skills, with an ability to clearly and diplomatically articulate issues, solutions and rationale; an effective trainer to raise the level of awareness of the control and compliance culture.
- Solid understanding of AML and ATF regulatory issues and product knowledge associated with a broad range of relevant financial services, Banking activities.
- High degree of judgment, good problem solving skills and be results oriented to ensure sound implementation of control and compliance processes and procedures.
- High personal standard of ethics, integrity and commitment to fulfilling the objectives of the position and protecting the interest of the Bank.

6.12.5 The Chief Anti Money Laundering Compliance Officer (CAMLCO):

- Must be familiar with the ways in which any of the Bank's products and services may be abused by money launderers.
- Must be able to assist the Bank to develop effective AML and ATF policies, including programs to provide AML and ATF training to all personnel.
- Must be able to assist the Bank to assess the ways in which products under development may be abused by money launderers in order to establish appropriate AML and ATF controls before any product is rolled out into the marketplace.
- Must be capable of assisting the Bank to evaluate whether questionable activity is suspicious under the standard set forth in the AML and ATF Policy and under any applicable law and regulation.



6.13 Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)

- 6.13.1 The Bank shall nominate one executive in the rank of Senior Vice President and above⁸ as Deputy CAMLCO.
- 6.13.2 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.
- 6.13.3 The Deputy CAMLCO shall be the Head of Anti Money Laundering Division and will report directly to the CAMLCO.

6.14 Branch Level Organization Structure

- 6.14.1 For the implementation of all existing acts, rules, BFIU's instructions and Bank's own policies on preventing Money Laundering & Terrorist Financing, CCC shall nominate an experienced Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch.
- 6.14.2 Branch Manager, Branch Operations Manager (the second man) 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.

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

- 6.15.1 The Branch Manager/ Branch Operations Manager/GB Incharge/ Credit Incharge/any 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 regarding all AML & ATF matters. Branch Manager shall have overall supervision ensuring that the AML & CTF 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.
- 6.15.2 **Branch Anti Money Laundering Compliance Committee (BAMLCC)**: Every branch shall create a Branch Anti Money Laundering Compliance Committee (BAMLCC) consisting at least with the following members:
1. Branch Manager/Head of Branch
 2. Branch Operations Manager
 3. General Banking In charge
 4. Credit In charge
 5. Foreign Exchange In charge
 6. Cash In Charge (Teller)
- 6.15.3 The BAMLCO shall arrange quarterly meetings with Branch Anti Money Laundering Compliance Committee (BAMLCC) to review the Anti-Money Laundering compliance status 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,
 - Identifying and reporting of Suspicious Transactions,

⁸ Ref.: Section 1.3.1 Kha of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).



- Implementation of Local Sanction List along with the resolutions of UN Sanctions Security Council,
- Self- Assessment Related activities,
- Record keeping,
- Training.

6.15.4 The BAMLCO shall maintain minutes of the meeting in documented form and shall send a copy of the minutes to AML Division. A copy of the minutes should be forwarded to the CAMLCO along with Self Assessment Report at Head Office for their information & records.

6.16 Individual Responsibilities (Branch Officials)

6.16.1 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:

6.16.2 Branch Manager (BM):

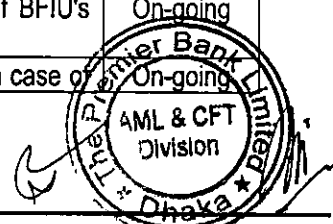
Key Responsibilities of the BM	Frequency
1. Owner of the business & compliance for the branch. Main objective is to achieve numbers towards enhancement of Bank's profit in strict compliance with applicable AML and ATF laws, regulations and policies.	On-going
2. Ensure that the AML and ATF program are 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 compliance of the branch by internal auditors as well as Bangladesh Bank inspectors.	On-going
7. <u>Job Rotation</u> : 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 ⁹ .	On-going
8. <u>Leave Management</u> : 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 ¹⁰ .	On-going

6.16.3 Branch Anti Money Laundering Compliance Officer (BAMLCO):

Key Responsibilities of the BAMLCO/CSM	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 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	On-going

⁹ Ref.: Letter no. MLPD (Special)267/2004-3918-3966 dated 19-10-2004 of Anti-Money Laundering Department of Bangladesh Bank.

¹⁰ Ref.: Letter no. MLPD (Special)267/2004-3918-3966 dated 19-10-2004 of Anti-Money Laundering Department of Bangladesh Bank.



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).	
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.	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 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 AMLD, HR and Learning & Talent Development Center.	As required
14. Ensure all the required information and document are submitted properly to AMLD and any freeze order or stop payment order are implemented properly.	As required
15. Submit branch returns including CTR, KYC Exception Report, Central Taskforce Biorony, etc. to the AMLD as per specific schedule.	Monthly, Bi-Monthly & Half Yearly
16. Communicate the updated policies including AML and ATF 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: <u>During Audit (Internal or External)/Inspection (Bangladesh Bank):</u> 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. <u>After Receiving the Audit/Inspection Report:</u> 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. <u>Continuous Monitoring about the progress of Compliance to the Report:</u> In case of any deviation, inform Branch Manager or related Head of Division immediately. <u>Compliance of All Parts and Send to AMLD within Stipulated Time Frame:</u> The response should be vetted by respective BAMLCO and Branch Manager.	Adhoc

6.17 Internal Control & Compliance Division:

- 6.17.1 Internal Audit or Internal Control and Compliance (ICC) shall have an important role for ensuring proper implementation of Bank's AML & CFT Compliance Program. The Bank shall ensure that ICC is equipped with enough manpower and autonomy to look after the prevention of

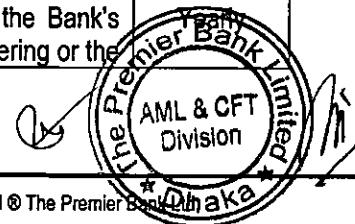


ICC has to oversee the implementation of the AML & CFT compliance program of the Bank and has to review the 'Self Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

The Internal Audit Officials must:	Frequency
1. understand ML & TF 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 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;	On-going
8. communicate the findings to the board and/or senior management in a timely manner;	On-going
9. recommend corrective action to address the identified deficiencies;	On-going
10. track previously identified deficiencies and ensures correction made by the concerned person;	On-going
11. examine that corrective actions have taken on deficiency identified by the BFIU or BB;	On-going
12. assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;	On-going
13. determine when assessing the training program and materials: a. the importance of the Board and the Senior Management's place on ongoing education, training and compliance b. the employee accountability for ensuring AML & CFT compliance c. comprehensiveness of training, in view of specific risks of individual business lines, d. training of personnel from all applicable areas of the Bank, e. frequency of training, f. coverage of Bank policies, procedures, processes and new rules and regulations, g. coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity, h. penalties for noncompliance and regulatory requirements.	On-going
14. Review of control procedures in the Bank to ensure legal and regulatory compliance and in the development of adequate and sufficient Independent Testing Procedures (ITP) to prevent and detect compliance lapses.	On-going
15. Perform AML Risk Assessment for the Business.	On-going
16. Perform periodic Quality Assurance on the AML program in the branches/divisions.	On-going

6.18 Managing Director & CEO:

Key Responsibilities of the MD & CEO	Frequency
1. Overall responsibility to ensure that the Bank has an AML and ATF 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	Yearly



funding of terrorist or criminal activities. If necessary, MD & CEO will also monitor the overall status of the compliance issue. ¹¹	
---	--

6.19 Initiatives by Human Resources Division

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

- Revised Code of Conduct & Ethics for the employees of The Premier 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 extraordinary preventive action vis a vis 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.

6.19.2 **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 The Premier Bank does not face any money laundering risk by any of its staffs¹²

6.19.3 **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.

6.20 Training and Awareness

6.20.1 **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.

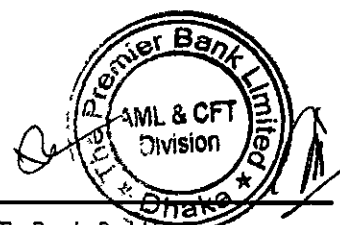
6.20.2 **Awareness for Senior Management, Customer & Mass People:** For effective implementation of AML & CFT measures in the Bank, Bank shall arrange awareness program for Senior Management, Customer and for Mass people. Details describe in Chapter 20.13 & 20.14 of this policy.

6.20.3 **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.

6.20.4 **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 leave at a time each year as mandatory leave.

¹¹ Ref.: Section 1.2. Kha of BFIU Circular No.-19/2017 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).

