

Infrastructure Development Company Ltd.
(IDCOL)

Policy Manual on Prevention of Money Laundering and Combating Financing of Terrorism



“Preface”

This Policy Manual on Prevention of Money Laundering and Combating Financing of Terrorism has been designed for Infrastructure Development Company Ltd. (IDCOL) to attain objectives in compliance with Bangladesh Bank directives in terms of Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act 2013 reproduced herein. The Policy Guidelines has been approved by Board of Directors in its meeting held dated December 29, 2016. The guideline contains the practices and procedures shall have to be followed and the Laws/Acts, Bangladesh Bank’s circulars, reporting formats, assessment format which shall be used by IDCOL for ready reference.

The policy will be complementing the Risk Management regarding Prevention of Money Laundering and Financing of Terrorism to keep within acceptable range.

The policy explicitly addresses issues of the Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act 2013, why and how IDCOL will act to prevent Money Laundering and combat financing of Terrorism in the FI. The policy addresses various issues that are necessary to be in place in order to support a strong risk management culture on Prevention of Money Laundering and Combat Financing of Terrorism.

The policy is meant to be a guiding principle for IDCOL and should not be construed as the limiting definition. The user of the policy should give priority to remain focused on the spirit of the policy. In all spheres of application, the policy would ensure abidance to the laws.

It is natural that there would be deficiencies in presentation of materials or otherwise. We would highly appreciate constructive suggestions for overall improvement of this guidelines which, if found in order, we shall gladly incorporate in the next edition.

Table of Contents

Chapter One: Introduction.....	5
1.1 Introduction	5
1.2 What is Money Laundering?	5
1.3 Why Money Laundering is done?	6
1.4 Why we must combat Money Laundering?	7
1.5 Why we must combat Financing of Terrorism?	8
1.6 Stages of Money Laundering	8
1.7 Vulnerability of the Financial System to Money Laundering	9
How IDCOL can help in Combating Money Laundering.....	10
1.8 How IDCOL can help in combating Terrorist Financing?	11
Chapter Two: International Initiatives	12
2.1 Introduction	12
2.2 Monitoring Members Progress	14
2.4 The NCCT List	14
2.5 ICRG.....	15
2.6 The Basel Committee on Banking Supervision	15
2.7 International Organization of Securities Commissioners	16
2.8 The Egmont Group of Financial Intelligence Units	16
2.9 Asia Pacific Group on Money Laundering (APG).....	17
Chapter Three: National Initiatives.....	18
3.1 National Initiatives	18
Chapter Four: Vulnerabilities of Financial Institutions	20
4.1 Vulnerability of the Financial System to Money Laundering	20
4.2 Vulnerabilities of Products and Services.....	21
Chapter Five: Compliance Requirements under the Law & Circular	23
5.1 Compliance Requirements under the Laws	23
5.2 Compliance Requirements under Circulars	29
5.3 Targeted Financial Sanctions	31
5.4 Self-Assessment	31
5.5 Independent Testing Procedure	31
Chapter Six: AML/CFT Policies and Procedures	33
6.1 Risk in Financial System	33
6.2 Features of AML/CFT Policy	33

6.3	Senior Management Commitment	34
6.4	Organizational Structure	34
6.5	Components of IDCOL's AML/CFT policies.....	38
Chapter Seven: Identification Procedures		39
7.1	Introduction	39
7.2	Know Your Customer (KYC) Policies and Procedures.....	40
7.3	Customer Acceptance Policy.....	41
7.4	Customer Identification	43
7.5	Individual Customers	43
7.6	Corporate Bodies and other Entities.....	44
7.7	Partnerships and Unincorporated Businesses	46
7.8	Powers of Attorney/ Mandates to Operate Accounts	46
7.9	Identification of Beneficial Owners and Verification of their Identities	46
7.10	Reliability of Information and Documentation	48
7.11	Non-Face-to-Face Verification	48
7.12	Timing and Duration of Verification.....	48
7.13	Simplified Customer Due Diligence.....	49
7.14	Enhanced CDD Measures	49
7.15	Politically Exposed Persons	50
7.16	Other High Risk Categories	51
7.17	Performance of CDD Measures.....	51
7.18	Risk Based Approach (RBA).....	52
7.19	Risk grading	54
7.20	Know Your Customer's Customer (KYCC)	55
7.21	Know Your Employee (KYE).....	55
Chapter Eight: Record Keeping		56
8.1	Statutory Requirement	56
8.2	Retrieval of Records	57
8.3	STR and Investigation.....	57
8.4	Training Records	58
8.5	Branch Level Record Keeping.....	58
8.6	Sharing of Record/Information of/to a Customer	58
Chapter Nine: Transaction Monitoring & Reporting.....		59
9.1	Reporting requirements.....	59
9.2	Cash Transaction Reports (CTRs)	59
9.3	Suspicious Transaction Reports (STRs)	59

9.4	Recognition of Suspicious Transactions.....	60
9.5	Suspicious Activity Reporting Process.....	60
9.6	Reporting of Suspicious Transactions	61
9.7	Reporting lines	62
9.8	Reporting destinations.....	63
Chapter Ten: Assessment Procedure.....		64
10.1	Self-Assessment Process.....	64
10.2	Independent Procedures Testing.....	64
Chapter Eleven: Training and awareness building.....		65
11.1	Employee Training and Awareness Program	65
11.2	Training Procedures	67
11.3	Refresher Training.....	68
ANNEXURE		69

IDCOL

Chapter One: Introduction

1.1 Introduction

- 1.1.1 This Policy *Guidelines on Prevention of Money Laundering and Financing of Terrorism* for Infrastructure Development Company Limited (IDCOL) have been prepared in line with the existing Money Laundering Prevention Act, 2012, Anti Terrorism (amendment) Act, 2013, circulars issued by Bangladesh Financial Intelligence Unit (BFIU), the revised Financial Action Task Force (FATF) Recommendations and the international best practices.
- 1.1.2 This *Guidelines are designed to assist IDCOL in complying* with the Bangladesh's Anti Money Laundering and Combating Financing of Terrorism regulations, this will also enable to assess the adequacy of the internal controls, policies and procedures to combat money laundering and terrorist financing of the Financial Institution (FI) subject to its supervision.
- 1.1.3 It is expected that all Executives & Officers of IDCOL, pay proper attention to this Guidelines while conducting relevant financial business and be vigilant for practicing suitable Anti-Money Laundering and Combating Financing of Terrorism procedures while discharging their duties. If any branch appears not doing so, it will arise various risks for IDCOL including financial sanctions from BFIU.
- 1.1.4 It is also expected that the Executives & Officers of IDCOL, will keep it in mind that prevention of Money Laundering and Financing of Terrorism is not simply a stand-alone requirement that is being imposed by the legislation, it is a part of IDCOL risk management policies and procedures.

1.2 What is Money Laundering?

- 1.2.1 A definition of what constitutes the offence of money laundering under AML Act, 2002 was – “Money Laundering” means –
(Au) Properties acquired or earned directly or indirectly through illegal means;
(Aa) Illegal transfer, conversion, concealment of location or assistance in the above act of the properties acquired or earned directly or indirectly through legal or illegal means; “
- 1.2.2 As per Section 2(V) of the Prevention of Money Laundering 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 Law.
 - v. convert or movement or transfer property with the intention to instigate or assist in 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.
- 1.2.3 Properties has been defined in section 2(bb) of the AML Act, 2012 as “Properties means –
- i. any type of tangible, intangible, movable, immovable property or
 - ii. cash, deed or any legal documents or any form including electronic or digital form giving evidence of title or evidence of interest related to title in the property which is located within or outside the country.
- 1.2.4 The U.S. Customs Service, an arm of the Department of the Treasury, provides a lengthy definition of money laundering as "the process whereby proceeds, reasonably believed to have been derived from criminal activity, are transported, transferred, transformed, converted or intermingled with legitimate funds for the purpose of concealing or disguising the true nature, source, disposition, movement or ownership of those proceeds. The goal of the money-laundering process is to make funds derived from, or associated with, illicit activity appear legitimate."
- 1.2.5 Another definition of Money Laundering under U.S Law is, "... the involvement in any one transaction or series of transactions that assists a criminal in keeping, concealing or disposing of proceeds derived from illegal activities."
- 1.2.6 The EU defines it as "the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime."
- 1.2.7 A concise working definition was adopted by Interpol General Secretariat Assembly in 1995, which defines money laundering as: "Any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources".
- 1.2.8 The Joint Money Laundering Sterling Group (JMLSG) of the U.K. defines it as "the process whereby criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecutions, conviction and confiscation of their criminal funds".
- 1.2.9 In lay terms Money Laundering is most often described as the “turning of dirty or black money into clean or white money”. If undertaken successfully, money laundering allows criminals to legitimize "dirty" money by mingling it with "clean" money, ultimately providing a legitimate cover for the source of their income. Generally, the act of conversion and concealment is considered crucial to the laundering process.

1.3 Why Money Laundering is done?

Criminals usually engage themselves in money laundering for three main reasons:

- 1.3.1 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.
- 1.3.2 Second, a trail of money from an offence 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.

- 1.3.3 Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their origin or, alternatively, make it legitimate in appearance.

