GUIDELINES ON PREVENTION OF MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM FOR CAPITAL MARKET INTERMEDIARIES

Bangladesh Financial Intelligence Unit
BANGLADESH BANK

Core Team

Coordinator

Mr. A K M Ehsan
Joint Director, Bangladesh Financial Intelligence Unit

Member

Mr. Mahbubul Alam
Deputy Director, Bangladesh Financial Intelligence Unit

Ms. Indranee Haque
Assistant Director, Bangladesh Financial Intelligence Unit

Mr. Md. Ferdous Zaman Sardar
Assistant Director, Bangladesh Financial Intelligence Unit

Member Secretary

Mr. Md Masud Rana
Deputy Director, Bangladesh Financial Intelligence Unit

Review Team

Mr. Md. Sirajul Islam
Joint Director, Bangladesh Financial Intelligence Unit

Mr. Md. Rafiqul Islam
Joint Director, Bangladesh Financial Intelligence Unit

Mr. Kamal Hossain
Deputy Director, Bangladesh Financial Intelligence Unit

Ms. Yasmin Rahman Bula
Deputy Director, Bangladesh Financial Intelligence Unit

Mr. A K M Ramizul Islam
Deputy Director, Bangladesh Financial Intelligence Unit

Mr. Mohammad Abdur Rab
Deputy Director, Bangladesh Financial Intelligence Unit

Mr. A K M Nurun Nabi
Deputy Director, Bangladesh Financial Intelligence Unit

Preface

The techniques of Money Laundering and Terrorist Financing (ML/TF) are ever evolving process. The methods and techniques used for money laundering and terrorist financing are changing in response to developing counter measures. Financial Action Task Force (FATF), the international standard setter for AML/CFT, has introduced 40+9 recommendations aiming to money laundering (ML) and financing of terrorism (TF), which applicable to all countries around the globe. Afterwards, in 2012 FATF has revised its 40+9 recommendations and introduced a new set of 40 recommendations by merging them.

In line with the international standards and initiatives, Bangladesh has passed Money Laundering Prevention Act (MLPA), 2002. Afterwards several amendments were made and this year a new Money Laundering Prevention Act, 2012 has been passed. The Government has also enacted Anti Terrorism Act (ATA) in 2009 aiming to combat terrorism and terrorism financing and this Act was also amended in 2012. Both the Acts have empowered Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank (BB) to perform the anchor role in combating ML/TF through issuing instructions and directives for reporting agencies and building awareness in the financial sectors.

This Guideline titled "Guidelines on prevention of money laundering & combating financing of terrorism for capital market intermediaries (referred herein as Guideline)" will be applicable for Capital Market Intermediaries (referred herein as CMI) as describes in section 2(w)(vii) of Money Laundering Prevention Act, 2012 (MLPA, 2012) and section 2(20)(g) in Anti Terrorism Act, 2009 (including amendment of 2012). This Guideline has been prepared specially for CMI to enable them to keep in place an effective preventative measures against ML/TF related issues which leads to establish ML/TF risks free business.

This Guideline is deemed to be the best practice but should not necessarily be used as a legal interpretation of the said Acts. Because of vulnerabilities of Capital Market being abused by money launderers and terrorist financiers, BFIU, as part of its supervisory process, will assess the adequacy of procedures adapted to AML/CFT by the CMI and the degree of compliance with such procedures. This guideline is designed to enable CMI to undertake its function in consistence with the Bangladesh's AML/CFT laws and regulations.

An overriding aim of this Guideline is to ensure that appropriate identification information is obtained in relation to their Clients by CMI. This is not only to assist the detection of suspect transactions but also to create an effective "audit trail" in the event of an investigation, if necessary. Each CMI will be responsible for formulating its own AML/CFT policies, programs and Guidelines in the light of this Guideline.

Table of contents

CHAPTER FIVE: Know Your Client (KYC) Policies and Procedures

CHAPTER SIX: Transaction Monitoring & Reporting Process

List of Abbreviations

ML/TF	Money Laundering/Terrorist Financing
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
BFIU	Bangladesh Financial Intelligence Unit
APG	Asia Pacific Group on Money Laundering
ATA	Anti Terrorism Act
ATO	Anti Terrorism Ordinance
BB	Bangladesh Bank
BDT	Bangladesh Taka
CMI	Capital Market Intermediaries
CDD	Client Due Diligence
CTC	Counter Terrorism Committee
FATF	Financial Action Task Force
FCBs	Foreign Commercial Banks
FIU	Financial Intelligence Unit
GoB	Government of Bangladesh
ICRG	International Cooperation Review Group
KYC	Know Your Client
MLPA	Money Laundering Prevention Act
MLPO	Money Laundering Prevention Ordinance
NCC	National Coordination Committee on AML/CFT
NCCT	Non-cooperating Countries and Territories
STR	Suspicious Transaction Report
UNCAC	United Nations Convention Against Corruption
UNODC	UN Office on Drugs and Crime
UNSCR	United Nations Security Council Resolution

Chapter: One

Basics of Money Laundering and Terrorist Financing

1.1 Introduction

For most countries money laundering and terrorist financing raise significant issues with regard to prevention, detection and prosecution. Sophisticated techniques are used to launder money and finance terrorism add to the complexity of these issues. Such techniques for money laundering may involve: multiple financial transactions, use of different financial instruments and other kinds of value-storing assets, different types of financial institutions, accountants, financial advisers, shell corporations and other service providers like remittance service; complex web of transfers to, through, and from different countries. On the other hand, terrorism financing involves intention to provide assets or assist in some way to conduct terrorist acts. A less simple concept, however, is defining terrorism itself, because the term may have significant political, religious, and national implications that may vary from country to country. Money laundering and terrorist financing often display similar transactional features, generally with the concealment and disguise the source of illicit proceeds.

Money launderers transfer or try to transfer illicit funds through legal channels in order to conceal their criminal origins, while those who finance terrorism, transfer funds that may be legal or illicit origin in such a way as to conceal their source and ultimate use. But the result is the same—reward. When money is laundered, criminals profit from their actions; they are rewarded by concealing the criminal act that generates the illicit proceeds and by disguising the origins of what appear to be legitimate proceeds. Similarly, those who finance terrorism are rewarded by concealing the origins of their funding and disguising the financial support to carry out their terrorist stratagems and attacks.

1.2 History of Money Laundering Prevention Activities

In response to the growing concern about money laundering and terrorist activities, the international community has acted on many fronts. This part of this Guideline 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 AML/CFT purposes.

1.2.1 United Nations and UN Security Council Resolutions

The United Nations (UN) was the first international organization to undertake significant action to fight against money laundering on a truly world-wide basis. The UN actively operates a program to fight against money laundering; the Global Program against Money Laundering, which is headquartered in Vienna, Austria, is part of the UN Office on Drugs and Crime (UNODC).

The UN has adopted United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) known as Vienna Convention and International Convention against Transnational Organized Crime (2000) known as Palermo Convention. In 2001, International Convention for the Suppression of the Financing of Terrorism (1999) was adopted. These conventions bind all the state parties of UN to place appropriate measures for combating money laundering and terrorist financing.

Apart from these conventions various UN Security Council Resolutions has adopted in response to a threat to international peace and security under Chapter VII of the UN Charter binding upon all UN member countries (UNSCR 1267 and its successors, 1373 and the resolutions related to the prevention, suppression and disruption of proliferation of weapons for mass destructions).

1.2.2 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 ML/TF.

FATF performs three primary functions with regard to money laundering and financing of terrorism:

- monitoring members' progress (directly or via regional bodies) in implementing AML/CFT measures;
- reviewing and reporting on laundering trends, techniques and counter-measures; and

- promoting the adoption and implementation of FATF AML/CFT standards globally.

FATF adopted a set of recommendations which constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. These recommendations were initially issued in 1990 and revised in 1996, 2003 and finally in 2012. Proliferation financing has been included in the new standards in 2012.

The FATF has set up the International Co-operation Review Group (ICRG) as a new process that is designed to notably engage the 'unwilling' and those jurisdictions that pose a real risk to the international financial system. The ICRG process is designed to bind FATF and FSRB members to show an effective commitment to implement international obligations. The time and money that one jurisdiction spend on creating an effective AML/CFT system in that country is wasted if 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 remedy the shortcomings underpinning the judgment of the FATF Plenary. That means that 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.

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

1.2.4 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, Organization for Economic Cooperation and Development, 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 (FATF).

The APG has five key roles:

- To assess compliance by APG members with the global AML/CFT 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 AML/CFT 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 on money laundering and terrorist financing trends and methods and inform APG members related 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.

1.2.5 International Organization of Securities Commissioners (IOSCO)

The International Organization of Securities Commissioners (IOSCO) is an organization of securities commissioners and administrators that have day-to-day responsibilities for securities regulation and the administration of securities laws in their respective countries. The current membership of IOSCO is comprised of regulatory bodies from 182 countries (ordinary member country-105, associate member country-11 and affiliated member country-62). With regard to money laundering, IOSCO passed a “Resolution on Money Laundering” in 1992. Like other international organizations of this type, IOSCO does not have law-making authority. IOSCO’s main objectives are to assist its members to:

- Cooperate together to promote high standards of regulation in order to maintain just, efficient and sound markets
- Exchange information on their respective experiences in order to promote the development of domestic markets
- Unite their efforts to establish standards and an effective surveillance of international securities transactions
- Provide mutual assistance to promote the integrity of the markets by a rigorous application of the standards and by effective enforcement against offenses.

1.2.6 UN Security Council Resolution 1267, 1373, 1540, 1718, 1737 and Successors

The UN Security Council acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the "Sanctions Committee" (now called the 1267 Committee). The initial Resolution 1267 of October 15, 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).

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. (www.un.org/sc/committees/1267/consolist.shtml)

United Nations Security Council Resolution 1373, adopted unanimously on 28 September 2001, is a counter-terrorism measure passed following the 11 September terrorist attacks on the United States. This resolution aimed to hinder terrorist groups in various ways. It recalled provisions from resolutions 1189 (1998), 1269 (1999) and 1368 (2001) concerning terrorism. UN member states were encouraged to share their intelligence on terrorist groups in order to assist in combating international terrorism. The resolution also calls on all states to adjust their national laws so that they can ratify all of the existing international conventions on terrorism. It stated that all States should also ensure that terrorist acts are established as serious criminal offences in domestic laws and regulations and that the seriousness of such acts is duly reflected in sentences served. The resolution established the Security Council's Counter Terrorism Committee [CTC] to monitor state compliance with is provisions.

United Nations Security Council resolutions 1540, 1718 and 1737 are related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and it's financing. The said resolutions are against North Korea and Iran.