¹² Ref.: Para 11.1 of BFIU Circular No. 19 dated 17-09-2017 of Bangladesh Financial Intelligence Unit (BFIU)



CHAPTER 7**CUSTOMER DUE DILIGENCE****1. KNOW YOUR CUSTOMER PROGRAM**

The adoption of effective Know Your Customer (KYC) program is an essential part of banks risk management policies. Having sufficiently verified/corrected information about customers - "Knowing Your Customer" (KYC) - and making use of that information underpins all AML/CFT efforts, and is the most effective defense against being used to launder the proceeds of crime.

Bank with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the bank's overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

2. KNOW YOUR CUSTOMER (KYC) PROCEDURE

Money Laundering Prevention Act 2012 requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. FATF recommendation 10 states that where the financial institution is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner and unable to obtaining information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

Nature of Customer's Business

When a business relationship is being established, the nature of the business that the customer expects to conduct with the bank should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. In order to judge whether a transaction is or is not suspicious, bank need to have a clear understanding of the business carried on by its customers.

Identifying Real Person

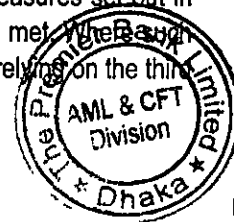
Bank must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally. This will safeguard against opening of fictitious account.

Document is not enough

The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that bank must know who its customers are, and have the necessary documentary evidence to verify this. Collection of document is not enough for KYC, identification is very important.

Reliance on Third party

Countries may permit financial institutions to rely on third parties to perform the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the bank relying on the third party.



The criteria that should be met are as follows:

- (a) A bank relying upon a third party should immediately obtain the necessary information.
- (b) Banks should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- (c) The bank should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements.

3. CUSTOMER PROFILING:

Followings are required:

1. Obtaining and document the customer's basic background information.
2. Try to use the information to evaluate the appropriateness of the customer's transaction activity.
3. Determine the customer's source of fund.

KYC profile should disclose:

- The customer expected transaction trend
- The source of wealth
- Net worth

KYC profile should be upgraded/ updated by:

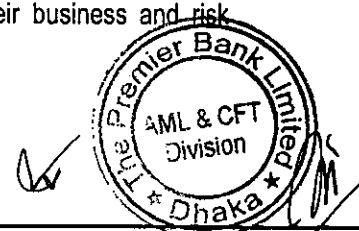
1. Regular review of transaction activity and balance fluctuation report
2. Newspaper and Magazine article, financial statement, brochures, industry activities relating to the customer.
3. Periodical discussion with the client relating to their business activities including future plan of the business for the next 12 month.

Customer Due Diligence (CDD):

As per FATF new standards Banks requires various Customer Due Diligence measures:

Normal CDD measures :

- A) Identifying the customer and verifying that customer identity using reliable, independent source documents, data of information
- B) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such as that the bank is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include banks understanding the ownership and control structure of the customer.
- C) Understanding and as appropriate, obtaining information on the purpose and intended nature of the business relationship,
- D) Conducting on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transaction being conducted are consistent with the bank's knowledge of the customer, their business and risk profile, including where necessary the source of funds.



Enhanced Customer Due Diligence

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

CDD measures that could be applied for higher Risk business relationship include :

- 1) Obtaining additional information on the customer (occupation, volume of assets, information available through public data base and internet etc. and updating more the identification data of customer and beneficial owner.
- 2) Obtaining additional information on the intended nature of the business relationship.
- 3) Obtaining information on the source of wealth of the customer.
- 4) Obtaining information on the reasons for intended or performed transaction
- 5) Obtaining the approval of senior management to commence or continue the business relationship
- 6) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination
- 7) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified Customer Due diligence :

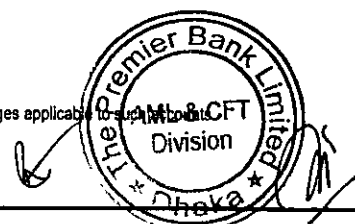
Where the risk of money laundering or terrorist financing are lower, bank could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors. Example of possible measures are :

- Verify the identity of the customer and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of customer identification update.
- Reducing the degree of on-going monitoring and scrutinizing transactions based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD shall be done for low risk accounts like Student Accounts, Farmer's Accounts and other No-Frill accounts^{13,14}. However, Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher risk scenarios apply.

¹³ 'No Frills' account is a basic banking account. Such account requires either nil minimum balance or very low minimum balance. Charges applicable to such account are low. Services available to such account is limited.

¹⁴ Ref.: Section 3.4.Ga of BFIU Circular No.19 dated 17-09-2017 of Bangladesh Financial Intelligence Unit



4. COMPONENTS OF KYC PROGRAM

Bank is in the process of designing the KYC program and has included certain key elements. Such essential elements have been started from the bank's risk management and control procedures and included -

- (1) Customer acceptance policy,
- (2) Customer identification,
- (3) On-going monitoring of high risk accounts, and
- (4) Identification of suspicious transactions.

Bank should not only establish the identity of its customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of bank's risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programs beyond these essential elements should be tailored to the degree of risk.

Who is a Customer?

For the purpose of KYC Procedure a "Customer" is defined in AML Circular No. 19 dated 17/09/2017, as:

- Any individual or entity that maintains an account of any type with a Bank or financial institution or have Banking related business.
- Any third party, either individual or entity, on whose behalf the account is operated (**Beneficial Owner¹⁵**) directly or indirectly.
- A professional intermediary (such as lawyer/law firm, chartered accountant etc.) appointed for operating an account of Account holder, Trust or the Beneficial Owner under the existing legal infrastructure.
- Any individual or entity involved with High value single Occasional Transaction or any monetary transaction that may create any risks including the reputational risks of the Bank. In this case if a transaction appears abnormal in relation to the usual transaction considering the business/profession/profile of the concerned individual or entity that transaction will be treated as "high value".
- Any individual or entity defined by BFIU time to time.

Customer Acceptance Policy

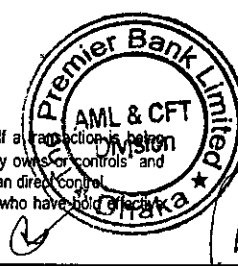
Bangladesh Bank has recommended in the Guidance Notes on Prevention on Money Laundering to develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers including a description of the types of customer that are likely to pose a higher than average risk to a financial institution. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures (if considered high risk) or politically exposed persons should be taken exclusively at senior management level.

The guidelines for Customer Acceptance policy for the Bank are as follows:

- No account can be opened in anonymous or fictitious name.

¹⁵ Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/ control is exercised through a chain of ownership or by means of control other than direct control. Note: It is required to conduct CDD of settlor, trustee, protector or any person with similar status or any beneficiary or class of beneficiaries who have hold effective control on trust, in case of identification of beneficial ownership of a legal arrangement.

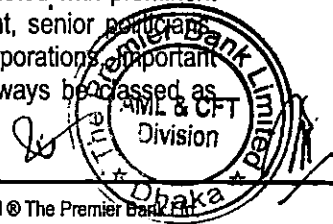


- Parameters of risk perception are clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grade.
- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.
- Not to open an account or close an account where the 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 customer or non reliability of the data/information furnished to the bank. Decision by the bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
- Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.
- Necessary checks before opening a new account 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 terrorists or terrorist organizations etc.
- The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.
- No account should be opened in the name of listed in UN Sanction lists, OFAC Sanction lists and directed by Bangladesh Bank or any other sanction lists.
- No account should 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 risk grading.
- No account should be opened for those customers 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
- No account should be opened for that customer for whom the collection of information for assessing their overall profile is impossible.
- No account should be opened for that 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.
- No account should be opened for that customer failing to provide all information required for the identification and verification of their identity.

Politically Exposed persons (PEPS) :

Bank shall assess and determine their all clients whether they are **PEP's or Influential Persons or Chief Executives or Top Level Officials of any International Organization and their Linked Entities or their Close Family Members and Close Associates**. These customers usually 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 (PEP's, Influential Persons and chief executives or top level officials of any international organization) itself does not incriminate individuals or entities. It does, however, put a prospective or existing Client into a higher risk category.

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 assessed 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.

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:

- i. establishes a business relationship
- ii. carries out an occasional transaction
- iii. Suspect money laundering or terrorist financing or
- iv. Doubt the veracity of documents, data or information previously obtained for the purpose of identification or verification.

Shell Bank: Bank will not establish correspondent relationship with Shell Bank (defined later) and the bank is maintaining relationship with 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.