1.4 Why we must combat Money Laundering?

- 1.4.1 Money laundering has potentially devastating effect on economy, national security, and social consequences. Money laundering is a process which has vital role to commit 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.
- 1.4.2 Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate. We also pay more taxes for public works expenditures inflated by corruption. And those of us who pay tax 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.
- 1.4.3 Money laundering distorts the price of asset and commodity and leads to deallocation 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.
- 1.4.4 One of the most serious micro-economic 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.
- 1.4.5 No one knows exactly how much "dirty" money flows through the world's financial system every year, but the amounts involved are undoubtedly huge. The International Money Fund has estimated that the magnitude of money laundering is between 3% to 7% of world gross domestic product, or at least USD 1.5 trillion to USD 3 trillion.
- 1.4.6 Among its other negative socio-economic 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.
- 1.4.7 The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing in Govt. and Private Offices 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.
- 1.4.8 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 -- fraud, counterfeiting, narcotics trafficking, and corruption -- weaken the reputation and standing of any financial institution. Actions taken 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 becomes accused by 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.
- 1.4.9 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, these Guidelines are drawn up.

1.5 Why we must combat Financing of Terrorism?

- 1.5.1 Financing of Terrorism was criminalized under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999. To reinforce the 1999 convention, United Nations adopted UNSC Resolutions 1373 and 1390 directing the member states to criminalize Financing of Terrorism and adopt regulatory regimes to detect, deter and freeze terrorists' assets. The resolutions oblige all states to deny financing, support and safe harbor for terrorists.
- 1.5.2 Bangladesh has actively involved in multinational and international institutions. Its international relationship and business, banking business in particular are regulated by some domestic and international regulations. So it is mandatory to abide by those regulations. Financial Action Task Force (FATF), the international standard setter, adopted Special Eight Recommendations on Terrorist Financing. So we must be involved in international effort to combat Financing of Terrorism.
- 1.5.3 It is increasingly evident that terrorists and their organizations need to raise significant amounts of cash for a wide variety of purposes for recruitment, training, travel and materials as well as often payment for safe haven protection. So to root up terrorism, we must stop the flow of funds that keep them in business.
- 1.5.4 The consequences of allowing the financial system to facilitate the movement of terrorist money are so horrendous that every effort must be made to prevent this from happening. So combating money laundering and financing of terrorism are not only the regulatory requirement but also an act of self-interest.

1.6 Stages of Money Laundering

- 1.6.1 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) for 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 in 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.
- 1.6.2 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.
- 1.6.3 The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap. However, the basic steps are used

depending on the available laundering mechanisms and the requirements of the criminal organizations. The table below provides some typical examples.

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

1.7 Vulnerability of the Financial System to Money Laundering

- 1.7.1 Money laundering is often thought to be associated solely with banks and moneychangers. All financial institutions, both banks and non-banks, are susceptible to money laundering activities. The sophisticated launderer often involves many other unwitting accomplices such as currency exchange houses, stock brokerage houses, gold dealers, real estate dealers, insurance companies, trading companies and others selling high value commodities and luxury goods.
- 1.7.2 Certain points of vulnerability have been identified in the laundering process, which the money launderer considers difficult to avoid, and where their activities are therefore more susceptible for being recognized. These are:
- Entry of cash into the financial system; [22]
 - Cross-border flows of cash; and [22]
 - Transfers within and from the financial system.
- 1.7.3 Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their procedures with due regard to that risk.
- 1.7.4 Although it may not appear obvious that the products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that weaknesses cannot be exploited.
- 1.7.5 Some liquid products offered by the Bank 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.
- 1.7.6 All banks and non-banking financial institutions, as providers of a wide range of money transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.
- 1.7.7 Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

- 1.7.8 However, in addition, banks and non-banking financial institutions, as providers of a wide range of services, are vulnerable for being used in the layering and integration stages. Other loan accounts may be used as a part of this process to create complex layers of transactions.
- 1.7.9 Some banks and non-banking financial institutions may additionally be susceptible to the attention of the more sophisticated criminal organizations and their “professional money launderers”. Such organizations, possibly under the disguise of front companies and nominees, may create large scale but false international trading activities in order to move their illicit monies from one country to another.
- 1.7.10 Investment and merchant banking businesses are less likely than banks and money changers to be at risk during the initial placement stage.
- 1.7.11 Investment and merchant banking businesses are more likely to find them for being used at the layering and integration stages of money laundering.
- 1.7.12 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.
- 1.7.13 Intermediaries and product providers who deal directly with the public may be used at the initial placement stage of money laundering, particularly if they receive cash.
- 1.7.14 Lump sum investments in liquid products are clearly most vulnerable to be used by the 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 source of funds.
- 1.7.15 Insurance and investment product providers and intermediaries should therefore keep transaction records that are comprehensively enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.
- 1.7.16 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.
- 1.7.17 The facility with which currency exchanges can be effected through a bureau is of particular attraction especially when such changes are effected in favor of a cheque or gold bullion.

How IDCOL can help in Combating Money Laundering

- 1.7.18 Assessment of ML/TF risk related with the IDCOL products, customers, delivery channels and services are the key elements to combat such risk. IDCOL should conduct such risk assessment in line with the national risk and vulnerability assessment, for every existing and future IDCOL’s products, customers, delivery channels and services.
- 1.7.19 The adoption of procedure by IDCOL “know your customer” is not only a principle of good business but it is also an essential tool to avoid involvement in money laundering. Having sound knowledge of a customer's business and pattern of financial transactions and commitments are the best methods by which IDCOL and their staff will recognize attempts at money laundering.
- 1.7.20 Thus efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognize and have therefore to a large extent concentrated on the deposit taking procedures of FIs i.e. the placement stage.
- 1.7.21 IDCOL must keep transaction records that are comprehensively enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

1.7.22 IDCOL will also be dealt with in staff training programs which are a fundamental part of the procedures designed to recognize and combat money laundering.

1.8 How IDCOL can help in combating Terrorist Financing?

- 1.8.1 The prevention of terrorist financing has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of preventing and deterring terrorist financing is a sound knowledge of a customer's business and pattern of financial transactions and commitments associates. The adoption of procedures by which Banks and other Financial Institutions "know their customer" is not only a principle of good business but is also an essential tool to avoid involvement in terrorist financing.
- 1.8.2 Thus efforts to combat terrorist financing largely focus on those points in the process where the terrorist's activities are more susceptible for recognition and have therefore to a large extent concentrated on the deposit taking procedures of FIs i.e. the placement stage.
- 1.8.3 The FI must keep transaction records that are comprehensively enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.
- 1.8.4 In complying with the requirements of the Anti-Terrorist Act, 2013 and in following these Guidance Notes, IDCOL should at all times pay particular attention to the fundamental principle of good business practice - 'know your customer'. Having a sound knowledge of a customer's business and pattern of financial transactions and commitments is one of the best methods by which IDCOL and their staff will recognize attempts at terrorist financing. It will also be dealt with in staff training programs which are a fundamental part of the procedures designed to recognize and combat Money Laundering and Terrorist Financing.

Chapter Two: International Initiatives

2.1 Introduction

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

- 2.1.1 **THE UNITED NATIONS-** the United Nations (UN) was the first international organization to undertake significant action to fight money laundering on a truly world-wide basis. The role of UN is important for several reasons which are - First, it is the international organization with the broadest range of membership. The UN, founded in 1945, has 191 members from all across the world. Second, the UN actively operates a program to fight money laundering; the Global Program against Money Laundering, which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC). Third, and perhaps most importantly, the UN has the ability to adopt international treaties or conventions that obligate the ratifying countries to reflect those treaties or conventions in their local laws. In certain cases, the UN Security Council has the authority to bind all member countries through a Security Council Resolution, regardless of other actions on the part of an individual country.
- 2.1.2 **The Vienna Convention** -due to growing concern about increased international drug trafficking and the tremendous amounts of related money entering into financial system, the UN, adopted the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) known as Vienna Convention, named after the city in which it was signed. The Vienna Convention deals primarily with provisions to fight the illicit drug trade and related law enforcement issues. At present, nearly 169 countries including Bangladesh are party to the convention. The convention came into force on November 11, 1990.
- 2.1.3 **The Palermo Convention-** In order to fight against internationally organized crimes, the UN adopted the International Convention against Transnational Organized Crime (2000), named after the city in which it was signed as Palermo Convention. The Palermo Convention specifically obligates each ratifying country to:
- i. Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;
 - ii. Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
 1. Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information; and
 2. Promote international cooperation. This convention has come into force from 29th September 2003, having been signed by 147 countries and ratified by 82 countries.
- 2.1.4 **International Convention for the Suppression of the Financing of Terrorism** The financing of terrorism was an international concern prior to the attacks on the United States on 11 September, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002, with 132 countries signing the convention and 112 countries ratifying it. The convention requires ratifying states to criminalize terrorism, terrorist organizations and terrorist acts. Under the convention, it is unlawful for any person to provide or collect funds

with the (1) intent that the funds be used for, or (2) knowledge that the funds be used to, carry out any of the acts of terrorism defined in the other specified conventions that are annexed to this convention.