All these resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity

designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

1.3 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 definition adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988) and the United Nations Convention against Transnational Organized Crime (the Palermo Convention, 2000). The definition of money laundering as per the above UN Convention is as follows:

- The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

- The concealing or disguising of 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), 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.”

According to the Section 2 of the Money Laundering Prevention Act, 2012 -

“Money Laundering” means –

(i) knowingly move, convert, or transfer proceeds of crime or property involved in an offence for the following purposes:

(1) concealing or disguising the illicit origin/nature, source, location, ownership or control of the proceeds of crime; or
(2) assist any person for evading the legal consequences of his or her action who is involved in the commission of the predicate offence;

(ii) smuggle funds or property abroad earned through legal or illegal means;

(iii) knowingly transfer or remit the proceeds of crime into or out of Bangladesh with the intention of hiding or disguising its illegal source;

(iv) conclude or attempt to conclude financial transactions in such a manner as to avoid reporting requirement under this Ordinance.

(v) convert or movement or transfer property with the intention to instigate or assist the carrying out of a predicate offence;

(vi) acquire, possess or use property, knowing that such property is the proceeds of a predicate offence; or

(vii) perform such activities so that illegal source of the proceeds of crime may be concealed or disguised; or

(viii) participate in, associate with, conspire to commit, attempt to commit or abet, instigate or counsel to commit any offences mentioned above.

1.4 What Is Terrorist Financing

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), United Nations defines TF in the following manner:

1. 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 annex to the convention; 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. 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)[1].

Some countries face difficulties in defining terrorism as not all countries have adopted the conventions agreed on specifically what actions constitute terrorism. In addition, the meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country. FATF, which is recognized as the international standard setter for combating financing of terrorism (CFT) efforts, does not specifically define the term financing of terrorism in its nine Special Recommendations on Terrorist Financing (Special Recommendations). Nonetheless, FATF urges countries to ratify and implement the 1999 United Nations International Convention for Suppression of the Financing of Terrorism. Thus, the above definition is the one most countries have adopted for purposes of defining terrorist financing.

According to the section 7 of the Anti Terrorism Act, 2009 (including amendment of 2012), financing of terrorism means:

[1] International Convention for the Suppression of the Financing of Terrorism (1999), Article, http://www.un.org/law/cod/finterr.htm. The treaties referred to annex in sub-paragraph 1(a) shall be available in this web link.

(1) If any person or entity knowingly supplies or expresses the intention to supply money, service, material support or any other property to another person or entity 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 committing the offence of financing for terrorist activities.

(2) 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 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 committing the offence of financing for terrorist activities.

(3) If any person or entity knowingly makes arrangements for collecting money, services, material support or any other property for another person or entity 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 committing the offence of financing for terrorist activities.

(4) If any person or entity knowingly instigate in such a manner, another person or entity to supply, receive, or arrange money, services, material support or any other property 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 committing the offence of financing for terrorist activities.

1.5 The Link between Money Laundering and Terrorist Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support

terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of fund for terrorist activities, 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.

For these reasons, FATF has recommended that each country criminalizes the financing of terrorism, terrorist acts and terrorist organizations, and designates such offenses as predicate offenses of money laundering. Finally, FATF has stated that the nine Special Recommendations combined with The Forty Recommendations on money laundering constitute the basic framework for preventing, detecting and suppressing both money laundering and terrorist financing.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved in terrorist financing may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to persons/organizations (e.g. foundations or charities) to support terrorist activities.

1.6 The reason of committing Money Laundering

Criminals engage in money laundering for three main reasons:

First, money represents the lifeblood of the organization that engages in criminal conduct for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

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.

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.

1.7 The reason of committing Terrorism Financing

Terrorism financing is done mainly to facilitate an extremist group by providing financial support aiming to establish or circulate their ideology. Such financial assistance may be provided directly or indirectly or may be attempted and amount of money may be significantly low with several in numbers.

1.8 Why we must combat Money Laundering

1.8.1 Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a process 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.

1.8.2 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. 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.

1.8.3 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 crises. The loss of credibility and

investor confidence can bring the potential of destabilizing financial systems, particularly in smaller economies.

1.8.4 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.

1.8.5 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.

1.8.6 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.

1.8.7 The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing of officials and governments 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.

1.8.8 Nations cannot afford to have their reputations and financial institutions tarnished by an association with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions and the underlying criminal activity, such as fraud, counterfeiting, narcotics

trafficking, and corruption, weaken the reputation and standing of any financial institution. Actions by banks to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A bank tainted by money laundering accusations from regulators, law enforcement agencies, or the press risk likely prosecution, the loss of their good market reputation, and damaging the reputation of the country. It is very difficult and requires significant resources to rectify a problem that could be prevented with proper anti-money-laundering controls.

1.8.9 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, this Guideline was drawn up.

1.9 Stages of Money Laundering

1.9.1 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.

1.9.2 Despite the variety of methods employed, the laundering is not a single act but a process accomplished in 3 basic stages which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity –

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.

1.9.3 The three basic steps may occur as separate and distinct phases. 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.

1.10 Vulnerabilities of the Financial System to Money Laundering

1.10.1 Money laundering is often thought to be associated solely with banks and moneychangers. But in reality financial institutions, both banks and non-banks, including capital market intermediaries, are susceptible to money laundering activities. Whilst the traditional capital market investment do offer a vital laundering mechanism, particularly in the initial conversion of cash to stock. Capital market investments schemes are one of the most attractive vehicles to the launderer.

1.10.2 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.

1.10.3 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 Client, and devise their procedures with due regard to that risk.

1.10.4 *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.

1.10.5 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.

1.10.6 Electronic funds transfer systems increase the vulnerability by enabling the purchase of securities to be switched rapidly between accounts in different names and different jurisdictions.

1.10.7 However, in addition, banks and non-banking financial institutions including capital market intermediaries, as providers of a wide range of services in buying and selling of securities, are vulnerable to being used in the layering and integration stages.

1.10.8 Some banks and non-banking financial institutions including capital market intermediaries may additionally be susceptible to the attention of the more sophisticated criminal organizations and “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.

1.10.9 Investment and merchant banking businesses are less likely than banks and money changers to be at risk during the initial placement stage. Because in most cases large fund cannot be deposited directly to the CMI; funds comes through a bank or other financial institutions.

1.10.10 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.

1.10.11 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 nontraditional banking products and services are not exploited.

1.10.12 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.

1.10.13 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.

1.10.14 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.

1.10.15 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.

1.10.16 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.

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

1.11 How Financial Institutions Can Combat ML/TF

1.11.1 The prevention of laundering the proceeds of crime has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of preventing and deterring money laundering is a sound knowledge of a Client's business and pattern of financial transactions and commitments. The adoption of procedures by which Banks and other Financial Institutions "know their Client" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering.

1.11.2 Thus efforts to combat money laundering largely focus on those points in the process where the launderer'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.

1.11.3 Institutions and intermediaries 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.

1.11.4 In complying with the requirements of the Act and in following this Guideline, financial institutions including capital market intermediaries should at all times pay particular attention to the fundamental principle of good business practice - 'know your Client'. Having a sound knowledge of a Client's business and pattern of financial transactions and commitments is one of the best methods by which financial institutions and their staff will be able to recognize attempts of money laundering.

Chapter: Two

Vulnerabilities of ML/TF in Capital Market

2.1 Introduction

Criminals and terrorists succeed largely in concealing the origins or sources of their funds and sanitize the proceeds of crime by moving them through national and international financial systems. Money laundering and the financing of terrorism have particularly significant economic and social consequences for a developing country like Bangladesh. The absence of, or a lax in AML/CFT regime in a particular country encourages criminals and terrorists to operate and expand their criminal pursuits fostering illegal activities such as corruption, drug traf-ficking, illicit trafficking and exploitation of human beings, arms trafficking, smuggling etc.

Asia Pacific Group on Money Laundering (APG) has identified several vulnerable sectors including capital market in Bangladesh during their Mutual Evaluation in 2008. APG suggested that Bangladesh should include Capital Market Intermediaries (CMI) in the AML/CFT regime. To comply with the Mutual Evaluation Recommendations, Bangladesh Government has incorporated CMI as reporting agency. Insider Trading and Market Manipulation are also been included as Predicate Offences under section 2 of Money Laundering Prevention Act, 2009, by the power conferred within that legislation on 30 September, 2010.

Afterwards, the Government amended Money Laundering Prevention Act, 2009 and enacted Money Laundering Prevention Act, 2012 (MLPA, 2012). MLPA, 2012, includes CMI, such as stock dealer and stock broker, portfolio manager and merchant banker, securities custodian and asset managers as reporting agencies. The MLPA, 2012 also include insider trading and market manipulation (Using the price sensitive information relating to the capital market in share transactions before it is published before the general public to take advantage of the market and attempting to manipulate the market for personal or institutional gain)-as predicate offences for money laundering.

2.2 Vulnerabilities Associated with Particular Types of Securities Products

The securities products can be utilized in the layering and integration stages of money laundering once illicit assets are placed in the financial system. However, the securities industry is relatively inhospitable to the placement of illicit assets

into the financial system. Nevertheless certain securities products do pose identifiable ML/TF vulnerabilities even at the placement stage. As in Bangladesh, illicit proceed may directly be placed for buying securities. This section focuses on the vulnerabilities of some specific types of securities products that may pose significant risk of ML/TF.

2.2.1 Broker-dealers

One of the most active participants in the securities market is the brokers or dealers in securities. A broker typically acts as an agent for an investor, and enters the securities markets on behalf of an investor to buy or sell a security. In this buying and selling process, some dealers provide liquidity to the capital market by its own capacity of buying and selling.

A specific vulnerability associated with broker-dealers is their reliance on another financial institution's CDD/KYC process. A broker-dealer might assume that, because another financial institution has opened an account for a Client, so the Client does not pose ML/TF risks for them. The CDD/KYC vulnerability is most problematic in relation to the funding of a securities account. If illicit assets are successfully placed at a depository institution, the broker-dealer may assume that, because the funds are from an institution which is subject to AML/CFT rules, the Client does not pose a ML/TF risk and therefore will accept cheques from that institution to fund a securities account. Once a securities account is funded, a Client can engage in a number of transactions that further conceal the source of his or her illicit funds, thereby successfully layering and integrating illicit assets that were placed through a depository institution. Important note is that, it is the responsibility of each institution to ensure that proper CDD process has been completed.

2.2.2 Asset Managers, Custodian and Portfolio Managers

Brokers and dealers in securities can be distinguished from those securities intermediaries that are regulated as asset manager, custodian and portfolio managers. The role of a broker and a dealer are clearly delineated from those of custodian or managers. In fact, different registration and regulatory standards may apply for them. Nonetheless,

functions can be housed in the same entity by means of multiple registrations. Such advisory functions and broker-dealer functions may be conducted under the same registration.