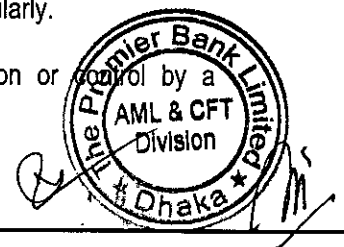
Beneficiaries should be identified when they are defined. In the case of a "Foundation", Branches should take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification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

Correspondent Banking relationship: Bank can maintain correspondent Banking relationship 1) following the terms and condition as laid down in AML circular no.24 issued dated March 03, 2012 (detailed mentioned later)

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.

NGO, NPO, Club, society, charitable organization: Bank can open the account in the mentioned name. All information in line AML policy to be fulfilled and transaction should be monitored regularly.

Account of customer providing financial or insurance services without authorisation or control by a supervisory authority.



Account in the name of Business organization: Necessary legal document to be obtained in support of the company. Personal information of all the Director's and signatories is required. If any beneficial owner is detected, full information should be obtained.

For the purpose of risk categorisation of customer, the relevant information shall be obtained from the customer at the time of account opening. Risk perception of different types of customers taking into account the back ground of the customer, nature of business activity, location of customer, activity and profile of his/her clients, country of origin, source of fund, social and financial status etc. shall be decided based on the relevant information provided by the customer.

Customer shall be accepted after verifying their identity as laid down in customer identification procedures. Documentation requirements and other information shall be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of AML Act, 2012 and instruction/ guidelines issued by BFIU, Bangladesh Bank from time to time.

The Branches will follow the identification procedures for their customers where locker service facilities exist. No locker should be opened without maintaining account properly.

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.

The customer address should be verified as per AML policy as well as PBL policy.

Classify customers into various risk categories and based on risk perception, apply the acceptance criteria for each category of customers. Also a profile of each customer will be prepared based on risk categories.

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. Customer Identification

Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for bank to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if the bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

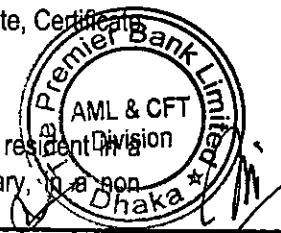
Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained.

6. What Constitutes a Customer's Identity

Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, corporate body, partnership, etc). For the purposes of this guidance, the two elements are:

- a) the physical identity (e.g. Birth Certificate, TIN/VAT Registration, Registration Certificate, Certificate of Incorporation, Passport/National ID/ Smart ID etc.); and
- b) the activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary.



money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issuance should be recorded.

The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the bank's own understanding of the applicant's business.

Once account relationship has been established, reasonable steps should be taken by the bank to ensure that descriptive information is kept up to date as opportunities arise. It is important to emphasize that the customer identification process does not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

7. Individual Customers

Bank shall obtain following information while opening accounts or establishing other relationships with individual customers:

- Correct name and/or names used;
- parent's names;
- Spouse Name
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income
- Contact information, such as – mobile/telephone no.

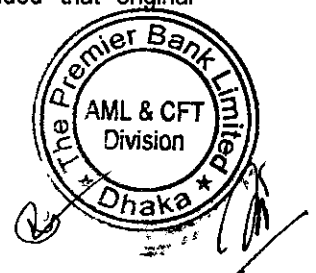
The original, certified copy of the following Photo ID also play vital role to identify the customer:

- (i) Current valid passport;
- (ii) National ID/ Smart ID Card;
- (iii) Birth Certificate along with any other Photo ID (Driving License, Employee ID etc.), bearing the photograph and signature of the applicant;

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, certificate from any local government organs, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which the bank is unfamiliar, either because of origin, format or language, the bank must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. Bank should also be aware of the authenticity of passports.

One or more of the following steps may be followed to verify addresses:

- provision of a recent utility bill, tax assessment or bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- checking the Voter lists;
- checking the telephone directory;
- visiting home/office;
- sending thanks letter.



The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

7.1 Non face-to-face contact: Where there is no face-to-face contact, photographic identification would clearly be inappropriate procedures to identify and authenticate the customer. Bank should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation or disguise. In the event that internal procedures require sight of a current passport or ID card where there is no face-to-face contact, then a certified true copy should be obtained. Bank should not allow non face to face contact to a resident in establishing relationship.

7.2 Genuineness of documents: There is obviously a wide range of documents which might be provided as evidence of identity. It is important for the bank to decide the genuineness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

7.3 Joint Accounts: In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should normally be verified in accordance with the procedures set out above.

7.4 Change in address or other details: Any subsequent change to the customer's name, address, or employment details of which the bank becomes aware should be recorded as part of the Know Your Customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

7.5 Record keeping: All documents collected or gathered for establishing relationship must be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file. If the bank regularly conducts one-off transactions, should record the details in a manner which allows cross reference to transaction records.

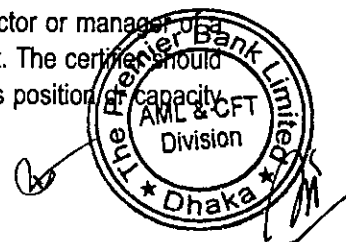
8. Introducer:

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.

9. Persons without Standard Identification Documentation

It is generally believed that financial inclusion is helpful in preventing money laundering and terrorist financing. Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should 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 and some flexibility without compromising sufficiently rigorous AML procedures is accepted. Internal procedures allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances. 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 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.

10. 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.

11. Corporate Bodies and other Entities

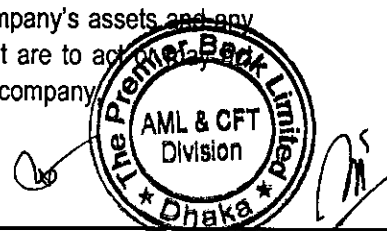
Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be 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, 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.

12. 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.

13. Partnerships and Unincorporated Businesses

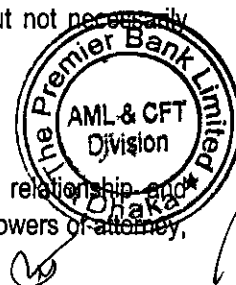
In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the bank, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership 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.

14. 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.

15. 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 should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority.

This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing.

Verification, once begun, should 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.

16. Risk categorization – Based on Activity / KYC Profile

When opening accounts, the concerned officer must assess the risk that the accounts could be used for "money laundering", and must classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form given in Annexure D in which following seven risk categories are scored using a scale of 1 to 5 where scale 4-5 denotes High Risk, 3- Medium Risk and 1-2 Low Risk:

- Occupation or nature of customer's business
- Net worth/monthly income of the customer
- Mode of opening the account
- Expected value of monthly transactions
- Expected number of monthly transactions
- Expected value of monthly cash transactions
- Expected number of monthly cash transactions
- Product & Services type
- Nationality
- Customer Contact details

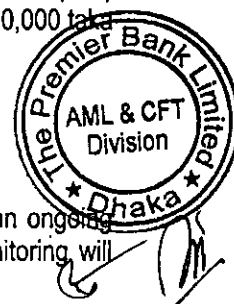
KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for "High Risk" accounts (as defined above). For "Low Risk" transactional accounts KYC Profiles and Transaction Profiles must be updated and re-approved in every five (5) years. These should, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern. Bank shall also update any account when deemed necessary.

If a person deposits or withdraws money from an account which is maintained with other branch through online banking, the branch must obtain KYC of depositors/ withdrawer as per format provided & preserve record one copy in a file & another with the voucher.

Customer other than account Holder (Walk in/ one off): For walk in customer transacting 50,000 taka or below, only name, address & tel. no. should be kept of applicant or beneficiary. For walk in customer transacting above 50,000 taka or below 5, 00,000 taka, along with name, address & tel no., Photo ID (PID) should also be kept. CDD should be performed for Walk-in Customers transacting amount of 5, 00,000 taka or more as Occasional Transaction.

17. Transaction Monitoring Process

17.1 Financial Institutions are expected to 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 Financial Institutions 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

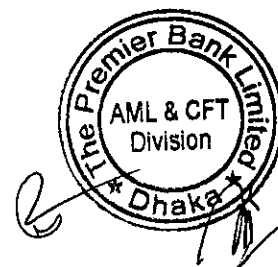
17.2 It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. To effective monitoring of account transaction AML software was introduced and branch has to monitor the transaction by the system.

17.3 Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be declared in a Transaction Profile (TP) at the time of opening account from the customer. Ideally any deviation from the normally expected TP should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account.

17.4 It may not be feasible for some institutions or specific branches of institutions 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.

17.5 On a monthly basis Branch/ concerned unit of the financial institution must prepare an exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer based on Anti-Money Laundering risk assessment exercise.