- 2.1.5 **Security Council Resolution 1267 and Successors** The UN Security Council has also 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.
- 2.1.6 **Security Council Resolution 1373** unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution passed in response to a threat to international peace and security under Chapter VII of the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to: -deny all forms of support for terrorist groups; -suppress the provision of safe haven or support for terrorist, including freeing funds or assets of persons, organizations or entities involved in terrorist acts; -prohibit active or passive assistance to terrorists; and - cooperate with other countries in criminal investigations and sharing information about planned terrorist acts.
- 2.1.7 **The Counter-Terrorism Committee** As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism. Resolution 1373 calls upon all countries to submit a report to the CTC on the steps taken to implement the resolution's measures and report regularly on progress. In this regard, the CTC has asked each country to perform a self-assessment of its existing legislation and mechanism to combat terrorism in relation to the requirements of Resolution 1373.
- 2.1.8 **Global Program against Money Laundering** the UN Global Program against Money Laundering (GPML) is within the UN Office of Drugs and Crime (UNODC). The GPML is a research and assistance project with the goal of increasing the effectiveness of international action against money laundering by offering technical expertise, training and advice to member countries upon request.
- 2.1.9 **THE FINANCIAL ACTION TASK FORCE** The Financial Action Task Force on Money Laundering (FATF), formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. The FATF currently

comprises 35 member jurisdictions and 2 regional organizations, representing most major financial centres in all parts of the globe (<http://www.fatf-gafi.org/>).

2.1.10 **FATF 40+9 Recommendations** FATF adopted a set of 40 recommendations to prevent money laundering. These Forty Recommendations constituted a comprehensive framework for AML and were designed for universal application by countries throughout the world. Although not binding as law upon a country, the Forty Recommendations was widely endorsed by the international community including World Bank and IMF and relevant organizations as the international standard for AML. The Forty Recommendations were initially issued in 1990 and revised in 1996 and 2003 to take account of new developments in money laundering and to reflect developing best practices internationally. To accomplish its expanded mission of combating financing of terrorism FATF adopted nine Special Recommendations in 2001.

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

Table 1: **Summary of new FATF 40 Standards Group**

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

2.2 Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of 40+9 recommendations is facilitated by a two-stage process: self-assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of 40+9 recommendations. In the mutual evaluation stage, each member is examined and assessed by experts from other member countries in every five years. The first Mutual Evaluation (ME) of Bangladesh was conducted by a joint team of World Bank and International Monetary Fund in October, 2002 and the report thereof was adopted by the APG in September, 2003. The 2nd Mutual Evaluation of Bangladesh was conducted by an APG team in August, 2008. (<http://www.fatf-gafi.org/countries/#Bangladesh>)

2.4 The NCCT List

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

FATF introduced new implementation mechanism known as International Cooperation and Review Group (ICRG).

2.5 ICRG

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

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

2.6 The Basel Committee on Banking Supervision

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

2.6.1 **Statement of Principles on Money Laundering**

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

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

2.6.2 **Basel Core Principles for Banking**

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provides a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. Core Principle 15, one of the 25 Core Principles, deals with money laundering; it provides:

Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict “know your customer” rules, that promote

high ethical and professional standards in the financial sector and prevent the bank from being used; intentionally or unintentionally, by criminal elements.

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

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

2.6.3 Customer Due Diligence

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

2.7 International Organization of Securities Commissioners

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 105 countries. 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. Similar to the Basel Committee and International Association of Insurance Supervisors (IAIS), it relies on its members to implement its recommendations within their respective countries.

2.8 The Egmont Group of Financial Intelligence Units

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

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

Bangladesh has got the membership of prestigious Egmont Group, formed with Financial Intelligence Units of various countries which help get global support in fighting against money laundering, terrorist financing and other financial crimes. It will help stop money laundering and terrorist financing. It won’t be easy now to launder money abroad through corruption.

2.9 Asia Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 40 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD(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 and Terrorist Financing.

The APG has five key roles: To assess compliance by APG members with the global standards through a robust mutual evaluation program;

- i. To coordinate bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region in order to improve compliance by APG members with the global standards;
- ii. 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;
- iii. To conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities; and
- iv. 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.

Chapter Three: National Initiatives

3.1 National Initiatives

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

- 3.1.1 Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40 recommendations. Subsequently, Bangladesh, as the first South Asian country, promulgated Money Laundering Prevention Act (MLPA), 2002 which came into force on 30 April, 2002. For exercising the power and shouldering the responsibilities, as stated in the MLPA, a separate department named Anti Money Laundering Department (AMLDD) was established at Bangladesh Bank.
- 3.1.2 To address the shortcomings of the MLPA, 2002 and to meet the international standards Bangladesh enacted Money Laundering Prevention Ordinance (MLPO) in 2008 which was replaced by MLPA, 2009 by the parliament in 2009. To address the deficiencies identified in the Mutual Evaluation Report (MER), Bangladesh has again enacted Money Laundering Prevention Act in February, 2012 repealing MLPA, 2009.
- 3.1.3 To combat terrorism and terrorist financing Bangladesh also enacted Anti Terrorism Act (ATA), 2009. To address the gap identified in the MER, some provisions of ATA 2009 have been amended through enactment of Anti Terrorism (Amendment) Act 2012.
- 3.1.4 Bangladesh has enacted Mutual Assistance in Criminal Matters Act, 2012 to enhance international cooperation on ML/TF and other related offences.
- 3.1.5 In the process of responding to international concern, Bangladesh Government formed a central and several regional taskforces on 27 January, 2002 to combat money laundering and illegal Hundi activities in Bangladesh.
- 3.1.6 On May 16, 2007 financial intelligence unit (FIU) was established in Bangladesh Bank for receiving, analyzing and disseminating Suspicious Transaction Reports (STRs) related to ML/TF and Cash Transaction Reports (CTRs). As per the provision of MLPA, 2012 AMLDD is now working as separate unit in Bangladesh Bank as Bangladesh Financial Intelligence Unit (BFIU).
- 3.1.7 Bangladesh Bank (BB) has already issued Guidance Notes under 'core risk' management titled 'Guidance Notes on Prevention of Money Laundering' for banks. Bangladesh Bank has also issued guidance notes for insurance companies and money changers.
- 3.1.8 Self assessment and independent testing procedure system were introduced for banks on March 24, 2008 to assess their own compliance. Side by side, Bangladesh Bank has also been monitoring the same through a process called system check inspection.
- 3.1.9 A rigorous Customer Due Diligence (CDD) procedure has been introduced to protect identity theft by customer through issuance of Uniform Account Opening Form for all banks. It includes standardized Know Your Customer (KYC), Transaction Profile (TP) and Risk Grading of Customer.
- 3.1.10 To facilitate exchange of information and intelligence among FIUs, Bangladesh FIU has already signed 13 (thirteen) MoUs with other FIUs.
- 3.1.11 To provide guidance for effective implementation of regime, a National Coordination Committee headed by the Honorable Finance Minister and a Working Committee headed by the secretary of Bank and Financial Institutions Division of Finance Ministry were formed consisting representatives from all regulatory authorities.

- 3.1.12 Bangladesh Government has developed the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2011-2013. The strategy consists of following 12 (twelve) strategies against 12 (twelve) strategic objectives:
- i. Strengthening the legal framework
 - ii. Enhancing effectiveness of the FIU
 - iii. Enforcing compliance of all reporting agencies
 - iv. Structural improvement and capacity building in tracing out methods, techniques and channels of money laundering and terrorist financing
 - v. Improving transparency in financial reporting on AML/CFT issues
 - vi. Ensuring transparency in the ownership of legal entities
 - vii. Enhancing financial inclusion
 - viii. Maintaining a comprehensive AML/CFT database
 - ix. Boosting national coordination both at policy and operational levels
 - x. Developing and maintaining international and regional cooperation on AML/CFT
 - xi. Heightening public awareness
 - xii. Stemming the illicit outflows and inflows of fund
- 3.1.13 Issued a comprehensive circular for banks and non bank financial institutions addressing the following issues:
- i. Definition of Customer for KYC purpose
 - ii. Process and timing of Customer Due Diligence(CDD)
 - iii. Defining and identifying Beneficial Owner
 - iv. Politically Exposed Persons related issues
 - v. Correspondent Banking
 - vi. Employee screening mechanism
 - vii. Awareness program for the customer
- 3.1.14 BFIU in cooperation with Anti Corruption Commission has assessed ML/TF risk and vulnerabilities in Bangladesh and drafted the National ML/TF Risk and Vulnerability Assessment Report.
- 3.1.15 Bangladesh has continued its pursuance to get membership of the Egmont Group, the global forum for cooperation from 2008. In this regard, the off-site evaluation has already been conducted by Malaysia and Thailand as sponsor and cosponsor respectively. Bangladesh has become a member of Egmont Group on 3rd July,2013 a global network of Financial Intelligence Units, which will help the country to combat cross- border money laundering and potential terrorist financing. Being 132nd member of Egmont Group, Bangladesh will have access to sensitive information on the Egmont Group website. The Bangladesh Bank's Financial Intelligence Unit will act as the national center for all works.
- 3.1.16 Separate annual conferences for the Chief Anti Money Laundering Compliance Officer (CAMLCO) of Banks, Insurance Companies and Financial Institutions were organized.
- 3.1.17 The Bank and Financial Institutions Division, Ministry of Finance has issued a circular instructing all the related agencies to provide relevant information to Bangladesh Bank.
- 3.1.18 BFIU has continued its effort to develop its IT infrastructure which is necessary for efficient and effective functioning of the unit. In this regard, it has finalized the procurement process of 'goAML' software for online reporting and software based analysis of CTRs and STRs.
- 3.1.19 BFIU has established MIS to preserve and update all the information and to generate necessary reports using the MIS.

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

Chapter Four: Vulnerabilities of Financial Institutions

4.1 Vulnerability of the Financial System to Money Laundering

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

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:

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

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

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

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.

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.