Role of the asset manager, custodian and portfolio manager is generally to advise on the composition of an investment portfolio or to hold securities of local or foreign clients or to manage the contents of investment accounts for retail or institutional Clients respectively.

Portfolio management typically involves the provision of financial services in a managed relationship with Clients who are often of high net worth. The value and complexity of products offered to high net worth Clients, together with the international nature of the business, make the provision of wealth management services potentially attractive to money launderers, to disguise their illicit assets. The custodian services, regardless the nationality of an investor, has same potential to money launderer as portfolio management and asset management services.

2.2.3 Trust, Nominee, and Omnibus accounts

Trust and nominee accounts present ML/TF vulnerabilities in the layering and integration stages. A particular risk involves if there is no requirement of collection of beneficial ownership information for individuals. As with shell companies or a front individual, a lack of beneficial ownership information regarding the individuals who benefit from the account may mask an individual's identity such that he or she would gain access to a financial system when such access would otherwise be restricted or forbidden.

An omnibus account is an account established for an entity that is acting as an intermediary on behalf of multiple individuals or entities. For example, a bank in jurisdiction X, on behalf of his several clients, could open an account with a securities intermediary in jurisdiction Y with its own name. In this scenario, the ML/TF vulnerability is that the securities intermediary only knows bank in jurisdiction X but they have no idea about the underlying clients of that bank. Accordingly when a CMI opens a bank account with its own name (pooled account) in a bank, then the accumulated fund of all Clients got the identity of CMI.

2.2.4 Shell Companies

The term “shell company” often refers to a non-publicly traded corporation or limited liability company that might have no physical presence and generates little or no independent economic value. These companies are commonly organized in a way that makes their ownership and transaction information easier to conceal. Thus, transactions involving shell companies present a high ML/TF vulnerability.

Whilst publicly traded shell companies can be used for illicit purposes, ML/TF vulnerabilities associated with shell companies are heightened when the company is privately held, such that beneficial ownership can be more readily obscured. For example, a domestic or international shell company securities account can be used to evade CDD/KYC investigations regarding the beneficial owners of certain assets. In particular, individuals or entities in high-risk areas/jurisdictions or conflict zones can disguise their true identities through a series of shell companies located in various jurisdictions to participate in a financial system that they otherwise would not be able to access.

Shell companies can also be used to introduce illicit funds into a financial system and/or generate illicit funds through manipulative or fraudulent securities activities. For example, a brokerage account can be opened in the name of shell companies and used to engage in fraudulent conduct with regard to low priced, illiquid, low volume or privately placed securities. In addition, a shell company can be established to accept payments from criminal organizations for non-existent services. These payments, which appear legitimate, can be deposited into depository or brokerage accounts and used to purchase securities products that are easily transferable or redeemable.

2.2.5 Margin Trading

One of the unique characteristics of the securities industry is that it can be used to both disguise the proceeds of criminal activity and to generate further profits. The use of margin account trading involves the investor borrowing funds to carry out trading. The securities themselves are used as collateral for the loan. By influencing the timing and value of trades

(and leverage), a launderer can potentially use the proceeds of a scheme to generate more funds.

2.2.6 Transfer Pricing

Large capitalization stocks are subject to a high degree of transparency and, subject to general market forces, generally fluctuate within an established price band. It is noted, however, that the market price on small capitalization stocks, which may be rarely traded, can be subject to more extreme price movements. In addition, the price of such an illiquid stock may be substantially affected by relatively small transactions. This mechanism has been exploited for money laundering purposes where block trades of illiquid stocks are transacted at a pre-agreed price between two parties. In such transactions, parties agree to the initial purchase of an illiquid security at an artificially low price with the same security being bought back some time later by the original seller or an associate at a significantly higher price.

2.2.7 Cheques

Cheques can be used to fund securities account with a securities intermediary. In addition, the use of cheques is not limited to those drawn from a depository account, but also can involve pay order/bank draft.

Money launderers can purchase pay orders/bank draft, pay order with cash over a period of time or through a series of transactions in order to avoid threshold currency reporting requirements. These cheques can then be deposited into securities accounts until a desired amount is reached and used to purchase a security, which is then sold or transferred.

Cheques from a depository account also present ML/TF vulnerability because they may unreasonably affect the securities intermediary's risk analysis, in particular with respect to CDD/KYC obligations. For example, if a cheque originates from another financial institution subject to an AML/CFT regulatory regime, a securities firm may not conduct a thorough CDD/KYC investigation because it believes that the originating financial institution has already conducted its own CDD/KYC investigation, or

because the firm perceives a reduced risk because the Client was able to open an account at another financial institution. This vulnerability can become systemic if numerous securities intermediaries perceive a reduced risk based on the activities of others.

In addition, even if the financial institution from which the cheque originated has conducted thorough CDD/KYC and not detected anything suspicious, there may still be an ML/TF risk that the securities intermediary, through its own knowledge of the investor, may be in a unique position to identify. In particular, CDD/KYC not only involves mere Client identification but establishing the purpose and intended nature of the business relationship.

Another vulnerability identified is the increasing use of the securities industry in offshore jurisdictions by criminals attempting to avoid domestic seizure of their assets. The ease by with which funds could be transferred electronically facilitates this. The use of this method of disguising funds has resulted in a reduction in the effectiveness of domestic seizure/forfeiture actions, marking a change in the laundering techniques used by criminals. The advantage of this method over, for example, the purchase of domestic real estate is that it is more difficult for law enforcement to trace and seize assets held offshore.

2.2.8 Low Priced Securities and Private Placement

Low priced securities refer to low-value equity interests in companies that are publicly traded or are about to become so. The issuers of these shares generally have legitimate business operations and revenue streams. However, some publicly traded low priced securities are really shell companies that may be used for a reverse merger. In any event, shares in these issuers will often be represented with physical securities that can be deposited with a securities intermediary. These shares are not likely to be traded on traditional exchanges, but rather in over-the-counter ("OTC") markets or on bulletin boards. Such stocks typically have very low trading volume but, unlike bearer securities, ownership of these shares will often be registered with the issuer and/or a transfer agent.

The ML/TF vulnerabilities posed by these securities are two-fold. First, these types of securities are often used to generate illicit assets through

market manipulation, insider trading, and fraud. Illicit actors can either use existing shares that are already publicly traded, or start a shell company for the express purpose of engaging in those illicit activities. In addition, criminal organizations have also been known to use illicit assets generated outside the securities industry to engage in market manipulation and fraud.

Second, these securities can be acquired by investing illicit assets into a company that is about to become public. Once the company goes public, the money launderer can sell his or her stake, thereby giving funds the appearance of having been derived from a legitimate securities transaction. Moreover, criminal organizations can also initially invest in a private company that they can then use as a front company for comingling illicit and legitimate assets. They can then take this company public through an offering in the public securities markets, thus creating what appear to be legitimate offering revenues. Alternatively, criminal organizations can acquire a publicly traded company and use it to launder illicit assets.

2.2.9 Short selling

In the securities industry short selling generally involves the practice of selling securities that are not actually owned by the seller, or that will be borrowed for delivery. In a "naked" short sale, the seller does not borrow or arrange to borrow the securities in time to make delivery to the buyer within the standard settlement period. The investment strategy behind short selling is the hope that a profit will be made from the difference in price of the assets sold and those purchased (at a lower price) for return to the borrower.

Short selling (where not approved) is a trading vehicle that can be linked to market manipulation or insider trading, which are both predicate offences that could be the basis for ML/TF.

2.2.10 Insider trading

Insider trading involves situations where the person who buys and sells securities, whether a company insider or not, does so in violation of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. This includes situations where a person in possession of material, non-public

information provides this information to someone else for trading where, depending on the circumstances, the recipient of the information can violate insider trading laws as well.

Insider trading is unique to the securities industry and generates illicit assets. As a predicate offence for money laundering this type of misconduct is reportable as STR and has proven useful in assisting law enforcement and regulators prosecute such misconduct.

The illicit assets generated by insider trading can be laundered through the securities industry itself or through other parts of the financial sector. The most common example of laundering would be the simple transfer of illicit proceeds to a bank account.

2.2.11 Market Manipulation

Market manipulation generally refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In particular, the manipulator's purpose is to drive the price of a security up or down in order to profit from price differentials. There are a number of methods that manipulators use to achieve these results.

The most pervasive market manipulation method involves what is colloquially referred to as a "pump-and-dump" scheme. This scheme involves touting a company's stock with false or misleading statements, often in conjunction with securities trades that raise the price of the security or make it appear as if the securities trading volume is higher than it actually is. Therefore the security price is artificially raised ("pumped"); the security is then sold ("dumped") for a profit. Often the underlying security is low priced, illiquid, and trades with little volume. Another most used method is circular trading. In this mechanism a group of syndicated persons manipulate share price by buying the selling of share at their own from different corner at their predetermined price.

2.2.12 Securities Fraud

Securities fraud broadly refers to deceptive practices in connection with the buy and sale of securities. In this regard, securities fraud encompasses insider trading and market manipulation activities and poses significant ML/TF risks for the CMI.

2.3 The Benefits of an Effective AML/CFT Framework

A strong AML/CFT institutional framework that includes a broad scope of predicate offenses for money laundering helps to fight against crime and corruption. An effective AML/CFT regime is deterrent to criminal activities related to capital market (e.g. Insider Trading, Market Manipulation, Securities Fraud etc.). In this regard, confiscation and forfeiture of money laundering proceeds impedes to earn profits from criminal activities, thereby reducing the incentive to commit criminal acts.

In addition, an effective AML/CFT regime reduces the possibilities of losses to the institutions originating from fraudulent activities. Proper Client identification procedures and determination of beneficial ownership provide specific due diligence for higher risk policies and ensure monitoring for suspicious activities. Such prudential internal controls play a vital role for the safe and sound operation of a financial institution. This enhances public confidence and permits investments in the capital market to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.

Chapter: Three

Requirements of Law

3.1 Compliance Requirements under the Laws

In Bangladesh, compliance requirements for CMI, as reporting agency, are based on Money Laundering Prevention Act (MLPA), 2012, Anti terrorism Act (ATA), 2009 (including amendment of 2012) and circulars or instructions issued by BFIU.

According to section 25 (1) of MLPA, 2012 CMI's responsibilities to prevent money laundering are -

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

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

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

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

According to section 16 of Anti Terrorism Act, 2009 (including amendment of 2012), CMI's responsibilities to combat financing of terrorism are -

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

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

3.2 Supervisory Power of Bangladesh Bank

According to the provision laid down in the section 23 of MLPA, 2012 and section 15 of Anti Terrorism Act, 2009 (including amendment of 2012) Bangladesh Bank is the core implementing agency.