17.6 Account Officers/Relationship Managers or other designated officer will review and sign-off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer. The concerned officer will document their review by initial on the report, and where necessary will prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the relevant Branch Manager and review with the BAMLCO. A copy of the transaction identified will be attached to the SARs.



CHAPTER 8**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.

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 seems 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.

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 Circulars issued by Bangladesh Bank time to time.

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.

4. IDENTIFICATION AND EVALUATION STR/SAR

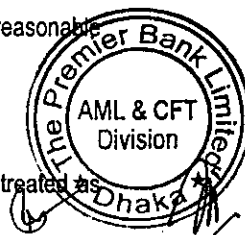
Identification of STR/SAR is very crucial for banks to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place by the banks. Such suspicion may not only at the time of transaction but also at the time of doing KYC and attempt to transaction.

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

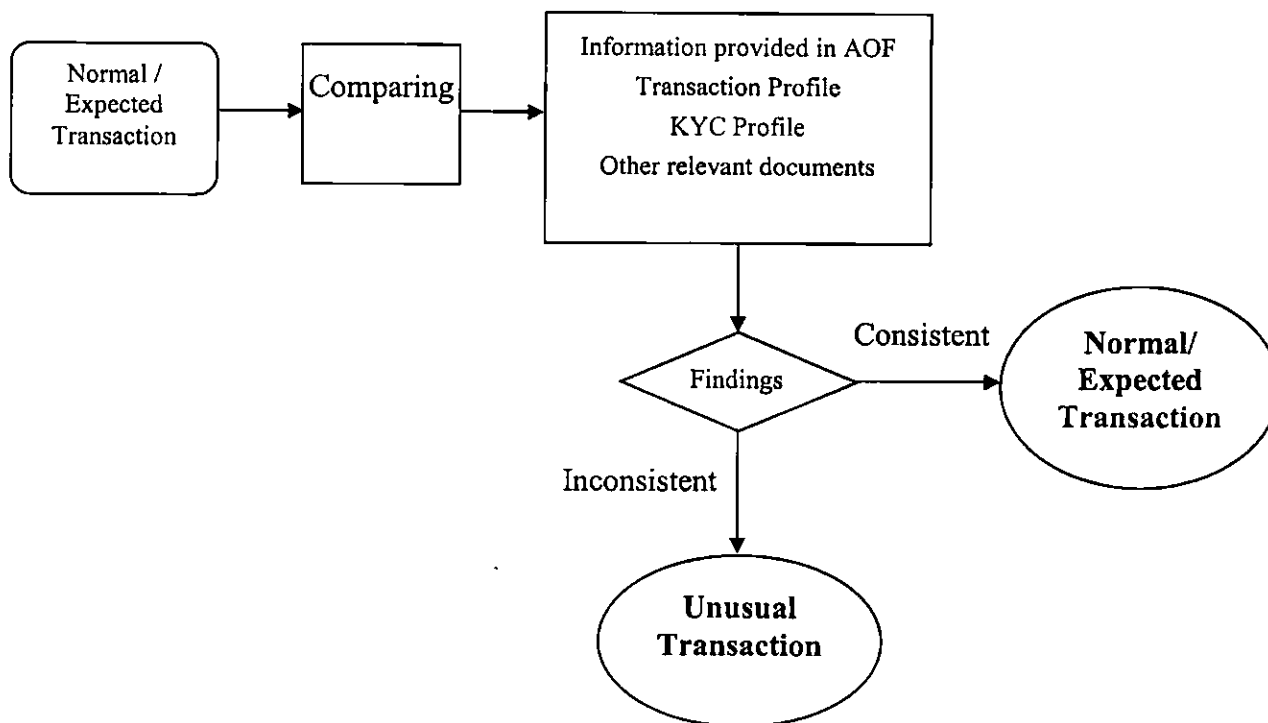


normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.

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:

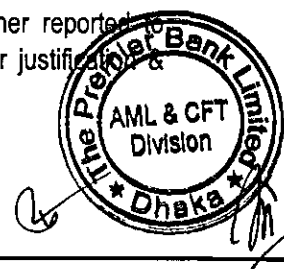
a) Identification:

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:

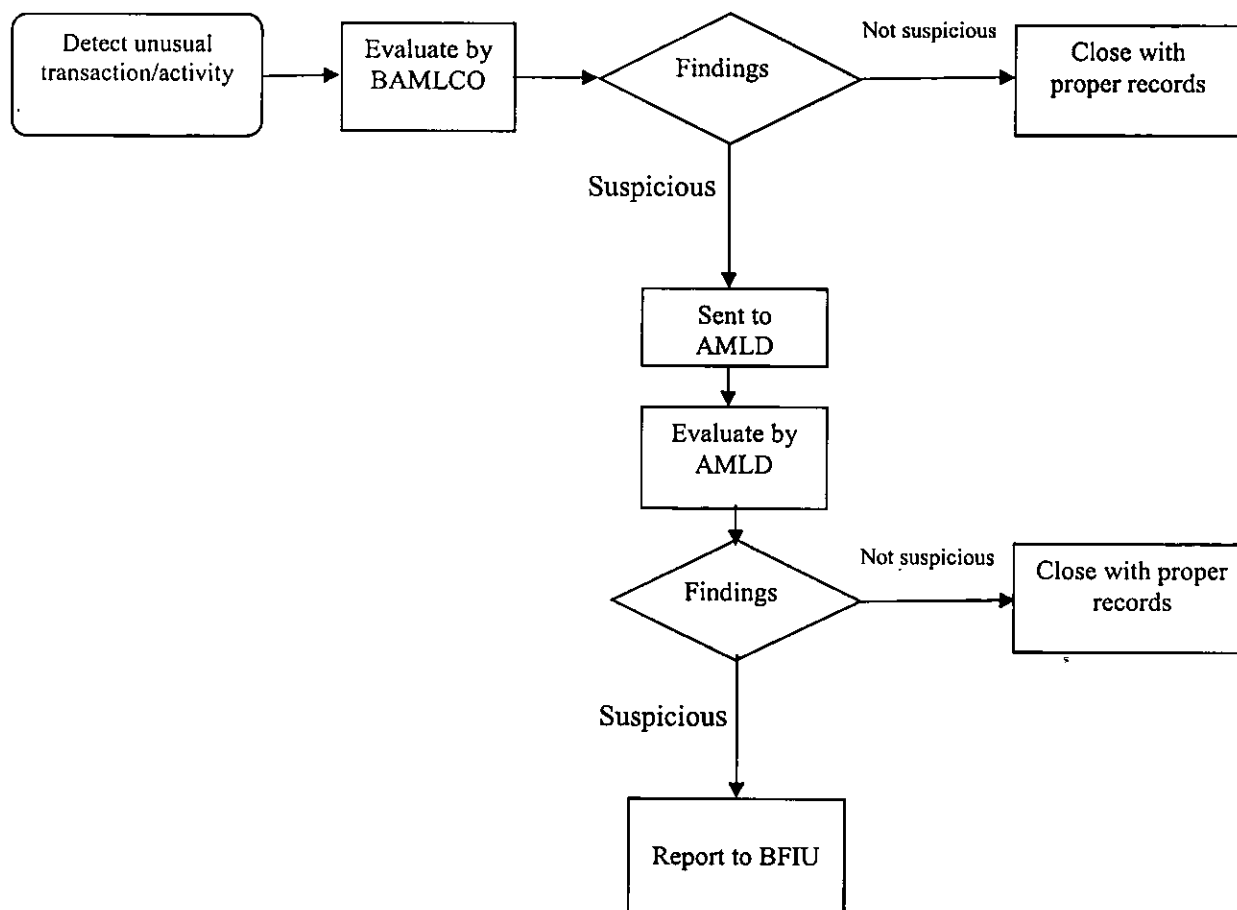
These problems must be in place at branch level and Anti-Money Laundering Division (AML). After identification of STR/SAR, at branch level BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BAMLCO must be tactful considering the tipping off provision of the acts. If BAMLCO is not satisfied, he should forward the report to AMLD. After receiving report from branch, AMLD 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:

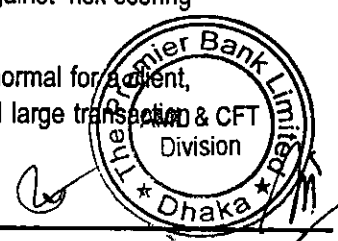
This is the final stage and FIs should submit STR/SAR to Bangladesh Bank if it is still suspicious.

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

**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 Wolfsberg 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 transactions are 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.

1.2 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?