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

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

Some banks and non-banking financial institutions may additionally be susceptible to the attention of the more sophisticated criminal organizations and their “professional money launderers”. Such organizations, possibly under the disguise of front companies and nominees, may create large scale but false international trading activities in order to move their illicit money 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.

4.2 Vulnerabilities of Products and Services

4.2.1 Factoring

In international factoring there is a provision that the two firms must be member of Factor Chain International or some association that can ensure the credit worthiness of the firms. In absence of this kind of private sector watchdog in the local factoring, the supplier and the buyer may ally together to legalize their proceeds of crime. Without conducting any bonafide transaction the supplier may get finance from FIs and FIs may get repayment from buyer. FIs may focus on getting repayment without considering the sources of fund which can be taken as an opportunity by the money launderer to place their ill-gotten money. In the under mentioned cases, Money Laundering may be happened occasionally out of usual/valid transactions. These may as under:

- i. Lease/Term Loan Finance
Front company can take lease/term loan finance from a financial institution and repay the loan from illegal source, and thus bring illegal money in the formal financial system in absence of proper measures. The firm can also repay the loan amount even before maturity period if they are not asked about the sources of fund. In case of financial or capital lease, the asset purchased with FI's financing facility can be sold immediately after repayment of the loan through illegal money and sold proceeds can be shown as legal. So the money launderers and terrorist financier can use this financial instrument for placement and layering of their ill-gotten money.
- ii. Private Placement of Equity/Securitization of Assets
Some FIs offer financing facilities to firms through private placement of equity and securitization of assets. FIs sell those financial instruments to private investors who may take this as an opportunity to make their money legal. Later the money launderers can sell these instruments and bring their money in the formal financial system.
- iii. Personal Loan/Car Loan/Home Loan
Any person can take personal loan from FIs and repay it by illegally earned money; thus he/she can launder money and bring it in the formal channel.
After taking home loan or car loan, money launderers can repay those with their illegally earned money, and later by selling that home/car, they can show the proceeds as legal money.
- iv. SME/Women Entrepreneur Loan
Small, medium and women entrepreneurs can take loan facilities from FIs and in many cases, repayment may be done by the illegally earned money. They even do so only to validate their money by even not utilizing the loan. This way they can bring the illegal money in the financial system.
- v. Deposit Scheme
FIs can sell deposit products with at least a six months maturity period. However, the depositor can encash their deposit money prior to the maturity date with prior approval from Bangladesh Bank, foregoing interest income. This deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.
- vi. Loan Backed Money Laundering

In the “loan backed” money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a “loan or mortgage” back to the money laundering for the same amount with all the necessary “loan or mortgage” documentation. This creates an illusion that the trafficker’s funds are legitimate. The scheme is reinforced through “legislatively” scheduled payments made on the loan by the money launderer.

4.2.2 **Structural Vulnerabilities**

- i. FIs are yet to develop sufficient capacity to verify the identity and source of funds of their clients.
- ii. The human resources are not skilled and trained enough to trace money laundering and terrorist financing activities.
- iii. None of the FIs has Anti Money Laundering software to monitor and report transactions of a suspicious nature to the financial intelligence unit of the central bank.

INDCOL

Chapter Five: Compliance Requirements under the Law & Circular

5.1 Compliance Requirements under the Laws

In Bangladesh, compliance requirements for FIs, as reporting organization, are based on Money Laundering Prevention Act (MLPA), 2012, Anti-terrorism (Amendment) Act, 2012 and circulars or instructions issued by BFIU.

5.1.1 Money Laundering Prevention Act, 2012

Under the Section –

- i. **Offence of Money Laundering and Punishment – (as per section 4 of MLPA 2012)**
 1. For the purpose of this Act, money laundering shall be an offence.
 2. Any person who commits the offence of money laundering, or abets or conspires in the commission of the offence of money laundering, shall be punishable with imprisonment for a minimum period of 4(four) years and not more than 12(twelve) years and in addition to this a fine equivalent to the twice of the value of the property involved in the offence or taka 10(ten) lacs, whichever is greater may be imposed.
 3. In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favor of the State which directly or indirectly involved or related with money laundering or any predicate offences.
 4. Any entity which commits an offense under this section shall be punishable with a fine of not less than twice the value of the property or taka 20(twenty) lac whichever is greater and in addition to this the registration of the said entity will be liable to be cancelled.
 5. It shall not be a prerequisite to be convicted or sentenced for any predicate offence to pass an order of conviction or sentence for a money laundering crime.
- ii. **Punishment for violation of a freezing or attachment order – (as per section 5 of MLPA 2012)**

Any person who violates a freeze order or order of attachment issued pursuant to this Act shall be punishable with an imprisonment for a maximum period of 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or both.
- iii. **Punishment for divulging information – (as per section 6 of MLPA 2012)**
 1. No person shall, with an ill motive, divulge any information relating to the investigation or any other related information, to any person, organization or news media.
 2. Any person empowered under this Act shall refrain from using, publishing or divulging any information collected, received, retrieved or known by him/herself during the course of employment or appointment by an institution or agent, or after the expiry of any contract of employment or appointment for any purpose other than the purpose of this Act.
 3. Whoever contravenes the provisions contained in sub-sections (1) and (2) shall be punishable by imprisonment of maximum period of 2 (two) years or a fine, not exceeding Tk. 50 (fifty) thousand or both.
- iv. **Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information – (as per section 7 of MLPA 2012)**
 1. Whoever, under this Act – Obstructs or declines to cooperate with any investigation officer carrying out the investigation; or Declines to supply information or submit a report when requested without any reasonable ground; He shall be held to have committed an offence under this Act.

2. Any person found guilty of an offence under sub-section (1) shall be punishable by imprisonment of maximum period of 1 (one) year or with a fine not exceeding Tk. 25 (twenty five) thousand or with both.

v. **Punishment for providing false information – (as per section 8 of MLPA 2012)**

1. No person shall knowingly provide false information in any manner regarding the source of fund, self identity, the identity of an account holder or the beneficiary or nominee of an account.

Any person who violates the provisions contained in sub-section (1) will be punishable by imprisonment of maximum period of 3 (three) years or a fine not exceeding Tk. 50 (fifty) thousand or both.

vi. **Powers and Responsibilities of Bangladesh Bank in Preventing and Restraining the Offence of Money Laundering – (as per section 23 of MLPA 2012)**

1. For the purposes of this Act Bangladesh Bank shall have the following powers and responsibilities:
 - a. analyze or review information related to cash transactions and suspicious transactions received from any reporting organizations and to collect additional information for the purpose of analyzing Cash Transaction Report (CTR) or Suspicious Transaction Report (STR) from reporting organizations and maintain data on the same and where appropriate provide said information to the relevant law enforcement agencies for taking the 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 involves 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 through the commission of any offence:
Provided that such order may be extended for additional period of 30 (thirty) days up to a maximum of 6 (six) months, if it appears necessary to uncover correct information relating to transactions of the account;
 - d. Issue from time to time to the reporting organizations any directions necessary for the prevention of money laundering;
 - 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 Bangladesh Bank, and where necessary, carry out on-site inspections of the reporting organizations to ascertain the same;
 - f. arrange for meetings and seminars including provide the training necessary for the purpose of ensuring proper implementation of this Act, to officers and staff of any organization or institution at the discretion of Bangladesh Bank, including reporting organizations;
 - g. carry out any other functions necessary to fulfill the purpose of this Act.
2. Provide with the information, if not obliged otherwise by the existing laws or any other cause, to the investigating organization if requested by them for information related to money laundering or suspicious transaction investigation.
3. If any reporting organization fails to provide requested information timely pursuant to this Section, Bangladesh Bank may impose fine such organization Tk.

10 (ten) thousand per day and up to a maximum of Tk. 5 (five) lacs. If an organization is fined more than 3 times in a financial year, Bangladesh Bank may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization

4. If any reporting organization provides false information or statement requested pursuant to this Section, Bangladesh Bank may impose fine to such organization not less than Tk. 20 (twenty) thousand but not more than Tk. 5 (five) lacs. If an organization is fined more than 3 times in a financial year, Bangladesh Bank may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization
5. If any reporting organization fails to comply with any instruction given by Bangladesh Bank pursuant to this Act, Bangladesh Bank may fine such organization Tk. 10 (ten) thousand per day and up to maximum Tk. 5 (five) lacs for each such non compliance. If an organization is fined more than 3 times in a financial year, Bangladesh Bank may suspend the registration or license with a purpose to close the operation of that organization or any of its branches/service centers/booths/agents, within Bangladesh or where appropriate, shall inform the registration or licensing authority about the subject matter so that the relevant authority may take appropriate action against the said organization.
6. If any reporting organization fails to comply with the freeze order or suspension order of transaction given by Bangladesh Bank under sub section 1(c), Bangladesh Bank may fine such organization not less than the balance held on that account but not more than twice of the balance at the time of issuance the order.
7. If any person 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 amount from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized Bangladesh Bank may make an application before the court for recovery and the court may pass any order which it deems fit.
8. If any reporting organization is fined under sub-sections 3, 4, 5 and 6, Bangladesh Bank may impose a fine upon the responsible owner, director, employees and officials or persons employed on a contractual basis of that reporting organization, not less than Tk. 10 (ten) thousand and a maximum up to Tk. 5 (five) lacs and where necessary may direct the relevant organization to take necessary administrative actions.

vii. Responsibilities of Reporting Organizations in Preventing the Offence of Money Laundering – (as per section 25 of MLPA 2012)