- **Powers under MLPA, 2012:**

Under section 23 of MLPA, 2012, Bangladesh Bank shall have the following powers and responsibilities to prevent money laundering and to resist any such activities:

a) to analyze or review information related to cash transactions and suspicious transactions received from any reporting organization and to collect additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data on the same and, as the case may be, provide with the said information to the relevant law enforcement agencies for taking necessary actions;

b) ask for any information or obtain a report from reporting organizations with regard to any transaction in which there are reasonable grounds to believe that the transaction is involved in money laundering or a predicate offence;

c) issue an order to any reporting organization to suspend or freeze transactions of any account for a period not exceeding 30 (thirty) days if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence;

Provided that such order may be extended for additional period of a maximum of 6 (six) months by 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;

d) issue, from time to time, any direction necessary for the prevention of money laundering to the reporting organizations;

e) monitor whether the reporting organizations have properly submitted information and reports requested by Bangladesh Bank and whether they have duly complied with the directions issued by it, and where necessary, carry out on-site inspections of the reporting organizations to ascertain the same;

f) arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by Bangladesh Bank;

g) carry out any other functions necessary for the purposes of this Act.

- **Powers under ATA,2009 (including amendment of 2012):**

The power and responsibilities of Bangladesh Bank under section 15(1) of Anti Terrorism Act, 2009 (including amendment of 2012) are as follows:

1) Bangladesh Bank may take necessary steps to prevent and identify any transaction carried out by any reporting agency with intent to commit an offence under this Act and for this purpose it shall have the following powers and authority, namely:-

(a) to call for a report relating to any suspicious transaction from any reporting agency;

(b) to provide the reports received in accordance with sub-clause (a) to the respective law enforcement agencies for taking necessary steps or, as the case may be, provide them to foreign law enforcement agencies upon their request or exchange information relating to the reports;

(c) to collect and preserve all statistics and records;

(d) to create and maintain a database containing the reports of all suspicious transactions;

(e) to analyze reports relating to suspicious transactions;

(f) if there are reasonable grounds to suspect that a transaction is connected to terrorist activities, to issue an written order to the respective reporting agency to suspend or freeze transactions of that relevant account for a period not exceeding 30 (thirty) days and, if it appears necessary to reveal correct information relating to transactions of the said account, such suspension or freezing order may be extended for an additional term not exceeding 6 (six) months by 30 (thirty) days at a time;

(g) to monitor and supervise the activities of reporting agency;

(h) to give directions to the reporting agencies to take preventive steps to prevent financing of terrorist activities;

(i) to inspect the reporting agencies for the purpose of identification of suspicious transactions connected with financing of terrorist activities; and

(j) to provide training to officers and employees of the reporting agencies for the purpose of identification and prevention of suspicious transactions connected with financing of terrorist activities.

(2) Bangladesh Bank, on identification of a reporting agency or its Client 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 facilitate their inquiries and investigations into the matter.

(3) If the trial of any offence committed in another country is pending, Bangladesh Bank shall take steps to seize the accounts of any person or entity pursuant to any international, regional or bilateral agreement, United Nations conventions ratified by the Government of Bangladesh or respective resolutions of the United Nations Security Council.

(4) The fund seized under sub-section (3) shall be subject to disposal by the concerned court pursuant to the concerned agreements,

conventions or resolutions adopted by the United Nations Security Council.

(5) In order to dispose of the responsibilities mentioned in sub-sections (1) to (3), governmental, semi-governmental, autonomous bodies shall provide requested information or, as the case may be, spontaneously provide information to the Bangladesh Financial Intelligence Unit.

(6) The Bangladesh Financial Intelligence Unit shall, on demand or, as the cases may be, spontaneously provide information relating to terrorist activities or financing of terrorist activities to financial intelligence units of other countries.

(7) For the purpose of investigation relating to financing of terrorist activities, the law enforcement agencies shall have the right to access any document or file of any bank under the following conditions:

(a) with an order from a competent court or tribunal; or
(b) with the approval of the Bangladesh Bank.

3.3 Penalties under MLPA, 2012:

According to section 25 (2) of MLPA, 2012, if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of MLPA, 2012, Bangladesh Bank may-

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

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

In addition to the above mentioned provisions there are some other provisions of penalties in the section 23 of MLPA, 2012. These are:

(3) If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.

(4) If any reporting organization provides with false information or statement requested under this section, Bangladesh Bank may impose a fine on such organization not less than Taka 20 (twenty) thousand but not exceeding Taka 5 (five) lacs and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the said organization.

(5) If any reporting organization fails to comply with any instruction given by Bangladesh Bank under this Act, Bangladesh Bank may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day for each of such non compliance and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant

authority may take appropriate measures against the said organization.

(6) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Bank under clause (c) of sub-section 23(1) of MLPA, 2012, Bangladesh Bank may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

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

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

3.4 Penalties under ATA, 2009 (including amendment of 2012):

The provision laid down in section 16 (3) of Anti Terrorism (Amendment) Act, 2012, if any reporting agency fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against

the agency. According to section 16 (4) if any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section 16 (3) of ATA, Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained in any bank or financial institution or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

Chapter: Four

AML/CFT policies and Organizational Structures for CMI

This section describes about various policies and organizational structure for Capital Market Intermediaries (CMI) with specific responsibility for specific individuals to prevent money laundering and combat financing of terrorism in line with the Money Laundering Prevention Act, 2012 and Anti Terrorism Act, 2009 (including amendment of 2012). This section highlights the roles and responsibilities of CMI to mitigate ML/TF risks and enable them to alleviate such risks in an appropriate manner.

4.1Senior Management Commitment

4.1.1 The senior management, including the Managing Director, the Board of Directors, Managers, whatever they may be called, of the CMI should be committed to the development and enforcement of the AML/CFT programs/strategies. ***Such programs/strategies should be drafted by following this Guideline and submitted to the BFIU within 03 (three) months from the date of issuance.***

4.1.2 The CMI Management should take necessary measures to assess and identify ML/TF risk related with CMI and should have in place an appropriate mechanism to mitigate those risks.

4.1.3 The CMI should establish an **"AML/CFT Compliance Unit"** headed by sufficiently senior official who will directly report to the CEO/MD.

4.1.4 The CMI Management should issue a policy/guidance to its all staff's to be cautious for preventing money laundering and terrorist financing. The policy/guidance will be written, approved by the Board of Directors. MD/CEO should also circulate this to its entire staff which includes:

- A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.

- A statement that all activities carried on by the CMI must comply with applicable governing laws and regulations.

- A statement that complying with rules and regulations is the responsibility of each individual in the CMI 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.

- A statement that employees will be held accountable for carrying out their compliance responsibilities.

4.2 Organizational Structure

The CMI should constitute an "AML/CFT Compliance Unit" **headed by maximum one/two tiers below than the MD/CEO** and Head of this unit shall directly report the MD/CEO. The head of other separate divisions (where applicable) may be member of AML/CFT Compliance Unit. ***Each CMI will establish an*** "AML/CFT Compliance Unit" ***and notify BFIU within 03 (three) months from the date of issuance of this Guideline*****.**

4.2.1 Functions of AML/CFT compliance unit:

- The AML/CFT compliance unit will assess the various types of ML/TF risk e.g. product risk, service risk, customer risk, country risk, and establish necessary measures for preventing those risks.

- It will review the AML/CFT policies regularly considering the risk based approach.

- It will update the legal, regulatory, business or operational changes including AML/CFT rules or regulations as and when required but at least once a year.

- It will implement the necessary AML/CFT policies, procedures and controls so as to deter criminals from adopting various techniques of ML/TF using their business services.

- It will supervise the implementation of necessary measures for preventing ML/TF risk and assess the effectiveness of applied measures.

- It will arrange necessary training for its staff.

- It will ensure that necessary steps are taken to identify suspicious transaction and report the same to the BFIU directly.

- It will place Memorandum (Assessment Report) before the Board of Directors/Appropriate Authority **half yearly basis** regarding the status of the AML/CFT initiatives undertaken by the CMI. ***(Sample format given in annexure-3)***

4.2.3 Functions of Head of AML/CFT Compliance Unit:

- circulate BFIU circulars/instructions of BFIU and Policy Guidelines to the branches and concern offices.

- monitor, review and coordinate, implement and enforces CMI's AML/CFT Compliance Policies

- formulate the policy of identification procedure "Know your Client (KYC)" for detecting of suspicious transactions / account activities in line with the Circulars/Guidelines issued by BFIU, Bangladesh Bank.

- respond queries of the branches to money laundering and terrorist financing apprehensions.

- report to the BFIU, Bangladesh Bank regarding suspicious transactions/activities of the Clients.

- issue necessary instructions to the branches.

- ensure timely reporting of STR/SAR and compliance to the BFIU instructions.

- extend all sorts of cooperation to Internal Audit Team, BFIU Inspection Team and other Law enforcing Agencies as and when required and appropriate.

- ***Assess the number of legacy accounts as describe in section 5.7 of this Guideline, prepare an Action Plan to update those legacy account within the stipulated time frame mentioned in this Guideline and submit this Action Plan to the BFIU (format-1 given in Annexure-4).***

- ***Monitor the progress of the Action Plan and report quarterly to the BFIU accurately (format-2 given in Annexure-4).***

4.2.3 Functions of Branch / Unit Head:

- The Branch/Unit head will ensure that the AML/CFT issues are in place in their branch/unit and the respective law, BFIU circulars and instructions are meticulously followed at all level.

- S/he will be responsible for educating and updating the officers of the branch regarding AML/CFT issues, circulars and strategies

- S/he will ensure that STR identification and reporting system is effectively in place within the branch/unit.

- In the monthly meeting of the Branch the AML/CFT agenda will come as an important one and the proceedings shall be recorded properly.

- In case of new accounts s/he shall ensure that the policy and identification procedure "Know your Client (KYC)" have been meticulously followed.

- S/he will ensure the preservation of complete and up-to-date account records of the Clients.

- S/he will ensure the periodical reporting of AML/CFT issues.

- S/he will report the unusual/suspected transactions to AML/CFT compliance unit for further advice and guidance.

- S/he will extend all sorts of cooperation to Internal Audit Team, BFIU Inspection Team and other Law enforcing Agencies as and when required and appropriate.

- S/he will consider any negative information from any sources, regarding the clients, as a matter of suspicion.

- S/he will play an anchor role in regard to update of legacy accounts and assessment functions.

4.2.5 Functions of Account Opening Officer:

- Perform due diligence on prospective clients prior to opening an account.

- Shall be vigilant regarding the identification of account holder and the suspicious activity of a prospective client while opening an account.

- Ensure all required documentation is completed satisfactorily as per this Guideline.

- In case of new accounts the concerned, s/he will follow the policy of identification procedure “Know your Client (KYC)” and analyze the track record of the existing accounts.