3. Internal Reporting Procedures and Records :

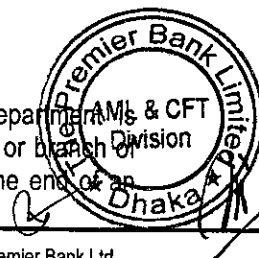
3.1 Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the CAMLCO. This ensures speed, confidentiality and accessibility to the CAMLCO. However, in line with accepted practice, some financial sector businesses may choose to require 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.

3.2 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.

3.3 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.

3.4 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

3.5 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.

3.6 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.

4 .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 AMLD of the bank by using specified format/instruction given by the BFIU.

SUSPICIOUS TRANSACTION TO BE REPORTED IMMEDIATELY ON DETECTION AS PER CIRCULAR NO. AML-19/008 DATED AUGUST 14,2008 ANNEXURE-A

4.1 STR to be submitted in the prescribe format directly by the CAMLCO to:

The General Manager
Bangladesh Financial Intelligence Unit (BFIU)
Bangladesh Bank
Head Office
Dhaka

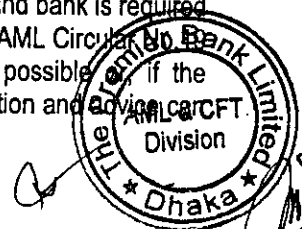
Under sealed cover marking "CONFIDENTIAL STR"

4.2 The Bangladesh Financial Unit of Bangladesh Bank can be contacted during office hours at the following numbers:

Telephone: (02) 9530118 , Fax: (02) 9530089

Email: gm.amld@bb.org.bd

4.3 The use of a standard format in the reporting of suspicious activities is important and bank is required to use the unusual/suspicious transactions reporting form as per Annexure KA of the AML Circular No. AML-19/008 dated 14th August, 2008. Suspicious activity reports should be typed whenever possible and if the standard layout is followed, generated on word-processing software. Further information and advice can be obtained from the Bangladesh Financial Intelligence Unit of Bangladesh Bank.



4.4 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.

4.5 Where additional relevant evidence is held which could be made available to the investigating officer, this should be noted on the form.

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.

5 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.

6 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.

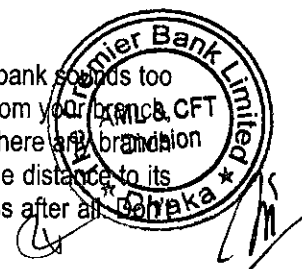
7 "SAFE HARBOR" PROVISIONS FOR REPORTING

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.

5. RED FLAGS OR INDICATORS OF STR

5.1 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.

5.2 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, CFT 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.



be bullied by the sales personnel who follow the "no question asked" philosophy of taking in new business.

5.3 Suspicious Customer Behavior:

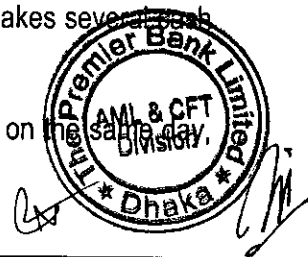
- Customer has an unusual or excessively nervous demeanor.
- Customer discusses the record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with 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.

5.4 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.

5.5 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.

5.6 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.

5.7 Suspicious Activity in Credit Transactions:

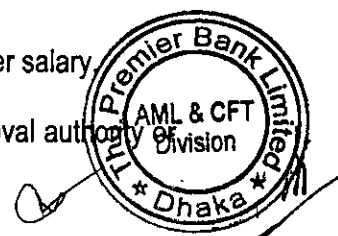
- A customer's financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.

5.8 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

5.9 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.



5.10 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 9**OTHER REPORTS****1. Cash Transaction Report (CTR)**

As per Bangladesh bank directives Bank shall submit CTR centrally for deposit and withdrawal of cash for such amount as determined by Bangladesh Bank from time to time. CTR of a particular month should be reported by AML Division to BFIU by 21st day of the following month through goAML Web. If in a particular month no CTR transaction is made by any Branch, Branch shall report to AML Division as "No CTR transaction has been occurred for the month of "XXX". AML Division shall report a list of such Branches through goAML Message Board while submitting the CTR for the reporting month. Inter Bank or Inter Branch transactions will not be reported. Only cash withdrawal transactions will be reported for Govt. accounts, Govt. owned entities, Semi Govt. owned entities and/or Autonomous organizations. At present CTR threshold amount is BDT10, 00,000.00 (Ten lakh) and above or equivalent either by single entry or multiple transaction in a day.

2. Structuring of Cash Transaction

As per Money Laundering prevention Act, structuring (unnecessary transaction) is an offence. If a customer intends to conduct such transactions to avoid reporting requirements, under the MLP Act, it is called structuring. Branch official should be vigilant to detect structuring and report to AMLD as STR. CTR should be analyzed before submitting by Branches and if any suspicious transaction found, Branch shall report it immediately to AML Division. If no suspicious transaction found, Branch shall report to AML Division as "No suspicious Transaction Found".

3. Half Yearly Report to be submitted to the CEO/ BOARD

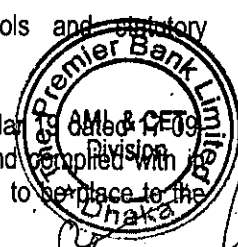
As per Bangladesh Bank directives in BFIU Circular No. 19 dated 17/09/2017, AMLD will submit a report on Half- Yearly basis on the implementation status/steps taken to combating money laundering and other related AML issues to the CEO/Board on regular basis.

4. Self-Assessment Process

Bank should **establish a half-yearly self-assessment process** that will assess how effectively the bank's anti-money laundering procedures enable 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, who performed it, how it was controlled and 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. The report should provide conclusions to three key questions:

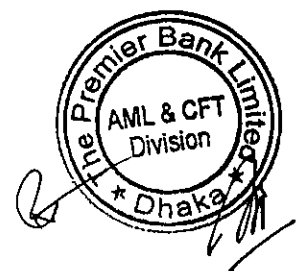
- Is anti-money laundering procedures in place?
- Is anti-money laundering procedures being adhered to?
- Do anti-money laundering procedures comply with all policies, controls and statutory requirements?

Branch shall assess their performance on half-yearly basis according to AML circular dated 17/09/2018, of BFIU, Bangladesh Bank. The shortcomings identified to be overcome and complied with in next half year and AMLD will prepare an appraisal report on half yearly basis and to be placed to the CEO with a copy to BFIU, Bangladesh bank.



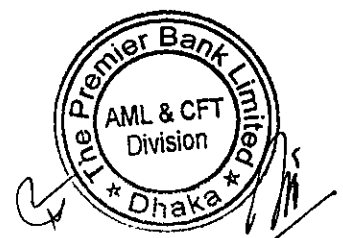
5. System of Independent Testing Procedures

As per the format given in AML circular no.19 dated 17-09-2018, 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 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, AMLD 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.



CHAPTER 10**RECORD KEEPING****1. Statutory Requirements:**

- 1.1 The requirement contained in Section 25 (1) of Money Laundering Prevention Act, 2012, to retain complete and accurate information 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.
- 1.2 FATF recommendation 11-states 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.
- 1.3 The records prepared and maintained by the bank on its customer relationships and transactions should be such that:
- requirements of legislation and Bangladesh Bank directives are fully met;
 - competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
 - any transactions effected via the institution can be reconstructed;
 - any customer can be properly identified and located;
 - all suspicious reports received internally and those made to Bangladesh Bank can be identified; and
 - the institution can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.
- 1.4 Records relating to verification of identity will generally comprise:
- a description of the nature of all the evidence received relating to the identity of the verification subject;
 - the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.
- 1.5 Records relating to transactions will generally comprise:
- details of personal identity, including the names and addresses, etc. pertaining to:
 - (1) the customer;
 - (2) the beneficial owner of the account or product;
 - (3) the non-account holder conducting any significant one-off transaction;
 - (4) any counter-party;
 - details of transaction including:
 - 1) nature of such transactions;
 - 2) volume of transactions customer's instruction(s) and authority(ies);
 - 3) source(s) of funds;
 - 4) destination(s) of funds;
 - 5) book entries;
 - 6) custody of documentation;
 - 7) date of the transaction;



- 8) form in which funds are offered and paid out.
- 9) parties to the transaction
- 10) identity of the person who conducted the transaction on behalf of the customer

1.6 These records of identity must be kept for at least five years from the date when the relationship with the customer has ended. This is the date of:

- i. the closing of an account
- ii. the providing of any financial services
- iii. the carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
- iv. the ending of the business relationship; or
- v. the commencement of proceedings to recover debts payable on insolvency.