1. Reporting Organizations shall have the following responsibilities in the prevention of money laundering:
 - a. maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;

- b. in case of closed account of any customer, keep previous records of transactions of such account for at least 5(five) years from the date of closure;
 - c. provide the information maintained under sub-sections (a) and (b) to Bangladesh Bank from time to time, as requested;
 - d. if any doubtful transaction or attempt of such transaction as defined under 2(n) is observed by reporting organization, it shall be reported as Suspicious Transaction Report (STR) to the Bangladesh Bank proactively and immediately.
2. If any reporting organization violates the provisions contained in sub-section (1), Bangladesh Bank may:
 - a. Impose a fine on the said reporting organization of a minimum of Tk. 50 (fifty) thousand and up to a maximum of Tk. 25 (twenty-five) lacs; and
 - b. Cancel the license or the authorization for carrying out commercial activities of the said Organization or any of its branches/service centers/booths/agents, in addition to the fine mentioned in clause (a), and where appropriate, shall inform the registration or licensing or authority about the subject matter so that the relevant authority may take appropriate action against the said Organization
 3. Bangladesh Bank shall collect the sum of fine received under sub-section (2) under manner determined by it and the sum received shall be deposited into the State Treasury.

viii. **Offences Committed by an Entity – (as per section 27 of MLPA 2012)**

1. If any offence under this Act is committed by an entity, every proprietor, director, manager, secretary or any other officer, staff or representative of the said entity who is directly involved in the offence shall be deemed to be guilty of the offence, unless he is able to prove that the said offence has been committed without his knowledge or he took steps to prevent the commission of the said offence.

Explanation – In this section – “Director” means any partner or the Board of Directors, by whatever name it is called; it also means its member.

5.1.2 **Anti terrorism (Amendment) Act, 2012**

Under the Section-

i. **Offences relating to financing for terrorist activities – (as per section 7 of ATA 2012)**

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.
5. If any person is found guilty of any of the offences set out in sub-sections (1) to (4), that person will be sentenced to imprisonment for a term between a maximum of twenty and a minimum of four years, and in addition to this a fine may be imposed not less than the greater of twice the value of the property involved with the offence or taka 10(ten) lac.
6. (1) If any entity is found guilty of any of the offences set out in sub-sections (1) to (4), steps may be taken under section 18 and in addition to this a fine may be imposed not less than the greater of thrice the value of the property involved with the offence or taka 50(fifty) lac ; and
(2) The head of such entity, Chairman, Managing Director, Chief Executive Officer whatever may be called by shall be punished with an imprisonment of a term up to maximum of 20 and a minimum of 4 years and in addition to this a fine may be imposed the greater of twice the value of the property involved with the offence or taka 20(twenty) lac unless he is able to prove that the said offence was committed without his knowledge or he had tried utmost to prevent the commission of the said offence.

ii. **Powers of Bangladesh Bank – (as per section 15 of ATA 2012)**

1. Bangladesh Bank may take the necessary steps to prevent and identify any transactions carried out through any reporting organization for the purpose of committing any offence under this Act, and for this purpose, it will have the following powers and authority –
 - a. Call for a report relating to any suspicious transactions from any reporting organization,
 - b. Provide the reports received under sub-section (a) to the respective law enforcement agencies for taking necessary steps or, where applicable, provide it to the foreign law enforcement agencies upon their request or, exchange information relating to the report with the foreign law enforcement agencies.
 - c. Collect and preserve of all statistics and records;
 - d. Create and maintain a database containing the reports of all suspicious transactions;
 - e. Analyze reports relating to suspicious transactions;
 - f. If there are reasonable grounds to suspect that any transaction is connected to terrorist activities issue an written order to the respective reporting organization to suspend or freeze transactions in the relevant account for a period not exceeding 30(thirty) days. Such order may be extended for additional periods of 30 (thirty) days up to a maximum of 6 (six) months, if it appears necessary to uncover correct information relating to transactions of the account;
 - g. Monitor and supervise the activities of reporting organizations;

- h. Give directions to reporting organizations to take preventive steps to combat the financing for terrorist activities;
 - i. Inspect reporting organizations for the purpose of identification of suspicious transactions connected to financing for terrorist activities; and
 - j. Provide training to officers and employees of reporting organizations for the purpose of identification and prevention of suspicious transactions connected to financing for terrorist activities.
2. Bangladesh Bank, on identification of a reporting organization or its customer as being involved in a suspicious transaction connected to financing for terrorist activities, shall inform the same to the relevant law enforcement agency and provide all necessary cooperation to the said law enforcement agency to facilitate their inquiries and investigations into the matter.
 3. In case of offences organized in other countries under trial, Bangladesh Bank shall take steps to seize the accounts of any person or entity pursuant to any international, regional or bilateral contract, UN conventions or respective resolutions of UN Security Council ratified by the government
 4. The fund seized under subsection (3) shall be subject to disposal by the respective court pursuant to the respective contracts, conventions or respective resolutions of UN Security Council.
 5. In order to perform the responsibilities set out in subsections (1) to (3), governmental, semi-governmental, autonomous bodies shall provide requested information or in certain cases spontaneously provide information to the Bangladesh Financial Intelligence Unit.
 6. The Bangladesh Financial Intelligence Unit on demand or in certain cases spontaneously provide information relating to terrorist activities or the financing for terrorist activities to the Financial Intelligence Units of other countries.
 7. For the purpose of investigation relating to financing for terrorism law enforcement agencies shall have the right to access any document or file of any bank as per the following conditions:
 - a. with an order from an appropriate court or tribunal;
 - b. with the approval of Bangladesh Bank.
- iii. **Duties of Reporting Organizations – (as per section 16 of ATA 2012)**
1. Each reporting organization shall take necessary measures, exercising appropriate caution and responsibility, to prevent and identify financial transactions through them connected to any offence committed under this act and if any suspicious transaction is identified, shall spontaneously report it to the Bangladesh Bank without any delay.
 2. The Board of Directors, or in the absence of the Board of Directors the Chief Executive Officer or whatever may be called by, of each reporting organization shall approve and issue directions regarding the duties of its officers, and will ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting organizations, have been complied with.
 3. If any reporting organization fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provide any wrong information or false information or statement, the said reporting organization shall be liable to pay a fine determined and directed by Bangladesh Bank, not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with a purpose to close the operation of the said agency/organization or any branch,

service centre, booth or agent of that organization within Bangladesh or where applicable, shall inform the registration/licensing authority about the subject matter to take appropriate action against the organization.

4. If any Reporting Organization fails to pay any fine imposed by Bangladesh Bank under sub sections 3 of this Act, Bangladesh Bank may recover the amount from the reporting organizations by debiting their accounts maintained in any bank or financial institution or Bangladesh Bank. In this regard if any amount of the fine remains unrealized Bangladesh Bank may make an application before the relevant court for recovery.

5.2 Compliance Requirements under Circulars

5.2.1 Policies for Prevention of Money Laundering and Terrorist Financing

In pursuance of section 16(2) of Anti-terrorism (Amendment) Act, 2012, and subsequent directives of Bangladesh Bank, all FIs must have their own policy manual approved by their Board of Directors/topmost committee to prevent money laundering and terrorist financing. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh. FIs shall from time to time review and confirm the meticulous compliance of the circulars issued by Bangladesh Bank.

To implement the policy manual and compliance of instructions of Bangladesh Bank, every FI must have to designate one high level officer as Chief Anti Money Laundering Compliance Officer (CAMLCO) in the Central Compliance Unit (CCU) and one officer as Branch Anti Money Laundering Compliance Officer (BAMLCO) in the branch level.

Financial Institutions shall not open or maintain numbered or anonymous account.

i. Customer Identification

It is mandatory to collect and verify the correct and complete identification of customers to prevent money laundering and terrorist financing and to keep the financial sector free from risks.

To protect FIs from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, the Money Laundering Prevention Policy Manual shall clearly state how to conduct Customer Due Diligence at different stages such as:

1. while establishing relationship with the customer;
2. while conducting financial transaction with the existing customer;

To be sure about the customer's identity and underlying purpose of establishing relationship with the institution, each institution shall collect adequate information up to its satisfaction. If a person operates an account on behalf of the customer, the concerned financial institution must satisfy itself that the person has due authorization to operate. Correct and complete information of the person, operating the account, is to be collected.

Legal status and accuracy of information of the operators are to be ascertained in case of the accounts operated by trustee and professional intermediaries (such as lawyers/law firm, chartered accountants, etc).

While establishing and maintaining business relationship and conducting financial transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories listed as

high risk country in FATF's public statements) enhanced due diligence shall have to be ensured.

The identity of the beneficial owner of the account shall have to be confirmed on the basis of the information obtained from reliable sources up to the satisfaction of the institution. Moreover, FIs have to do the followings:

1. Complete and correct information of identity of the persons besides the customer, shall have to be collected and preserved if a customer operate an account on behalf of another person in his/her own name.
2. The controller or the owner of the customer shall have to be identified.
3. Complete and correct information of identity of the beneficial owners shall have to be collected and preserved. For the purpose of this subsection, a person will be treated as a beneficial owner if :
 - a. he has controlling share of a company or/and
 - b. hold 20% or more shares of a company.

ii. **Politically exposed Persons (PEPs)**

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised.