- Ensure that customer information are verified and undertake reviewing of customer information after a certain period

Chapter: Five

Know Your Client (KYC) Policies and Procedures

Having sufficient and verified information about client - “know your Client” (KYC) - and making use of that information underpins all AML/CFT efforts is the most effective defense against being used to launder the proceeds of crime. If a Client has established a BO (beneficial ownership) account or any related accounts using a false identity, s/he may be doing so to defraud the institution itself, or to ensure that s/he cannot be traced or linked to the crime proceeds of which the institution is being used to launder. A false name or address or date of birth will usually mean that law enforcement agencies cannot trace the client if s/he is needed for interview as part of an investigation.

Section 25 (1)(a) of the Money Laundering Prevention Act, 2012 (MLPA, 2012) requires all reporting institutions to obtain complete and correct information regarding the clients identity of those with whom they deal (referred herein this Guideline as verification of identity). ***Unless full and complete and correct information regarding the identity of potential Clients is obtained in good time, the business relationship should not be proceed.***

When a business relationship is being established, the nature of the business that the client expects to conduct with the institution 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 be able to judge whether a transaction is or is not suspicious, institutions need to have a clear understanding of the business carried on by their clients.

The CMI or its branch/unit should establish to its satisfaction that it is dealing with a person (natural or legal), and should verify the identity of persons who are authorized to operate account, or transact business on behalf of the Client.

The verification procedures needed to establish the identity of a prospective client should basically be the same whatever type of account or service is required. The best identification documents are generally those that cannot be obtain illegally or difficult to forge. ***No single piece of identification document 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 every institution must know who their clients are, and have the necessary documentary evidence to verify the identity of its client completely and correctly.

Section 25 (1)(b) of MLPA, 2012 requires that all records including the records of the verification of identity must be retained for 05 (five) years after a BO account or any related account is closed or the business relationship ended.

5.1 Client Acceptance Policy

All CMI must have a clear cut Client Acceptance Policies and procedures including a description of the types of client that are likely to pose a higher than average risk to the CMI. While formulating such policies, factors such as clients' background, public or high profile position (refer to the PEP), business activities, high risk country or other risk indicators should be considered. Such policy should incorporate the CMI will not establish a relationship with shell companies or any entity or individual designated by UN sanction committee or proscribed and scheduled by Bangladesh Government.

5.2 Client Identification

5.2.1 Client identification is an essential element of KYC standards. For the purposes of this Guideline, a client includes:

- the person or entity that maintains a BO account or related account with the CMI or those on whose behalf an account is maintained (i.e. beneficial owners);
- the beneficiaries of transactions conducted by professional intermediaries or receivers of financial services provided by the CMI; and
- any person or entity connected with a financial services/transactions who can pose a significant reputational or other risk to the CMI.

5.2.2 ***No BO or related account will be opened in fictitious/false or anonymous name.*** That's why the client 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 CMI to undertake regular reviews of

existing records. An appropriate time to do so is when a significant transaction takes place, or when status of a client change substantially, or when there is a material change in the way of the BO account or related account is operated. However, if a branch/unit becomes aware at any time that it lacks sufficient information about an existing client, it should take steps to ensure that all relevant information is obtained as quickly as possible.

5.2.3 Whenever the opening of a BO account or other business relationship is being considered, identification procedures must be followed. Identity must also be verified in all cases by applying appropriate measures.

5.2.4 Once verification of identity has been satisfactorily completed, no further evidence is needed then transactions may be undertaken. Records must be maintained as set out Section 25 of MLPA, 2012, and information should be updated or reviewed as appropriate.

5.2.5 Identity generally means a set of attributes which uniquely define a natural or legal person. For the purposes of this guideline, the three elements which constitutes the identity of client are:

- the physical identity (e.g. name, date of birth, fathers/mothers/spouse name, address etc.);
- Documentary proof for physical identity (TIN, National ID, employer ID, Passport, Driving License, etc.); and
- the activity undertaken (relationship with client).

5.2.6 ***When a CMI acts as a Trustee, Custodian, Issue Manager, Portfolio Manager, Asset Manager or any other service providing role, it must meticulously follow the relevant Securities and Exchange Commission Rules. Apart from that CMI also need to follow identification procedures, mentioned in this Guideline, during providing such services to the individual or corporate Client. Any sort of inconsistency of the relevant document(s) should be considered a trigger for suspicion and reporting.***

5.2.7 ***In case of providing custodian services through correspondent bank, the CMI must collect a written letter from the correspondent bank that KYC has been completed for these underlying clients, with a commitment to provide information as and when necessary.***

5.2.8 ***A CMI should collect the detail information on client's professions, sources of fund and other personal information, as per their satisfaction, in the light of the risk associated with the client*.**

5.3 Individual clients

5.3.1 Where verification of identity is required, the following information should be obtained from all individual applicants for opening accounts or other relationships, and **should be independently verified by the institution itself**:

- Name and/or names used;
- Name of the spouse;
- parent's names;
- date of birth;
- current and permanent address;
- details of occupation/employment; and
- sources of income/fund

5.3.2 One or more of the following steps is recommended 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 should be examined);
- checking the National ID database (if possible);
- checking the telephone directory;
- physical visit to home/office.
- Mailing thanks letter etc.

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

5.3.3 The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard.

5.3.4 Identification documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:

- Valid passport;
- Valid driving license;
- National ID Card;
- Employers ID card;
- A Bangladeshi employer ID card bearing the photograph and signature of the applicant; or
- A certificate from any local government organs such as Union Council chairman, Ward Commissioner, etc. or any respectable person acceptable to the CMI.
- Any other identification documents with photograph, which is acceptable to the CMI.

5.3.5 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, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible.

5.3.6 ***Generally a CMI should not open a BO or related account of a non face-to-face Client.*** With some exceptions, where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the Client 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.

5.3.7 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.

5.3.8 Any subsequent change to the client's name, address, or employment details of which the CMI becomes aware should be verified and recorded as part of the Know Your Client process.

5.3.9 File copies of supporting evidence should be retained. The relevant details should be recorded on the applicant's file.

5.3.10 An introduction from a respected existing client personally known to the management, or from a staff, may assist the verification procedure but does not substitute the need for verification of address as set out above. Details of the introduction/introducer information should be recorded on the client's file.

5.4 Corporate Bodies and other Entities

5.4.1. 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 CMI shall 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.

5.4.2 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, struck off or wound-up.

5.4.3 Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh.

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

5.4.5 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 the 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 20% share or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories of the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship is required. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.
- Two recent photographs of the Account operators duly attested by the company secretary/MD/CEO.
- Current and complete information of account operators.

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

5.4.7 The following persons (i.e. natural or legal persons) 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.

5.4.8 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.

5.5 Partnerships and Unincorporated Businesses

5.5.1 In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the CMI, the identity of all the partners or equivalent should be verified in line with the requirements for personal clients. 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.

5.5.2 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).

5.5.3 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.

5.6 Powers of Attorney / Nominee / Mandates to operate account

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, a CMI require undertaking KYC process and establishing the identities of holders of powers of attorney, the grantor of the power of attorney, nominee and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept properly.

5.7 Requirements in respect of accounts opened prior to 30 September 2010

5.7.1 CMI's are included as reporting agencies on 30 September, 2010 as per MLPA, 2009. So AML/CFT legislation and requirements including KYC requirements for business relationships did not apply prior to 30 September, 2010. It is therefore reasonable to assume that business relationships commenced before that date may not satisfy the requirements of these Guideline in terms of supporting documentary evidence.

5.7.2 In such circumstances, the lack of up to date documentary evidence to support existing business relationships may pose operational and other risks to the institution. The CMI must review existing business relationships with the client commenced prior to 30 September, 2010 (referred herein as "Legacy Accounts") to establish whether any documentary evidence required by their current KYC procedures is lacking. ***The review must be completed by 31 December 2015.***

5.7.3 A CMI must ensure the management of reviewing the Legacy Accounts within the stipulated time frame as mentioned above. CMI has to assess first how many legacy accounts are maintained by them. Then they will prepare an Action Plan to complete the KYC procedures of the assessed Legacy accounts within the above time frame. ***CMI should submit this Action Plan to the BFIU within 03 (three) months from the date of issuance of this Guideline and also report quarterly progress of their review as per annexed format (Annexure-4).***

5.7.4 In carrying out their review of Legacy Accounts, management must decide whether to obtain any missing elements of the documentary evidence, or to decide that, in light of the existing nature of the business relationship.

5.7.5 ***A CMI also ensure that the BO accounts that were opened after 30 September, 2010 to till date (i.e date of issuance of this Guideline), satisfy the existing KYC/CDD norms. If any of such accounts do not satisfy the KYC/CDD norms, it must be regularized within 06 (Six) months from the date of issuance of this Guideline.***

5.7.6 When reviewing the nature of a business relationship, The CMI should take into account a number of considerations, such as the length of time the relationship has been in place, the frequency with which the institution has contacted with the client, and the volumes and numbers of transactions. Such factors will help to determine whether it is necessary to update or supplement KYC documentation already held.

5.7.7 When a CMI seeking for missing documentation, the institution must do so at the earliest possible opportunity and persist until the information is received, or the original decision revised. Where missing information is not obtained within a reasonable period of time, the institution should consider termination of the business relationship

5.8 Identification of Beneficial Owners and Verification of their Identities

5.8.1 CMIs are under a duty to take steps to determine if there exists any beneficial owner of the accounts who is hiding behind the client dealing with.

Generally, the CMI should assess and determine the measures which would be appropriate to determine the beneficial owners, if any. The CMI should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

5.8.2. The CMI may also consider obtaining an undertaking or declaration from the client on the identity of, and the information relating to, the beneficial owner. This Guideline makes reference to the case where the client is a portfolio manager. In that situation, as well as other instances where the client has a *bona fide* and legitimate interest or duty not to disclose to the CMI the

identity or particulars of beneficial owners who are known to exist, the CMI may consider the application of simplified CDD.

5.8.3. It is widely recognized that it would be unnecessary to attempt to determine if beneficial owners exist in relation to the entities information would already be available. For example, in the case of publicly listed companies, the shareholders would be changing relatively frequently and there would already be disclosure obligations imposed on substantial shareholders of such companies. In the case of financial institutions supervised by the Authority, there would have been adequate disclosure of the ownership and structure to the Authority.

5.9 Reliability of Information and Documentation

5.9.1 Where the CMI obtains information or documents from the client or a third party, it should take reasonable steps to assure itself that such information or documents are reliable and where appropriate, reasonably up to date at the time they are provided to the CMI.

5.9.2. Where the client is unable to produce original documents, the CMI may consider accepting documents that are certified by qualified persons, such as lawyers and accountants or any respectable person acceptable to the CMI.