Bank should ensure that records pertaining to the identification of the customer, his/her address (e.g. copies of documents like passport, national ID/ smart ID card, driving license, trade license, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended and should be made available to the competent authorities upon request without delay.

2. RETRIEVAL OF RECORDS

To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of the bank, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduce and recollected without undue delay.

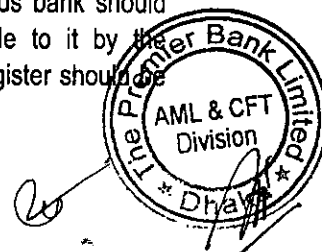
It is not always necessary to retain documents in their original hard copy form, provided that the firm has reliable procedures for holding records in microfiche or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, bank may rely on the records of a third party, such as a financial institution or clearing house in respect of details of payments made by customers. However, the primary requirement is on the bank itself and the obligation is thus on the business to ensure that the third party 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.

3. INSPECTION AND INVESTIGATION

Where 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 consent of the BFIU or conclusion of the case even though the five-year limit may have been reached. To ensure the preservation of such records bank should maintain a register or tabular records of all investigations and inspection made to it by the investigating authority or Bangladesh Bank and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

- i. the date of submission and reference of the STR;
- ii. the date and nature of the enquiry;



- iii. the authority who made the enquiry, investigation and reference; and
- iv. details of the account(s) involved.

In PBL Branches should introduce such register and follow the procedure.

4. TRAINING RECORDS

Bank will comply with the regulations concerning staff training, they shall maintain training records which include:-

- (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 staffs understanding of the requirements;
- (v) an on-going training plan.

5. BRANCH LEVEL RECORD KEEPING

To ensure the effective monitoring and demonstrate their compliance with the concerned regulations, bank will ensure the keeping or availability of the following records at the branch level either in hard form or electronic form:

- 1. Information regarding Identification of the customer,
- 2. KYC information of a customer,
- 3. Transaction report,
- 4. Suspicious Transaction Report generated from the branch,
- 5. Exception report,
- 6. Training record,
- 7. Return submitted or information provided to the Head Office or competent authority.
- 8. BAMLCC Meeting Minutes

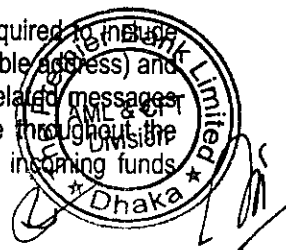
6. SHARING OF RECORD/ INFORMATION OF/TO A CUSTOMER

Under the provisions of MLPA 2012, Bank shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having approval from the court and prior approval from Bangladesh Bank.

7. Wire Transfer Transactions:

7.1 Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of **telegraphic transfers (TT)** and electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction.

7.2 Following the recent focus on terrorist financing, relevant financial businesses are required to ensure accurate and meaningful information of originator (name, account number, and where possible address) and beneficiary (account name and/or account number) on all outgoing funds transfers and related messages that are sent, and this information should remain with the transfer or related message throughout the payment chain. Bank should conduct enhanced scrutiny of and monitor for suspicious incoming funds transfers which do not contain meaningful originator information.

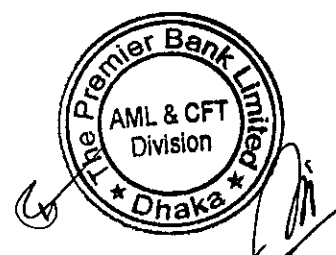


7.3 The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a minimum of five years.

Cross Border Wire transfer:

- a) All cross border wire transfer must be accompanied by accurate and meaningful originator information.
- b) Information accompanying cross border wire transfer must contain the name and address of the originator and where an account exists, the number of that account. In absence of an account, a unique reference number, as prevalent in the country concerned, must be included.
- c) 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 (b) above.

In PBL, both in Head Office and Branch level, a register must be maintained following the procedure narrated hereinabove.



CHAPTER III**AWARENESS PROGRAMS****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.

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.

3. Education and Training programs:

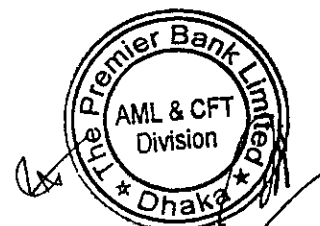
All relevant staff should be educated in the process of the "know your customer" requirements for money laundering and terrorist financing prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship 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.

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.

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 issues should also be different for each category. Job specific AML trainings are discussed below:

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.

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.

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 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.

5.4 Credit Officers:

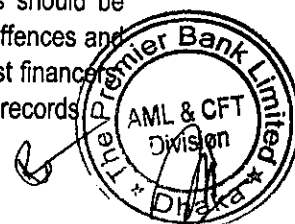
Training should reflect an understanding of the credit function. Judgments about collateral and credit all require awareness and vigilance toward possible money laundering activities. Indirect lending programs and lease financing also call for KYC efforts and sensitivity to laundering risks.

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.

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 financing, internal reporting procedures and the requirements for verification of identity and the retention of records.



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.

5.8 AML & CFT Compliance Officer

The AML 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 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.

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 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.

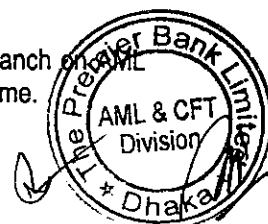
7. Refresher Training

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 suspicious activity.

8. In-house discussion :

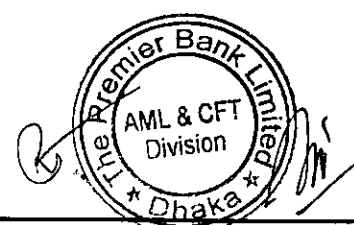
Branch will arrange in house discussion on regular basis to update the employees of the branch on AML laws and regulation and circulars issued from Bangladesh Bank and Head office from time to time.



9. Education and Training of Customer:

As instructed by Bangladesh Bank vide BFIU circular 19 issued dated 17-09-2017, 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 issue, their respective responsibilities and the various control and procedures introduced by the bank to deter money laundering and terrorist financing.



CHAPTER 12**1. Correspondent Banking Relationship**

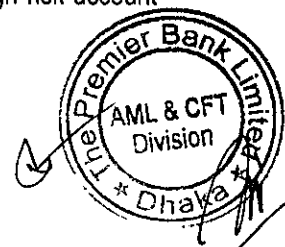
Correspondent Banking relationship sometimes creates a risk that the other Bank's customer may be using that Bank to launder funds. It is not necessary possible to conduct due diligence on that Bank's customer base and as such. These relationships require care and attention to guard against becoming unwilling participants in these activities. The following control should be implemented for establishing corresponding banking relationship.

- (a) Before providing correspondent banking service CAMLCO'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 Ka of BFIU Circular No. 19 dated 17/09/2017 - 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.
- (b) Bank should not establish or continue a correspondent banking relationship with **SHELL BANK** or **Banks 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).
- (c) 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.
- (d) 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.
- (e) Enhanced due diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customer to transact business on their behalf (i.e. payable through account)
- (f) The Bank will review correspondent banking relationship as and when required.
- (g) Before establishing relation Bank will be satisfied with the respondent institution's Anti money laundering and Anti-Terrorism control.
- (h) CDD measures are almost same but such measures also apply for securities transaction or fund transfer, whether for the cross border financial institution as principal or for its customer

2. Non-Profit Organizations (NPO) AND NGO :

Account of Charities, NGO & NPO to be treated as high risk account. No account shall open without the registration from the appropriate authorities i.e. Bureau of NGO, Directorate of Co-operative society, Directors of social welfare where applicable.

Enhance Due Diligence (EDD) will be performed for opening and operating such account to prevent money laundering. As per foreign donation regulations (voluntary Activities) ordinance, 1978 and The 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 Govt. It is punishable offence. The Bank shall release the fund to ensure the approval of the Bureau of NGO. 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 should be monitored the transaction regularly.



3. KYC requirement for High Net Worth Customer

Complete the form for high net worth customer falling under the following criterion:

- 1) New customer whose initial deposit is more than Tk.50.00 lac (initial means within one month of account opening)
- 2) Existing customer whose total asset under management grow to > Tk. 50.00 lac for 3 consecutive months

3) Source of Wealth

i. Type of source of wealth

Business ownership
Profession

Top executive
investment

Inheritance
Others

Instruction: Please refer to the questions to be used when obtaining source of wealth. You may need to choose more than one category for a business owner with inherited wealth.

4) Notes of face to face meeting with customers.