Following instructions shall have to be followed to ensure Enhanced Due Diligence:

1. a risk management system shall have to be introduced to identify risks associated with the accounts opening and operating of PEPs;
2. take reasonable measures to establish the source of wealth and source of funds;
3. ongoing monitoring of the transactions have to be conducted; and
4. the FIs should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

All instructions as detailed for PEPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputational risk to the FI.

The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

iii. **Appointment and Training**

Employee Screening: One of the major purposes of combating money laundering and terrorist financing activities is to protect the FIs from risks arising out of money laundering and terrorist financing. To meet this objective, FIs shall have to undertake proper screening mechanism in their different appointment procedures so that they do not face money laundering and terrorist financing risks by any of their staff.

Training for the officials: To ensure proper compliance of ML/TF activities each FI shall arrange suitable training for their officials.

Education and training for customers: Financial Institutions shall respond to customers on different matters including KYC. Financial Institutions shall time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and also arrange to stick posters in every branch at a visible place.

iv. **Suspicious Transaction Reporting (STR)**

According to the provision of section 25 (1) (d) of MLPA, 2012, the FIs have to report Bangladesh Bank proactively and immediately, facts on suspicious, unusual or doubtful

transactions likely to be related to money laundering. Bangladesh Bank has the power to call STR from FIs related to financing of terrorism according to section 15(a) of Anti terrorism (Amendment) Act, 2012.

5.3 Targeted Financial Sanctions

United Nations Security Council Resolution 1267 and 1373 have been adopted under Article VII of UNSCR charter, which means these resolutions are obligatory for every jurisdiction. BFIU has instructed all banks and FIs to take necessary action on UNSCR 1267 and 1373 (targeted financial sanctions). To comply with this direction FI should consult the UN sanction list regularly and if find any account with it, FI should inform BFIU immediately.

5.4 Self-Assessment

As per AML circular 15, Branch (es) shall assess them quarterly by its own and submit their report to Internal Control and Compliance Department with a copy to Central Compliance Unit (CCU), AMLD. Then CCU, AMLD of each FI would prepare half yearly self-assessment procedure that will assume how effectively the FI's AML/CFT program is working. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations. The self-assessment should advise management whether the internal procedures and statutory obligations of the FI have been properly discharged.

Each branch will assess its AML/CFT activities covering the following areas on quarterly basis and submit the report to CCU within next 20 days of the following month:

- i. The percentage of officers/employees that received official training on AML/CFT;
- ii. The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and Bangladesh Bank's instructions and guidelines;
- iii. The arrangement of AML/CFT related meeting on regular interval;
- iv. The effectiveness of the customer identification during opening an individual, corporate and other account;
- v. The risk categorization of customers by the branch;
- vi. Regular update of customer profile upon reassessment;
- vii. The monitoring of customers' transactions with their declared TP after categorizing the customers based on risk or transactions over specific limit;
- viii. Identification of Suspicious Transaction Reports (STRs);
- ix. The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- x. The measures taken by the branch during opening of account of PEPs;
- xi. Consideration of UN Sanction List while conducting any business.

The compliance with AML/CFT weaknesses/irregularities, as the FI's Head Office and Bangladesh Bank's inspection report mentioned.

5.5 Independent Testing Procedure

As per AML circular 15, testing is to be conducted at least annually by financial institutions' internal audit personnel, compliance department, and by an outside party such as the institution's external auditors. The test will cover the following areas:

- i. Branch Compliance Unit/BAMLCO
- ii. Knowledge of officers/employees on AML/CFT issues
- iii. Customer Identification (KYC) process
- iv. Branch's receipt of customer's expected transaction profile and monitoring

- v. Process and action to identify Suspicious Transaction Reports (STRs)
- vi. Regular submission of reports to CCU
- vii. Proper record keeping
- viii. Overall AML related activities by the branch

The tests include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the financial institution's Anti Money Laundering procedures.

- i. As sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- ii. test of the validity and reasonableness of any exemption granted by the financial institution; and
- iii. test of the record keeping system according to the provisions of the laws. Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline.

INDICOL

Chapter Six: AML/CFT Policies and Procedures

6.1 Risk in Financial System

In the context of AML/CFT issues IDCOL may face following types of risks while doing its business.

- 6.1.1 **Reputational risk** is a major threat to IDCOL, since the nature of their business requires maintaining the confidence of depositors, borrowers and the general stakeholders. Reputational risk is defined as the potential that adverse publicity regarding organization's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. IDCOL is especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by its customers. They need to protect themselves by means of continuous vigilance through an effective KYC program. Assets management, or held on a fiduciary basis, can pose particular reputational dangers.
- 6.1.2 **Operational risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failing of internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of IDCOL's programs, ineffective control procedures and failure to practice due diligence.
- 6.1.3 **Legal risk** is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the organization. IDCOL may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, it can, for example, suffer fines, criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving the organization may have far greater cost implications for its business than just the legal costs. IDCOL will be unable to protect themselves effectively from such legal risks if it does not practice due diligence in identifying its customers and understanding their business.
- 6.1.4 On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by the lenders or the large depositors, with potentially damaging consequences for IDCOL's liquidity.

6.2 Features of AML/CFT Policy

An effective AML/CFT Compliance Program must be able to control the risks associated with the IDCOL's products, services, customers, entities and geographic locations. Therefore, an effective risk assessment is required to be an ongoing process, not a one-time exercise.

- 6.2.1 The AML/CFT policy of IDCOL is written, approved by the Board of Directors, and noted as such in the board meeting minutes.
- 6.2.2 The AML/CFT compliance policy establishes clear responsibilities and accountabilities within the organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using IDCOL's facilities for money laundering and the financing of terrorist activities, thus ensuring that it comply with its obligations under the law.
- 6.2.3 The Policies are based upon assessment of the money laundering risks, taking into account IDCOL's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering.
- 6.2.4 The Policies include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures addresses IDCOL's Know Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring

existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness.

- 6.2.5 The policy includes a description of the roles the Anti-Money Laundering Compliance Officers(s)/Unit and other appropriate personnel will play in monitoring compliance with and effectiveness of money laundering policies and procedures.
- 6.2.6 The AML/CFT policies will be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing anti-money laundering rules and regulations or business.
- 6.2.7 In addition the policy emphasizes the responsibility of every employee to protect IDCOL from exploitation by money launderers, and should set forth the consequence of noncompliance with the applicable laws and the institution's policy, including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any association with money laundering and terrorist financing activity.

6.3 Senior Management Commitment

- 6.3.1 The senior management, including the Chief Executive Officer and the Board of Directors of IDCOL need to be committed to the development and enforcement of the anti-money laundering objectives.
- 6.3.2 The IDCOL Management also should be concern about taking necessary measures to assess and identify ML/TF risk related with the organization and place an appropriate mechanism to mitigate those risks.
- 6.3.3 The IDCOL need to establish a "Central Compliance Unit on AML/CFT" headed by sufficiently senior official in the rank who will directly report to the CEO/MD.
- 6.3.4 IDCOL Management should issue a message addressed to its all staff's to be cautious for preventing money laundering and terrorist financing at least once year. The compliance policy will be written, approved by the Board of Directors, and noted in the board meeting minutes. MD/CEO should also circulate AML Compliance Policy to its entire staff which includes:
 - i. A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.
 - ii. A statement that all activities carried on by IDCOL must comply with applicable governing laws and regulations.
 - iii. A statement that complying with rules and regulations is the responsibility of each individual in the organization 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 about the rules and regulations is no excuse for non-compliance.
 - iv. A statement that employees will be held accountable for carrying out their compliance responsibilities.

6.4 Organizational Structure

IDCOL constitutes a Central Anti-Money Laundering Compliance Committee headed by the Deputy Managing Director. The Concern Deputy Managing Director will also act as a Chief Anti Money Laundering Compliance Officer (CAMLCO).

The committees/teams/roles of IDCOL under Bangladesh Bank guideline & circulars regarding prevention money laundering & combating financing of terrorism are hereby formed:

Central Anti-Money Laundering Compliance Committee	<ul style="list-style-type: none"> a) Deputy Managing Director Chief Anti-Money Laundering Compliance Officer (CAMLCO) b) Chief Financial Officer c) Head of Renewable Energy d) Head of Investment & Advisory e) Head of Credit Management f) Head of Internal Control & Compliance
Deputy CAMLCO/BAMLCO/AMLCO	<ul style="list-style-type: none"> a) Mr. M. Maftun Ahmed, Company Secretary Deputy CAMLCO/BAMLCO b) Unit Heads, All Business Units - AMLCO c) Unit Heads, All Operations Units - AMLCO d) Unit Heads, All Risk Units - AMLCO
United Nations Security Council Resolutions (UNSCRs) implementation Committee	<ul style="list-style-type: none"> a) Unit Head, Credit Administration b) Unit Head, IT & MIS c) Unit Head, Legal Affairs
AML/CFT Review Team	<ul style="list-style-type: none"> a) Unit Head, Credit Risk Management b) Unit Head, Internal Audit c) Unit Head, Legal Affairs

6.4.1 Functions of Central Anti-Money Laundering Compliance Committee (CAMLCC):

- i. The Committee will review the Anti-Money Laundering policies regularly
- ii. It will update the legal, regulatory, business or operational changes including Anti Money Laundering rules or regulations as and when required but at least once a year.
- iii. It will recommend the necessary Anti-Money Laundering policies, procedures and controls so as to deter criminals from adopting various techniques of Money Laundering.