5.10 Non-Face-to-Face Verification

5.10.1 Where business relations are established or financial services are provided without face-to-face contact. In particular, a CMI should take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by clients over the internet, the post or the telephone.

5.10.2 As a guide, CMIs should take one or more of the following measures to mitigate the risk associated with not being able to have face-to-face contact when establishing business relations:

- telephone contact with the client at a residential or business number that can be verified independently;

- confirmation of the client's address through an exchange of correspondence or other appropriate method;
- subject to the client's consent, telephone confirmation of the client's employment status with the client's employer's personnel department at a listed business number of the employer;
- confirmation of the client's salary/income details by requiring the presentation of recent bank statements from a bank;
- certification of identification documents by lawyers or notary publics presented by the Client;
- requiring the client to make an initial deposit using a cheque drawn on the client's personal account with a bank; and
- any other reliable verification checks adopted by the CMI for non-face-to-face client.

5.11 Simplified Client Due Diligence

5.11.1 Simplified CDD measures are applicable in cases where the CMI is satisfied that the risk of money laundering or terrorist financing is low.

5.11.2. The CMI should assess the risks of money laundering or terrorist financing, having regard to the circumstances of each case, before applying the lesser or reduced CDD measures. Where the CMI adopts such lesser or reduced CDD measures, such measures should be commensurate with the CMI's assessment of the risks. Examples of when the CMI might adopt lesser or reduced CDD measures are:

- where reliable information on the client is publicly available to the CMI;
- the CMI is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or
- the client is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set

by the FATF, or a listed company that is subject to regulatory disclosure requirements.

5.11.3. Above paragraph makes clear the circumstances when simplified CDD measures are not permitted, namely, where the Clients are from or in countries and jurisdictions known to have inadequate AML/CFT measures, or where the CMI suspects that money laundering or terrorist financing is involved.

5.12 Identifying and Dealing with PEPs

5.12.1 As per FATF, PEPs refers

PEPs are individuals who are or have been entrusted with prominent public functions of 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 definition of PEPs is not intended to cover middle ranking or more junior individuals but it also cover the family members and/or close associates of a PEP. Another important thing is that not only client, a PEP but also may be a beneficial of an account.

5.12.2 ***PEPs accounts must be marked as High Risk accounts and consider the followings while opening and maintaining the accounts of any PEPs, A CMI must in place the following Enhanced Due Diligence (EDD):***

- have appropriate risk-management systems to determine whether the client or the beneficial owner is a politically exposed person;
- obtain senior management approval for establishing (or continuing, for existing clients) such business relationships;
- take reasonable measures to establish the source of wealth and source of funds; and
- conduct enhanced ongoing monitoring of the business relationship.

5.13 Other High Risk Categories and Enhanced Due Diligence (EDD)

5.13.1 This paragraph requires EDD measures to be applied to other categories of clients apart from PEPs, which a CMI may consider to pose a greater risk of

money laundering or terrorist financing. In assessing the risk of money laundering or terrorist financing, the CMI may take into account factors such as the type of client, the type of product that the client purchases, the geographical area of operation of the client's business and in place EDD measures for higher risk scenario.

5.13.2. CMIs are also required to give particular **attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures or under FATF Public Statement.** For this purpose, CMIs may take a range of steps, including the adoption of EDD measures similar to those for PEPs and other high risk categories.

5.14 Comply with the UN and Local Sanctions

5.14.1. While opening of a BO or related account, a CMI should in place a screening mechanism whether the name of the client (individual or entity) listed under United Nations Security Council Resolution 1267 and its successors, 1373, 1540, 1718, 1737. A CMI should also consider such local sanction list as provided by BFIU or GoB.

5.14.2 If a CMI identify any name of a prospective client mentioned the above paragraph, it should not entertain that relationship and immediately notify the matter to BFIU. If the persons or entities mentioned in the above paragraph are found as a client, a CMI should immediately freeze that account without delay and without prior notice and immediately notify BFIU.

5.15 Performance of CDD Measures by Intermediaries

5.15.1. Where a CMI wishes to rely on an intermediary to perform elements of the CDD measures, requires the CMI to be satisfied of various matters, including that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with the standards set by the FATF, and that the intermediary has measures in place to comply with the requirements.

5.15.2. The CMI may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements:

- referring to any publicly available reports or material on the quality of AML/CFT supervision in the jurisdiction where that intermediary operates (such as mutual evaluation reports of the FATF and its associate bodies, or assessment reports made under the Financial Sector Assessment Program of the International Monetary Fund and the World Bank);

- referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;

- obtaining professional advice as to the extent of AML/CFT obligations to which the intermediary is subject by the laws of the jurisdiction in which the intermediary operates;

- examining the AML/CFT laws in the jurisdiction where the intermediary operates and determining its comparability with the AML/CFT laws of Bangladesh.

5.15.3. To the extent that the performance of CDD is undertaken by the intermediary rather than by the CMI, the CMI is required to immediately obtain from the intermediary the information relating to CDD obtained by the intermediary.

5.15.4 In addition, where the CMI relies on the intermediary to undertake the performance of CDD, the CMI should be able to justify that the conditions of paragraph above have been met. The CMI should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

5.16 Review and Update

A CMI have to review all the information related with their clients that they preserved, after a certain period of time. If there any substantial changes in client's business, profession, address, status or any other things, a CMI need to update that and preserve duly.

Chapter: Six

Transaction Monitoring and Reporting Process

One of the major responsibilities of CMI under MLPA, 2012 and ATA, 2009 (including amendment of 2012) is to make the Suspicious Transaction Report (STR). The reporting of suspicious transaction is the excellent tool for mitigating AML/CFT risks. All staff's of CMI should be vigilant to detect suspicious transaction or activity done by their clients. A CMI must in place appropriate tools to detect client unusual or complex pattern of transaction. The CMI should not only consider suspicious transaction but also consider the suspicious activity or unusual behavior of the client. If they identified any unusual behavior or activity, it should also be reported.

6.1 What is Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)

6.1.1 ***Generally, STR/SAR means a formatted report of suspicious transactions/ activities where there is a reasonable ground to believe that funds are the proceeds of crime or may be linked to money laundering or terrorist financing, insider trading & market manipulation related activity or the transactions do not seem to be usual.*** Such unusual activities or transactions must be reported to competent authorities. Herein the competent authority refers to Bangladesh Financial Intelligence Unit (BFIU) as per MLPA, 2012 and ATA, 2009 (including amendment of 2012).

6.1.2 Section 2(z) of Money laundering Prevention Act, 2012 defines Suspicious Transaction as follows:

"Suspicious Transaction" means such transactions –

- That deviates from usual transactions;
- 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'
- 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.

6.1.3 Section 2(16) of ATA, 2009 (including amendment of 2012) defines Suspicious Transaction as follows:

"Suspicious Transaction" means such transaction –

(i) which is different from usual transactions;

(ii) which invokes presumption that -

(a) it is the proceeds of an offence,

(b) it finances to terrorist activities, a terrorist group or an individual terrorist;

(iii) which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act;

6.2 Obligations of STR/SAR

According to the provision laid down in the section 25(1)(d) of MLPA 2012, reporting agencies (including CMI) are obligated to submit STR/SAR to the BFIU spontaneously. This Guideline also creates an obligation for CMI to submit STR/SAR with the purview of the legislation mentioned above.

6.3 Importance of STR/SAR

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

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

6.4. How to identify a suspicious transaction

6.4.1 Transactions, whether completed or attempted, may give rise to reasonable grounds to suspect that they are related to money laundering or terrorist financing, insider trading & market manipulation related activity regardless of the sum of money involved. There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist financing offence, insider trading & market manipulation related offence. As a general guide, a transaction may be connected to money laundering or terrorist financing when it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

6.4.2 The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business and from one client to another. Evaluation of transactions should be done in terms of what seems appropriate and is within normal practices of CMI business, and based on CMI's knowledge of their client. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist financing, insider trading & market manipulation related activity. An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the client's business, financial history, background and behavior. It should be remembered that behavior is suspicious, not people. Also, it could be the consideration of many factors—not just one factor— that will lead to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering or terrorist financing, insider trading & market manipulation related offences.

6.4.3 Any transaction seems to be suspicious in terms of the nature, activity, volume, complexity etc., or significantly mismatch with client's declared information. It also depends on the prudence of concern official of CMI. If s/he does not get satisfactory answer for any unusual or suspicion, it should be reported and/or recorded. I***mportant note is that suspicion may not arise only at the time***

of transaction but also may be arised at the time of completing KYC and attempted transaction.

6.4.4 ***A CMI also need to follow the UN and the Local Sanction list.*** If a CMI identify any persons or entities, while opening account, transaction or attempted transaction taken place, listed under United Nations Security Council Resolution and 1267 and its successors, 1373, 1540, 1718, 1737, it should immediately freeze the account and report to the BFIU as early as possible.

6.5. Transaction Monitoring Tools

6.5.1 The CMI should have systems and controls in place to monitor on an ongoing basis the relevant activities of its client 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 of a CMI is to be vigilant for any significant changes or inconsistencies in the pattern of transactions or any fraudulent activities, insider trading & market manipulation activities. Inconsistency is measured against the stated original purpose of the accounts. The following areas could be monitored:

- transaction type
- frequency
- Pattern of transaction
- unusually large amounts
- geographical origin/destination
- Activity related to account
- Possible trade related to market manipulation
- Possible trade related to insider trading
- Any type of fraudulent activates

6.5.2 It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and manual solutions. All

CMI have to develop a corporate compliance culture, and properly trained, vigilant staff who will form an effective monitoring method through their day-to-day dealing with clients/transactions.

6.5.3 A CMI may also consider the list of indicators as given ***section 6.9*** of this Guideline, while detecting and reporting of STR/SAR.

6.6 Suspicious Transaction / Activity Reporting Process

6.6.1. CMI must establish written internal procedures so that, in the event of a suspicious transaction/activity being discovered, all staff is aware of the reporting chain and the procedures to follow. Such procedures should be periodically updated by AML/CFT Compliance Unit to reflect any regulatory changes.

6.6.2 ***All reports of suspicious transactions/ activities must reach to the Head of AML/CFT Compliance Unit and he should have the authority to determine whether a disclosure in accordance with the regulation is appropriate. This type of reporting may be called as "Internal reporting". Branch or the officials of CMI will use the annexed format for internal reporting (Annexure-2).*** However the Branch Manager/Unit Head can be permitted to add his comments to the suspicion report indicating any evidence as to why he/she believes the suspicion is not justified.