5) Annual review of customer profile

Profession -- e.g. Physician, Lawyer, engineer, accountant and sports professional etc.

Investment--- some ones who buys and sells assets of any type: real estate, securities, companies, royalties and patents etc.

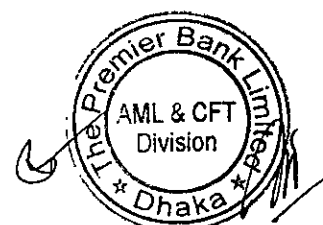
Prepared by: Account Officer/Relationship Manager:
With name & date

Reviewed by : Branch Manager/ Operations Manager &BAMLCO :
With name & date:

Model question to be used when obtaining source of wealth:

6. Wealth generated from Business ownership

- > Description & nature of business and its operation
- > Ownership type: private or public
- > What kind of economy
- > Percent of ownership?
- > Estimated sales volume?
- > Estimated net income?
- > Estimated net worth?
- > How long in Business?
- > How was the business established?
- > Other owners or partners: Yes/ No



- > Names of other owners or Partners?
- > Percent owned by other owners or partners?
- > Number of employees?
- > Number of Locations?
- > Geographic trade areas of business?
- > Other family members in business?
- > Significant revenue from govt. contact or license ?

7. Wealth derived from on being a Top executive

- > Estimate of compensation
- > What does the company do (for example, service, and manufacturer -----?)
- > Position held (For example, CEO, president etc.)
- > Length of time with the company
- > Area of experience (for Example, finance, production etc.
- > Publicly or private owned
- > Clients past experience (CFO at another com.)

8. Primary sources of wealth

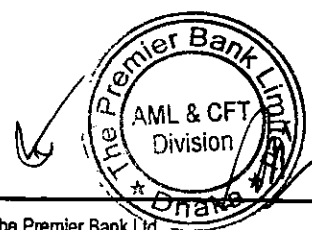
- > in what business was the wealth generated
- > Inherited from whom
- > Type of asset inherited
- > When were the asset inherited (land, securities, companies trust)
- > Percent ownership for a business that is inherited
- > How much was inherited

9. Wealth generated from a profession (Physician, Doctor, Lawyer, Engineer, Entertainer etc.)

- > What is profession, including area of specialty (example: Arts, singer, construction – engineer etc.)?
- > Source of wealth
- > Estimate of income

10. Wealth generated from investment

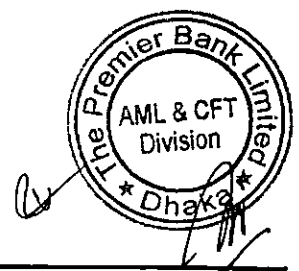
- > Where did the source of wealth come from?
- > What do the currently invest in (ex. Invested in share, bonds)?
- > What is the size of investment?
- > Cite notable public transactions if any
- > What is the client's role in transaction?
- > Estimated annual income/ capital appreciation?
- > How long has the client been an investor?



COMBATING FINANCING OF TERRORISM GUIDELINE



ANTI-MONEY LAUNDERING DIVISION
The Premier Bank Limited
Head Office, Dhaka.



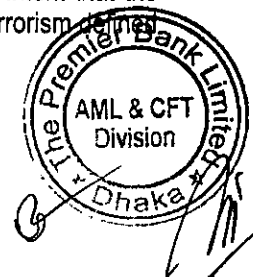
CHAPTER 1**BACKGROUND****Introduction**

- 1.1 This 'Combating Financing of Terrorism Policy' for The Premier 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.
- 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 section 16 (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 Guidelines is designed to assist The Premier 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 The Premier 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 The Premier 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 The Premier 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 The Premier Bank Limited in conjunction with the 'Anti Money Laundering Policy' for The Premier 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.

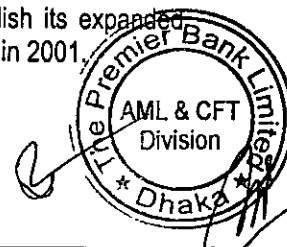
2.4.2 Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution's measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism 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

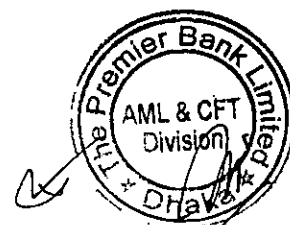
FATF adopted a set of 40 recommendations to prevent money laundering. To accomplish its expanded mission of combating financing of terrorism FATF adopted nine Special Recommendations in 2001.



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)

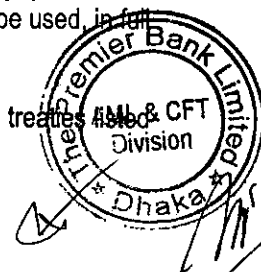
If any foreign national commits an offence under sub section (a), (b) or (c) he or she shall commit the offence of organizing "terrorist activities".

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 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.

2.4 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.

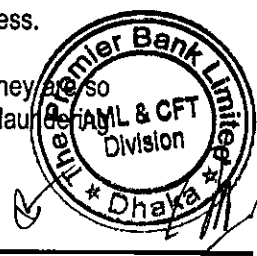
3. WHY WE MUST COMBAT FINANCING OF TERRORISM?

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 harbour 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.

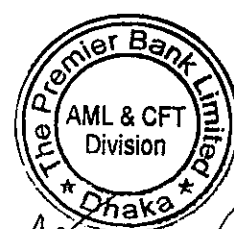
5.0 HOW THE PREMIER BANK LIMITED CAN HELP IN COMBATING TERRORIST FINANCING

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, The Premier 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 The Premier 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 –

(i) Bank;

(ii) Financial institution;

(iii) Insurer;

(iv) Money changer;

(v) Any company or institution which remits or transfers money or money value;

(vi) Any other institution carrying out its business with the approval of Bangladesh Bank;

(vii)

1) Stock dealer and stock broker,

2) Portfolio manager and merchant banker,

3) Security Custodian;

4) Asset Manager;

(viii)

1) Non-profit organization

2) Non Governmental Organization

3) Cooperative Society

(ix) Real estate Developer;

(x) Dealer in precious metals and/or stones;

(xi) Trust and Company Service Provider;

(xii) Lawyer, notary, other legal professionals and accountant;

(xiii) 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 –

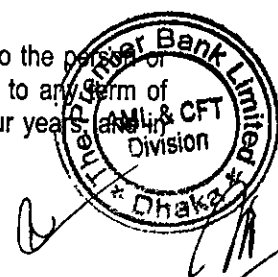
- a) Kills, injures seriously, puts confinement or kidnaps any person or abets to do the same, or damages any property belonging to any person or entity or the State or abets to do the same
- b) Instigates any person to kill, injure seriously, puts in confinement or kidnap any person, or to instigate 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) lacs.

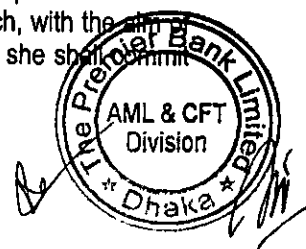
3.6) (a) If any entity is found guilty of any of the offences set out in sub-sections (1) to (4), steps may be taken under section 18 and in addition to this a fine may be imposed not less than the greater of thrice the value of the property involved with the offence or taka 50(fifty) lacs ; and

(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

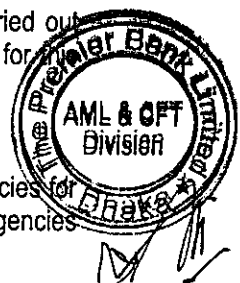
(a.3) If the punishment of that offence is life imprisonment or imprisonment of any other term then, shall be liable for imprisonment for at least three years and a fine may be imposed in addition to this;

(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 that 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.

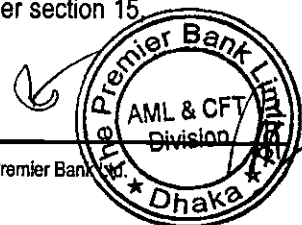
(7) For the purpose of investigation relating to financing of terrorism law enforcement agencies shall have the right to access any document or file of any bank as per the following conditions:

- 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.

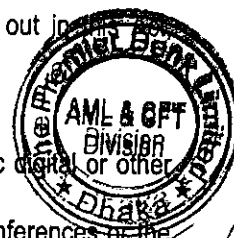
(2) If the application for review under sub-section (1) is refused, the said aggrieved organization, within thirty days of such refusal, may prefer an appeal before the High Court Division.

(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 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 trial of offence triable 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.