6.4.2 Functions of Chief Anti-Money Laundering Compliance Officer (CAMLCO):

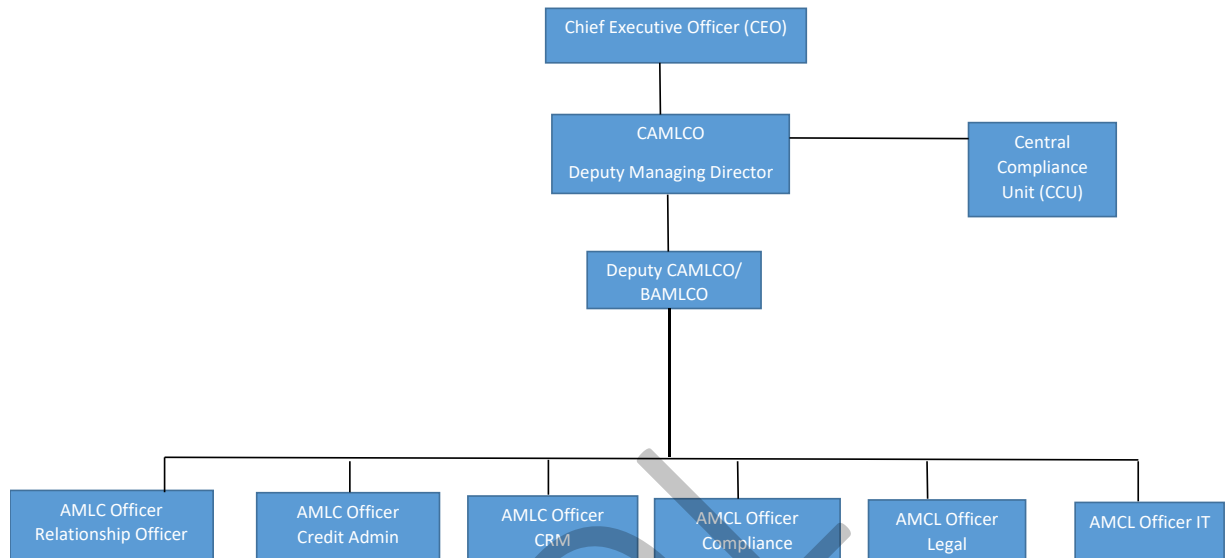
- i. He will issue Anti-Money Laundering circulars, instructions and circulate Bangladesh Bank Circulars and Policy Guidelines to the concerned offices of IDCOL.
- ii. He will monitor, review and coordinate, implement and enforces IDCOL's Anti-Money Laundering Compliance Policies.
- iii. He will take necessary actions for proper risk assessment of organization's existing and new product, services and delivery channel and in place appropriate tools to mitigate those risks.
- iv. He will formulate the policy and identification procedure "Know your Customer (KYC)" for detecting of suspicious transactions / account activities.
- v. He will respond queries of concerned offices of IDCOL (i.e. branches) so as to money laundering apprehensions.
- vi. He will report to Bangladesh Bank regarding suspicious transactions of the Clients accordingly.
- vii. He will issue necessary instructions for compliance.
- viii. He will keep the top Management informed about the issue.
- ix. He will ensure timely AML Reporting and Compliance to Bangladesh Bank.

- x. He will place Memorandum before the Board of Directors at least once a year regarding the status of the Anti-Money Laundering activities undertaken by IDCOL.
 - xi. He will extend all out cooperation to Internal Audit Team, Bangladesh Bank Audit Team and other Law enforcing Agencies as and when required.
- 6.4.3 Functions of BAMLCO:
- i. The BAMLCO will ensure that the AML is effective in the Branch and the AML Act, 2012, Bangladesh Bank circulars and guidelines are meticulously followed at all level.
 - ii. He will be responsible for educating and updating the Officers of the branch regarding AML issue, circulars and strategies.
 - iii. In the Monthly meeting of the Branch the AML agenda will come as an important one and the proceedings shall be recorded properly.
 - iv. In case of new Accounts the BAMLCO shall ensure that the policy and identification procedure “Know your Customer (KYC)” have been meticulously followed.
 - v. He will ensure the preservation of complete and up-to-date Account records of the Clients.
 - vi. He will ensure the periodical Reporting of AML issues to CCU.
 - vii. He will report the unusual / suspected cases to CCU for further advice and guidance.
 - viii. He will extend all sorts of cooperation to the Internal Audit team, Bangladesh Bank Audit and other Law enforcing Agencies.
- 6.4.4 Functions of Anti-Money Laundering Compliance Officer (AMLCO):
- i. The In-charge of Account Opening, Loan Processing desks / Units will monitor the transactions of the accounts.
 - ii. They will be called Anti-Money Laundering Compliance Officer (AMLCO).
 - iii. They will act in good faith, without negligence regarding any financial transactions, where there is no reasonable ground to believe that the transaction (s) is a laundered one.
 - iv. In case of new and existing Accounts the concerned Officer will follow the policy and identification procedure “Know your Customer (KYC)”.
 - v. They will have to be satisfied that the money involved in the transaction is not a laundered one.
 - vi. They must obtain documentary evidence of Large Cash Deposits or Inward Bills for collections.
 - vii. If necessary, he/they must take declaration letter from the client citing the source of fund to be routed to the account.
 - viii. Escalate any suspicion, report to the BAMLCO.
 - ix. They will in no way involve themselves in any transaction relating to Money Laundering.
 - x. Any crucial information shall not be disclosed to anyone except the BAMLCO.
 - xi. They will report to the BAMLCO.
- 6.4.5 Functions of Account Opening Officer/Relationship Officer:
- i. To perform due diligence on prospective Clients prior to opening an account.
 - ii. Shall be diligent regarding the identification of accountholder and the transaction to be made with IDCOL.
 - iii. Ensure that all required documentation is completed satisfactorily as per BB Guidelines.
 - iv. Complete the Client Information (KYC) profile.
 - v. In case of new accounts the concerned officer will follow the policy and identification procedure “Know your Customer (KYC)”.
 - vi. Any negative information regarding prospective client, from any source shall be taken into consideration and report to the BAMLCO.

- 6.4.6 The responsibilities of Internal Auditors are:
- i. Address the adequacy of AML/CFT risk assessment.
 - ii. Examine/attest the overall integrity and effectiveness of the management systems and the control environment.
 - iii. Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements.
 - iv. Determine personnel adherence to IDCOL's AML/CFT policies, procedures and processes.
 - v. Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations).
 - vi. Assess the adequacy of IDCOL's processes for identifying and reporting suspicious activity.
 - vii. Communicate the findings to the Board and/or Senior Management in a timely manner.
 - viii. Recommend corrective action for deficiencies.
 - ix. Track previously identified deficiencies and ensures that management corrects them.
 - x. Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
 - xi. Determine when assessing the training program and materials:
 1. The importance that the Board and the Senior Management place on ongoing education, training and compliance.
 2. Employee accountability for ensuring AML/CFT compliance.
 3. Comprehensiveness of training, in view of specific risks of individual business lines.
 4. Participation of personnel from all applicable areas of the organization.
 5. Frequency of training.
 6. Coverage of IDCOL's policies, procedures, processes and new rules and regulations.
 7. Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
 8. Penalties for noncompliance and regulatory requirements.
- 6.4.7 The responsibilities of IT & MIS Officer:
- i. Ensures that the required reports and systems are in place to maintain an effective program.
- 6.4.8 The responsibilities of Operations Staffs:
- i. Ensure that all control points are completed prior to transaction monitoring
 - ii. Be diligent on transaction trends for clients.
- 6.4.9 Role of Chief Executive Officer:
- i. Overall responsibility to ensure that the organization has the AML/CFT program in place and it is working effectively.
- 6.4.10 Role of External auditor is:
- i. External auditor shall play an essential part in reviewing the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External audit should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors.

6.4.11 The AML Organization chart of IDCOL is given below:

Anti-Money Laundering Organization Structure of IDCOL



BAMLCO=Branch* Anti-Money Laundering Compliance Officer
**Head Office to be considered as Principal Branch & Deputy CAMLCO will act as BAMLCO of H/Office*
AMLC = Anti-Money Laundering Compliance

6.5 Components of IDCOL's AML/CFT policies

In line with the Money Laundering Prevention Act, 2012, Anti-Terrorism (amendment) Act, 2009, Bangladesh Bank's circulars and guidelines on AML/CFT and considering the business and products of the organization, IDCOL's AML/CFT policy comprises of the following elements:

- Senior Management Commitment.
- Customer Acceptance Policy.
- Sound KYC policy.
- Suspicious Transaction detection and reporting mechanism.
- Record keeping.
- Training and awareness building.
- Assessment and Audit function.