6.6.3 ***All reports of suspicious transaction should be filed as per the format given in the Annexure-1 or as per the circulars issued by BFIU from time to time.*** All reports to be sent to the address below:

General Manager

Bangladesh Financial Intelligence Unit (11th Floor)

Bangladesh Bank

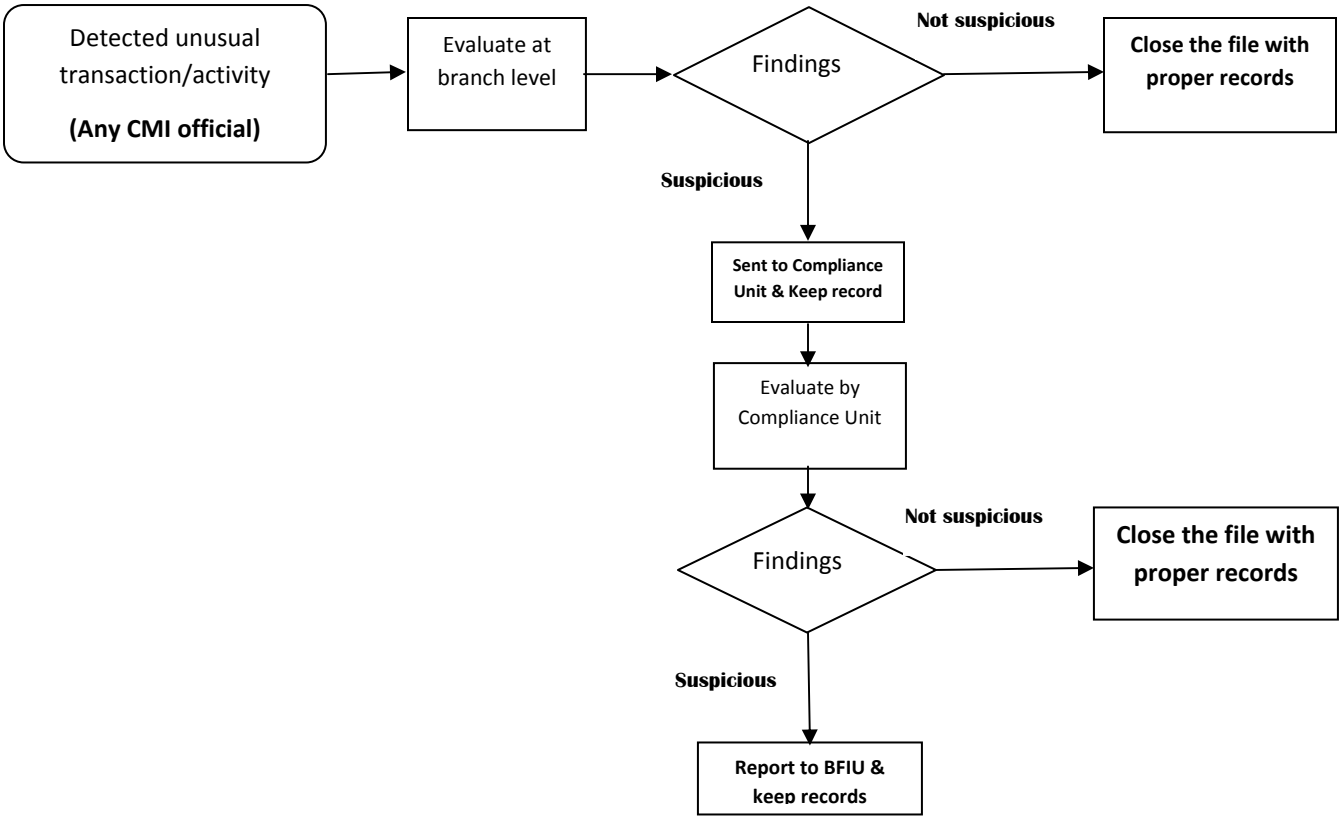
Head Office, Motijheel

Dhaka-1000

6.6.4 The CMI must keep proper records when there is an internal report for any suspicious activity or transaction or when there is any STR/SAR reported to the BFIU.

6.6.5 A CMI have to report half yearly basis to the BFIU incorporating the summary of STRs that has already been reported to BFIU by the CMI. Such report should reach to the BFIU on the 15th of next month after a completed half year by using the format given in <u>Annexure-5</u>. If any CMI, not be able to identify any STR/SAR in any quarter, the CMI still need to submit report to the BFIU as "Nil" Report for that quarter.

6.6.6 For simplification, the outlined flow chart given below shows STR/SAR identification and reporting procedures at a glance:



6.7 “Safe Harbor” provisions for reporting

MLPA, 2012 encourage CMI to report suspicious transactions/activities by protecting them and their employees from any criminal and civil suits when they report suspicious transactions/activities in good faith to competent authority i.e. BFIU. Section (28) of MLPA, 2012 provides the safe harbor for reporting. However, if the CMI fail to report STR/SAR they will be subject to punishment under section 23 (2) of MLPA, 2012.

6.8 “Tipping Off” provisions for reporting

Divulge of any information or information related to STR/SAR is strictly prohibited under section 6 of MLPA, 2012. No person of CMI will divulge 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 MLPA, 2012.

6.9 Suspicion Indicators

The following are examples of common indicators that may point to a suspicious transaction, whether completed or attempted as explained below:

- Client provides false information or information that seems unreliable.
- Client offers money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- It is observed that a client is the subject of a money laundering, terrorist financing, insider trading or market manipulation related investigation.
- It is known from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity.
- A client name listed under UN or Local sanctions list.
- A new or prospective client is known to you as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).
- Client attempts to convince employee not to complete necessary documentation required for the transaction/CDD process.
- Client makes inquiries that would indicate a desire to avoid reporting.

- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client is quick to volunteer that funds are “clean” or “not being laundered.”
- Client appears to be collaborating with others to avoid record keeping, Client identification or reporting thresholds.
- Client provides doubtful or vague information.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client refuses to produce personal identification documents.
- Client only submits copies of personal identification documents.
- Client wants to establish identity using something other than his or her personal identification documents.
- Client’s supporting documentation lacks important details such as a phone number.
- Client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Client presents different identification documents at different times.
- Client alters the transaction after being asked for identity documents.
- Client presents different identification documents each time a transaction is conducted.
- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the Client or his/her financial ability.
- Any dealing with a third party when the identity of the beneficiary or counterparty is undisclosed.
- Client attempts to purchase investments with cash.
- Client admits or makes statements about involvement in criminal activities.
- Client does not want correspondence sent to home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client repeatedly uses an address but frequently changes the names involved.
- Client shows uncommon curiosity about internal systems, controls and policies.

- Client presents confusing details about the transaction or knows few details about its purpose.
- Client appears to informally record large volume transactions, using unconventional bookkeeping methods or “off-the-record” books.
- Client over justifies or explains the transaction.
- Client is secretive and reluctant to meet in person.
- Client is nervous, not in keeping with the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client’s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact Client shortly after opening account.
- Normal attempts to verify the background of a new or prospective Client are difficult.
- Client appears to be acting on behalf of a third party, but does not tell you.
- Client insists that a transaction be done quickly.
- Inconsistencies appear in the Client’s presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the Client.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client uses aliases and a variety of similar but different addresses.
- Client spells his or her name differently from one transaction to another.
- Client uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the Client or their financial ability.
- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the Client.
- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the Client.
- Client makes large or unusual settlements of securities in cash.

- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the Client.
- Several Clients open accounts within a short period of time to trade the same stock.
- Client is an institutional trader that trades large blocks of low priced securities on behalf of an unidentified party.
- Unrelated Clients redirect funds toward the same account.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large size which may manipulate stock price.
- All principals of Client are located outside of Bangladesh.
- Client attempts to purchase investments with instruments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the Client.
- Transactions made by employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which Clients make settlements with cheques drawn by or remittances from, third parties.
- Unusually large amounts of securities or stock certificates in the names of individuals other than the Client.
- Client maintains bank accounts and custodian or brokerage accounts at offshore banking centers with no explanation by Client as to the purpose for such relationships.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money laundering system.

Chapter: Seven

Other requirements for CMI

7.1 Training and awareness

7.1.1 Section 23 (1)(f) of the MLPA, 2012, requires BFIU, Bangladesh Bank to provide training to the staff/officers of all reporting agencies and stakeholders including CMI. CMI will also take necessary actions to train up 100% of its staff.

7.1.2 All relevant staff should be educated in the process of the "Know Your Client" requirements for AML/CFT purposes. The training in this respect should cover not only the need to know the true identity of the client but also, where a business relationship is being established, the need to know enough about the type of business activities of the client what might constitute suspicious activity. Relevant staff should be equipped to identify any change in the pattern of a client's transactions or circumstances that might constitute criminal activity.

7.1.3 Some form of high-level general awareness raising training program is therefore suggested for high level Management.

7.1.4 A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Head of AML/CFT Compliance Unit will be provided to all new employees who are likely to be dealing with clients or their transactions, irrespective of the level of seniority. They should be made aware of the importance of the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a statutory obligation to do so.

7.1.5 Training will have to be tailored to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities.

7.2 Recruitment

All CMI must in place a rigorous recruitment procedure to select the proper and skilled staff. During the screening process all CMI should complete back ground checking of its prospective staff.

7.3 Record Keeping Obligations

All CMI must preserve any type of records at least for five years after termination of relationship. Such records may contain as follows-

- Account opening records;
- Client identity documents;
- Accounts or transactions
- Signature cards, account operating agreements or account applications
- Certain records created in the normal course of business
- Confirmations of purchase or sale;
- Trade authorizations;
- Powers of attorney and joint account agreements; and
- All correspondence, including electronic mail, about the operation of accounts.
- Client statements
- Suspicious transaction report records
- Identification information on all records
- Identification documents
- Keeping Client identification information up to date
- Beneficial Ownership Records
- Politically Exposed Foreign Person Determination and Related Records

7.3.1 STR and Investigation Related Record Keeping

Where a CMI submits a STR to the BFIU or where it is known that a client or his transaction is under investigation, it should not destroy any records related to that client without the consent of the BFIU or conclusion of the case even though the five-year time limit may have been elapsed. To ensure the preservation of such records the CMI should maintain a register or tabular records of all investigations and inspection made by the investigating authority or 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/SAR;

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.

7.4 Self-Assessment & Independent Testing Process

The AML/CFT Compliance Unit will time to time (half yearly basis) inform CEO/Board whether the internal procedures and statutory obligations of the CMI have been properly discharged. The report should provide conclusions to three key questions:

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

The sample format of self assessment is given in ***annexure-3*** of this Guideline.

Apart from the Self Assessment (internal Assessment), A CMI will appoint an Independent Audit firm to access AML/CFT risks and effectives of the policies and procedures in place to combat such risks.