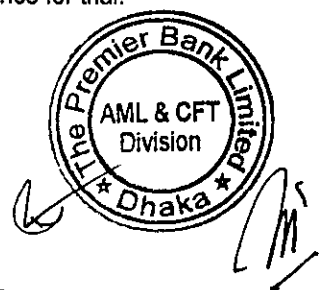
General Provisions

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.

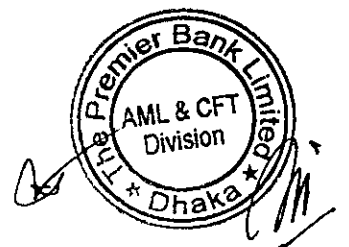
Original text and English text – The original text of this Act shall be in Bangla and there shall be a reliable English translation.

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. The Premier 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 The Premier 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. 19 dated 17-09-2017 issued by BFIU, guided to have defined responsibilities of Banks to combat financing of terrorism. The Premier 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, The Premier 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.

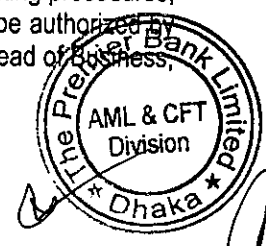
2.4 We are strongly committed to assist and cooperate with the relevant law enforcement authorities in Bangladesh whenever possible and to the fullest extent possible. Furthermore, The Premier Bank Limited also renew it's commitments to:

- 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 The Premier 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/D). The AML/D is responsible for overall supervision & implementation of AML/CFT policy in the Bank in compliance with BFIU, Bangladesh Bank's instructions.

5.2 The Premier 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 The Premier Bank Limited is written, approved by the Board of Directors, and noted as such in the board meeting minutes.

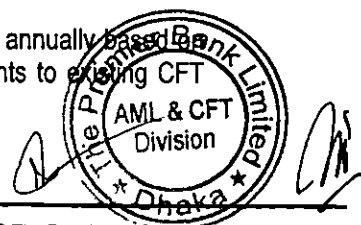
6.2 The CFT compliance policy establishes clear responsibilities and accountabilities within the bank to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using its facilities for the financing of terrorist activities, thus ensuring that it comply 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 its 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 financier 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 Circular

According to the AML circular 19 banks shall perform the following activities as per requirements under the Anti-Terrorism Act, 2009 (including amendments of 2012):

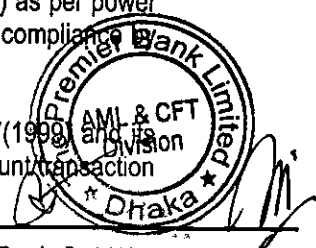
- a) Anti-Money Laundering Division of the Head office and the officer nominated at the branch level shall perform the duty of compliance and internal monitoring of the instructions Anti-Terrorism Act, 2009 (including amendments of 2012) and the relevant instructions issued by the Bangladesh Bank.
- 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 AMLD of the bank. AMLD 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 AMLD 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 Circular 19 shall have to be used to report the STRs related to terrorist financing.

4. AML 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. The Premier 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

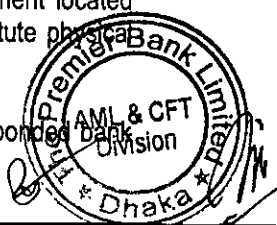
Correspondent banking relationships sometimes creates a risk that the other Bank's customer may be using that Bank for financing terrorism. It is not necessarily possible to conduct due diligence on that Bank's customer base and as such, these relationships require additional care and attention to guard against becoming unwilling participants in this activity. The following control should be implemented for establishing corresponding banking relationship (Reference: Bangladesh Bank AML 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 with in 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 respondent 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 The Premier 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:

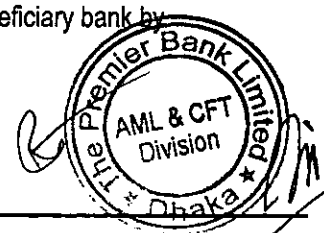
4.1) All cross-border wire transfer must be accompanied by accurate and meaningful originator information.

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

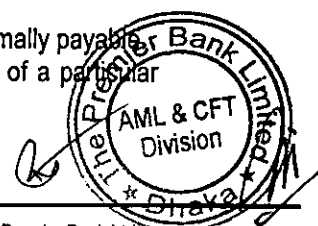
It may not be feasible for specific branches of the bank having very large number of customers to track every single account against the TP where a risk based approach should be taken for monitoring transactions based on use of "Customer Categories" and "Transaction Limits" (individual and aggregate) 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 :

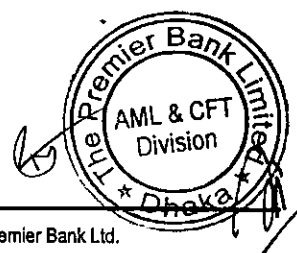
When there is suspicion that funds are linked to terrorist financing, staff members are required to submit STRs to their respective Branch Anti Money laundering officer (BAMLCO). BAMLCO must send (if justified) STR to AMLD on the same day as per format provided by Bangladesh Bank in BFIU Circular No. 19/2017. 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:

- ① Customer is evasive or unwilling to provide document & information as & when requested.
- ① Customer using different identification for different transaction.
- ① Customers frequently visit high risk countries.
- ① Customer exchanging small denomination notes into large denomination notes, in large quality.
- ① Customer having relations with persons working abroad in an illegal job.
- ① Customer giving false information.
- ① Persons directly or indirectly involved in smuggling.
- ① Information given in KYC is inconsistent with his income and business.
- ① Person's Transaction is not consistent with his income and business.
- ① Source of fund does not cover his transaction profile.
- ① Deposits of funds with a request for their immediate transfer elsewhere;
- ① Unwarranted and unexplained international transfers.
- ① The payment of commissions or fees that appears excessive in relation to those normally payable
- ① Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type of transaction or particular method of transacting.
- ① Transactions do not appear to be in keeping with normal industry practices.



- ① Purchase of commodities at prices significantly above or below market price.
- ① Unnecessarily complex transactions;/structuring of transactions to avoid CTR.
- ① Buying or selling securities with no apparent concern for making a profit or avoiding a loss.
- ① The transaction in which there is reason to believe that the proceeds came from illegal / criminal activities.
- ① Large cash deposit through online.
- ① Change of transaction pattern i.e. maximum number transaction than previous.
- ① Remittance received from different places which are not consistent with the clients business or income.
- ① Frequent transaction with Border areas branches.
- ① Huge transaction in deposit/withdrawal but less available balance.
- ① Sudden huge cash deposit/ transfer deposit.
- ① Customer withdrawing large sum of money in cash immediately after receipt of credit
- ① Branch request to customer to contact us which customer avoided or did not respond.
- ① Customer reluctance or refusal to disclose other banking relationships.
- ① Large number of individuals making payment in to the same account without an adequate explanation.
- ① 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 :

The Premier 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.19 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.

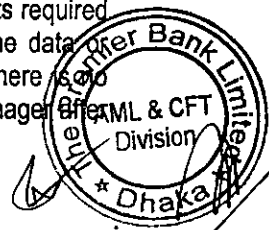
4. Customer Acceptance policy

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 (ies)
- 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 categorisation 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 disadvantaged.

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 SI. 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.19 issued dated 17/09/2017 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.

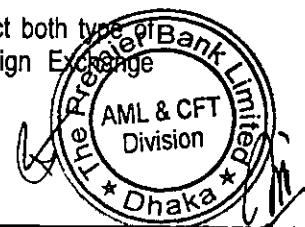
16) SHELL BANK: Bank will not establish correspondent relationship with Shell Bank and the bank is maintaining relationship with Shell bank.

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. 19 dated 17/09/2017.

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 PBL 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.

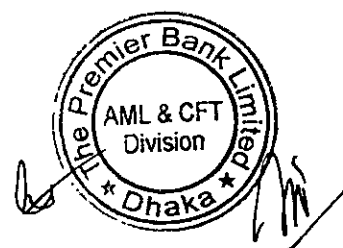
FATF also recommended that financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction 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

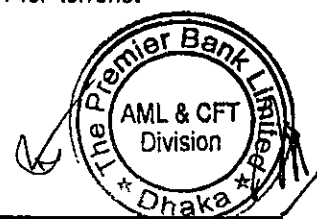
Under the provisions of Anti Terrorism Act-2012 (sec.15 sub. sec.7) , Bank shall not share account related information & document to the law enforcing agencies to investigate financing of terrorism cases without having approval from the appropriate court or tribunal or prior approval from Bangladesh Bank.



CHAPTER 8**RESPONSIBILITIES OF BANK OFFICIALS**

To comply with AML 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 The Premier 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 AMLD 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.



--- THE END ---