7.5 Cooperation in the investigation process

Any sort of non cooperation in the investigation including obstructs or declines to cooperate with any investigation officer or declines to supply information or submit a report being requested without any reasonable ground is an offence under section 7 of MLPA, 2012. So a CMI should be careful when they receive any request from appropriate investigative authority.

7.6 Exception Scheme for investment in Capital Market

7.6.1 Bangladesh Government is pleased to reduce the tax rate at ten percent for investment in share of a company or units of a mutual fund listed in any stock exchange of Bangladesh made by any class of assessee other than public limited company with income from legitimate source within the period of 1st July, 2011 to 30th June, 2012 subject to the following conditions:-

(a) A declaration related to such investment shall be submitted to the respective Deputy Commissioner of Taxes upon payment of tax at the rate of 10 percent within 15th of July, 2012 in such form as may be prescribed.

(b) The investment declared under clause (a) shall be considered as explained income for the purpose of assessment of tax;

(c) Declaration made as per clause (a) shall be accompanied by proof of payment of such tax in the form of pay order, portfolio statement in support of such investment and copy of the ledger of respective beneficiary owners (BO) account;

(d) Such invested amount shall not be withdrawn or transferred before 30th June, 2013;

(e) The benefit stipulated under this circular shall not be entitled for any income derived from any criminal activities under any other law for the time being in force;

(f) The benefit stipulated under this circular shall not be applicable for person whose tax evasion has been detected and action thereof have been initiated under section 93 of Income-tax Ordinance, 1984 on or before 30th June, 2011.

(2) The Government is pleased to rescind its Notification No S.R.O 237/Law/Income Tax dated the 6th July 2011.

7.6.2 Bangladesh Government has complied with the FATF best practices while announcing such program. The FATF best practice is based on the 04 (four) principle. A country must follow these principles while announce such tax exemption. These 04 (four) principles are as follows:

Principle 1: The effective application of AML/CFT preventative measures is a prerequisite for addressing and mitigating the money laundering and terrorist financing risks associated with implementing any type of voluntary tax compliance program.

Principle 2: The FATF Recommendations do not allow for full or partial exemptions from AML/CFT requirements in the context of implementing a voluntary tax compliance program. Therefore, when implementing a voluntary tax compliance program, national authorities should ensure that its terms do not allow, in law or in practice, for full or partial exemptions from AML/CFT requirements as set out in the FATF Recommendations. Voluntary tax compliance program which do so are in breach of the FATF Recommendations.

Principle 3: When implementing a voluntary tax compliance program, it should be ensured that all relevant domestic competent authorities be able to co-ordinate and co-operate, and exchange information, as appropriate, with a view to detecting, investigating and prosecuting any ML/FT abuse of the program.

Principle 4: The widest possible range of mutual legal assistance and exchange of information in ML/FT investigations, prosecutions and related proceedings relating to the abuse of voluntary tax compliance programs, including asset recovery investigations and proceedings, should be provided.

7.6.3 A CMI should keep in mind that any VTC program being implemented does not explicitly set out full or partial exemptions from AML/CFT requirements, or result in such exemptions in practice. This means that the VTC program is consistent with the following AML/CFT requirements, as relevant:

(a) CMI are required to conduct CDD on the client under VTC scheme who are transferring, repatriating or depositing assets under the program, as appropriate, based on an assessment of the applicable risks.

(b) CMI is required to identify the beneficial owner of the account into which the assets are being transferred, repatriated or deposited under the program.

(c) CMI should, where necessary, take reasonable measures to establish the origin of the assets being transferred, repatriated or deposited, in accordance with applicable CDD requirements.

(d) CMI are prohibited from accepting funds under the program by way of wire transfers that are not accompanied by required originator information and required beneficiary information, as required by this Guideline.

(e) CMI should keep in mind that individual or entities under such program are not exempted from reporting suspicious transactions to the BFIU.

Annexure -1

SUSPICIOUS TRANSACTION REPORT (STR)

(INDIVIDUAL/JOINT CLIENT)

A. Reporting Institution :

1. Name of the Institutions:
2. Name of the Branch:

B. Details of Report:

1. Date of sending report:
2. Is this the addition of an earlier report? Yes ☐ No ☐
3. If yes, mention the date of previous report

C. Suspect Account Details :

1. BO Account Number:
2. Folio Number/Cliant Code:
3. Name of the account:
4. Nature of the account:
(Margin/Non Margin/Portfolio/other, pls. specify)
5. Nature of ownership:
(Individual/joint/proprietorship/partnership/company/other, pls. specify)
6. Date of opening:
7. Address:

D. Account holder details (in case of Individual)**:**

1. 1. Name of the account holder:
   2. Address:
   3. Profession (in details):
   4. Nationality:
   5. Other account(s) number (if any):
   6. Other business:
   7. Father's name:
   8. Mother's Name:
   9. Date of birth:
   10 Operators/ Mandate Holder information
   11. Contact: Mobile No/Email.
   12. Bank account details:
   13. TIN:
2. 1. Name of the account holder: (if joint/multiple)

2. Relation with the account holder mention in sl. no. D1	
3. Address:	
4. Profession:	
5. Nationality:	
6. Other account(s) number(if any):	
7. Other business:	
8. Father's name:	
9. Mother's Name:	
10. Date of birth:	
11. Contact: Mobile No/Email:	
11. Bank account details:	
12. TIN:	

E. Introducer Details :

1. Name of introducer:	
2. BO and Cliant Code number:	
3.Relation with account holder:	
4. Address:	
5. Date of opening:	
6. Whether introducer is active/inactive cliant	

F. Reasons for considering the transaction(s) as unusual/suspicious?

a. ☐ Identity of Clients
b. ☐ Activity in account
c. ☐ Background of Client
d. ☐ Multiple accounts
e. ☐ Nature of transaction
f. ☐ Value of transaction
g. ☐ Other reason (Pls. Specify)

_____

_____

(Mention summery of suspicion and consequence of events)
(Use separate sheet if needed)

F. Name of the associates and volume of transaction

(Mention summery of suspicion and consequence of events) *(Use separate sheet if needed)*

H. Documents to be enclosed
1. Account opening form along with submitted documents 2. KYC Profile; 3. Transaction Statement 4. Othetr supporting documents (if any)

Signature :
(Authorized officer of AML Risk Management Unit)
Name :
Designation :
Phone :
Date :

SUSPICIOUS TRANSACTION REPORT (STR)

(CORPORATE CLIENT)

A. Reporting Institution :

1. Name of the Institutions:
2. Name of the Branch:

B. Details of Report:

1. Date of sending report:
2. Is this the addition of an earlier report? Yes ☐ No ☐
3. If yes, mention the date of previous report

C. Suspect Account Details :

1. BO Account Number:
2. Folio Number/Cliant Code:
3. Name of the Legal Person:
4. Nature of the account:
(Margin/Non Margin/Portfolio/other, pls. specify)
5. Nature of ownership:
(proprietorship/partnership/company/other, pls. specify)
6. Registration No.:
7. Registration No. & Authority:
8. Address in details :
9. Contact Details:
10. List of related Directors/Partners (at least 2, with contact details) :
11. Operators/Mandate Holders information
12. Bank account details:
13. TIN:
14. BIN:

D. Reasons for considering the transaction(s) as unusual/suspicious?

a. ☐ Identity of Clients
b. ☐ Activity in account
c. ☐ Background of Client
d. ☐ Multiple accounts
e. ☐ Nature of transaction
f. ☐ Value of transaction
g. ☐ Other reason (Pls. Specify)

_____

_____

(Mention summery of suspicion and consequence of events)

E. Name of the associates and volume of transaction

(Mention summery of suspicion and consequence of events) *(Use separate sheet if needed)*

F. Documents to be enclosed
1. Account opening form along with submitted documents 2. KYC Profile; 3. Transaction Statement 4. Othetr supporting documents (if any)

Signature :
(Authorized officer of AML Risk Management Unit)
Name :
Designation :
Phone :
Date :

Annexure-2

Internal Suspicious Transaction / Activity Report Form

Strictly Private & confidential

To	Anti Money Laundering Compliance Officer	Date:
From	Head of the branch/unit	Branch/Department
	Job Title	STR/SAR Ref No.

Client/ Business Name	Account Number(s)
Transaction Date(s)	Copies of Transactions and Account Details Attached

Description of Transaction(s). *(Nature of transaction, Origin & destination of Transaction etc)*

Source of Funds and Purpose of Transaction

Reasons for suspicion (*Give as much details as possible*)

Signatures branch /unit head

ACTION TAKEN TO VALIDATE

- Acknowledgement sent to the originator on _____.
- Reviewed account documentation
- Discuss with the relationship manager/ branch manager.

- Other.

AGREED SUSPICIOUS. Yes/No

COMMENTS

Signature

Date.

Annexure-3

Internal Assessment/Control Checklist

- Has your CMI Established separate "AML/CFT Compliance Unit (AML/CFT Compliance Unit)" and appoint sufficiently senior head of AML/CFT Compliance Unit?
- Has the senior management of CMI sufficiently committed to place AML/CFT measures over the institutions?
- Has the board of Directors approved AML/CFT policies & procedures and follow up the implementation status of AML/CFT policies and procedures?
- Have branch/unit carried out a review of processes in its day to day business to identify where money laundering is most likely to occur?
- Is this review regularly updated?
- Has branch/unit established procedures and controls to prevent or detect money laundering?
- Is the effectiveness of such controls tested?
- Is all staff aware of AML/CFT policies and procedures?
- Is all staff aware of their responsibilities with regard to money laundering?
- Do they receive regular money laundering training?
- Are all members of staff sufficiently capable of identifying suspicious transactions?
- Are your systems capable of highlighting suspicious transactions (i.e. those not conforming to usual parameters)?
- Do all members of staff know the identity of their Head of AML/CFT COMPLIANCE UNIT?

- Do you thoroughly check and verify the identity of all your Clients?
- Do you have Client accounts in the name of fictitious persons/entities?
- Do you know the identity of the beneficial owner of all your corporate clients?
- Is this identity verified?
- Are all suspicious transactions reported to BFIU?

Annexure-4

Format-1

Reporting of Legacy accounts opened before 30 September, 2010

Total number of BO account opened before 30 September, 2010	Total number of BO account opened after September, 2010	Total number of accounts need to undertake KYC updates	Estimated number of BO accounts needs to be updated in each quarter.

Format-2

Quarterly reporting format of Legacy accounts

Total number of accounts need to undertake KYC updates	Number of accounts to be update in this quarter as per Action Plan	Number of accounts already updates in this quarter	Cumulative number of accounts already updates upto. this quarter	Number of outstanding accounts need to update KYC

Annexure-5

Quarterly Summary of Suspicious Transaction Report
January-June OR July to December
Year

Sl. No.	Subject of STR	Reference Number	Reporting Date	Summary of Suspicion	Comment