Chapter Seven: Identification Procedures

7.1 Introduction

- 7.1.1 Sound Know Your Customer (KYC) procedures are critical elements in the effective management of banking risks. KYC safeguards go beyond simple account opening and recordkeeping and require FIs to formulate a customer acceptance policy and a tiered customer identification program that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.
- 7.1.2 Sound KYC procedures have particular relevance to the safety and soundness of financial institutions, in that:
- i. they help to protect financial institution's reputation and the integrity of banking systems by reducing the likelihood of banks/FIs becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
 - ii. they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).
- 7.1.3 The inadequacy or absence of KYC standards can subject FIs to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to FIs (e.g. through the withdrawal of funds by depositors, claims against the FIs, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.
- 7.1.4 Reputational risk poses a major threat to FIs, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a FI's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. FIs are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC program. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.
- 7.1.5 Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of FIs' programs, ineffective control procedures and failure to practice due diligence. A public perception that a FI is not able to manage its operational risk effectively can disrupt or adversely affect the business of the FI.
- 7.1.6 Legal risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a FI. FIs may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, FIs can, for example, suffer fines, criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving a FI may have far greater cost implications for its business than just the legal costs. FIs will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.
- 7.1.7 On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the FI's liquidity. Funding risk is more likely to be higher in the case of small

FIs and those that are less active in the wholesale markets. Analyzing deposit concentrations requires FIs to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small FIs not only know but also maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

- 7.1.8 Customers frequently have multiple accounts with the same FI, but in offices located in different areas. To effectively manage the reputational, compliance and legal risk arising from such accounts, FIs should be able to aggregate and monitor activity in these accounts on a fully consolidated countrywide basis.

7.2 Know Your Customer (KYC) Policies and Procedures

7.2.1 Features of a sound KYC

Having sufficient information about your customer - "knowing your customer" (KYC) - and making use of that information underpins all AML/CFT efforts, and is the most effective defense against being used to launder the proceeds of crime. If a customer has established an account 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 the proceeds of which the institution is being used to launder. A false name, address or date of birth will usually mean that law enforcement agencies cannot trace the customer if s/he is needed for interview as part of an investigation.

- 7.2.2 Section 25 (1) (a) Ka of the Prevention of Money Laundering Act 2012 requires all institutions to seek *satisfactory evidence* of the identity of those with whom they deal (referred to in these Guidance Notes as verification of identity). Unless satisfactory evidence of the identity of potential customer is obtained in good time, the business relationship must not proceed.
- 7.2.3 When a business relationship is being established, the nature of the business that the customer 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 customers.
- 7.2.4 The Branches of the FIs must establish its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally.
- 7.2.5 The verification procedures need to establish the identity of a prospective customer should basically be the same whatever the type of account or service is required. The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that every institution must know who their customers are, and have the necessary documentary evidence to verify this.
- 7.2.6 Section 25 (1) (a) Ka of the Prevention of Money Laundering Act 2012 requires that all records including the records of the verification of identity must be retained for 05 (five) years after an account is closed or the business relationship ended.

7.3 Customer Acceptance Policy

7.3.1 Introduction

Customers are vitally important for banking business. Increasing competition is forcing FIs to pay much more attention to satisfy customers. IDCOL is also aware that sometimes customers pose the risk of money laundering and financing of terrorism. So the inadequacy or absence of KYC standards can result in serious customer and counterparty risks, especially reputation, operational, legal and compliance risks.

Collecting sufficient information about our customers is the most effective defense against being used as the medium to launder the proceeds of crimes and to finance the terrorism through banking channel. As per Sec. 25 Clause (a) & (d) of Anti-Money Laundering Act, 2012 each FI requires to keep correct and complete evidence of the identity of those it deals with and also requires making necessary arrangement to prevent any transaction related to crimes as described in Anti-Terrorism Act, 2013.

7.3.2 Definition of customer

Broadly, a customer can be defined as a user or potential user of FI's services. So defined, a 'Customer' may include:

- i. A person or entity that maintains an account and /or has a business relationship with the FI.
- ii. One on whose behalf the account is maintained, i.e. beneficial owner. 'Beneficial owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person.
- iii. Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- iv. Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the FI.

7.3.3 It is also the responsibility of the FI to identify suspicious transactions of their customers with due care and diligence. Pursuant to above legal bindings, Guidance Notes on Prevention of Money Laundering and Terrorist Financing issued by Bangladesh Bank and apropos to international standard the Management of IDCOL has developed the Customer Acceptance Policy as under:

i. Due Diligence requirements

1. IDCOL shall not open accounts or deal with customers of un-known identity or have fictitious or unreal or anonymous names.
2. IDCOL shall not open an account, where the FI is unable to apply appropriate customer due diligence measures i.e. IDCOL is unable to verify the identity and/or obtain documents required due to non-cooperation of the customer or non-reliability of the data/information furnished to the relevant officials. But the officer must be careful to avoid unnecessary harassment of the customer.
3. IDCOL shall not establish any relationship with persons/entities found/available in the UN/OFAC Sanction List.
4. Staff should identify and verify the customer's and actual beneficiary's identity whether the customer is a natural or juridical person.
5. Staff should apply due diligence procedures for customers and actual beneficiaries in case IDCOL has any suspicion in respect of accuracy or adequacy of the information obtained in relation to the customer's identity.
6. Establishing continuous business relationship with new customers.

7. In case of opening a Politically Exposed Person's (PEP) account, Influential Person's Account or Account of a High Official of an International Organization; the FI shall comply the instructions contained in BFIU Circular No. 12 dated 29.06.2015 issued by Bangladesh Bank, FATF (40+9) Recommendations and IDCOL's Policy for Politically Exposed Persons (PEPs). Such types of account will be classified as high risk and will be required very high level monitoring.
8. At the time of opening new account IDCOL must take care to seek only such information from the customer which is relevant and is not intrusive. It is mentioned that the customer profile is a confidential document and the details contained therein shall not be divulged for any other purposes.
9. Source of funds, income or wealth and complete information on the actual or beneficial owners of the accounts holding 20% or more share of the account must be obtained at the time of opening of any account.
10. IDCOL will conduct necessary checks before opening a new account or establishing a new relationship so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
11. IDCOL will strive not to cause inconvenience to the general public, especially those who are financially or socially disadvantaged.
12. IDCOL shall verify the identity of the customers using reliable sources, documents etc. but it must retain copies of all references, documents used to verify the identity of the customer.
13. IDCOL should not enter into a business relationship or execute any transactions before applying due diligence procedures stipulated in these instructions.
14. IDCOL may postpone the verification of the customer's identity until after the establishment of the business relationship provided that the verification should happen as soon as possible and that this postponement is necessary for the business requirement, and provided there is control on the risk of money.
15. In case IDCOL enters in a business relationship with the customer and could not complete the verification procedures, it should terminate this relationship and consider notifying the Central Compliance Unit (CCU).
16. IDCOL should update the customer's identification information periodically and every 5 years at the maximum, taking into consideration the customer's risk level, and in the event of any doubt about the identity information or about the customer himself. IDCOL should obtain a declaration from the customer determining the actual beneficiary and informing the FI of any change in his personal data, and an undertaking that he shall provide IDCOL with the relevant supporting documents.
17. IDCOL shall not enter into any banking relationship with any shell bank.

7.3.4 **Risk perception:** Parameters of risk perception which are used to determine the profile and risk category of a customer are as follows :

- i. Customers' constitution: Individual, proprietorship, partnership, public or private ltd. etc.
- ii. Business segment.
- iii. Product subscription.
- iv. Geographical location.
- v. Country of residence/ Nationality: Whether Bangladeshi or any overseas location.
- vi. Economic profile: High net worth individual, Public limited Co. etc.
- vii. Relationship status: New, Existing etc.

- viii. Presence in regulatory negative/ PEP/Defaulter/Fraudster etc.
- ix. Suspicious Transaction Report (STR) filed for the customer.
- x. AML alerts.

7.4 Customer Identification

- 7.4.1 Customer identification is an essential element of KYC standards. For the purposes of this Guidance Notes, a customer includes:
- i. The person or entity that maintains an account with IDCOL or those on whose behalf an account is maintained (i.e. beneficial owners);
 - ii. The beneficiaries of transactions conducted by professional intermediaries; and
 - iii. Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to IDCOL.
- 7.4.2 The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for IDCOL to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if IDCOL becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.
- 7.4.3 Whenever the opening of an account or business relationship is being considered, identification procedures must be followed. Identity must also be verified in all cases by applying appropriate measures.
- 7.4.4 Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained as set out Section 25 of MLPA, 2012, and information should be updated or reviewed as appropriate.
- 7.4.5 Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, body corporate, partnership, etc.). For the purposes of this guidance, the two elements are:
- i. The physical identity (e.g. name, date of birth, TIN/voter registration/passport/ID number, etc.); and
 - ii. The activity undertaken.

7.5 Individual Customers

- 7.5.1 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 IDCOL itself:
- i. True name and/or names used;
 - ii. Parent's names;
 - iii. Date of birth;
 - iv. Current and permanent address;
 - v. Details of occupation/employment; and
 - vi. Sources of wealth or income
- 7.5.2 One or more of the following steps is recommended to verify the recorded addresses:
- i. Provision of a recent utility bill, tax assessment or bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are to be examined);
 - ii. Checking the NID or Voter lists;

- iii. Checking the telephone directory;
 - iv. Record of home/office visit.
 - v. Mailing thanks letter etc.
The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is the propose person which account is going.
- 7.5.3 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, it will provide an additional safeguard.
- 7.5.4 Identification documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:
- i. National ID Card;
 - ii. Current valid passport;
 - iii. Valid driving license;
 - iv. Armed Forces ID card;
 - v. A Bangladeshi employer ID card bearing the photograph and signature of the applicant; or A certificate from any local government organizations such as Parishad Council chairman, Ward Commissioner, etc. or any respectable person acceptable to the institution.
 - vi. Any identification documents with photo.
- 7.5.5 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.
- 7.5.6 Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm the address and personal identity. At least one additional check should be undertaken to guard against impersonation.
- 7.5.7 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.
- 7.5.8 Any subsequent change to the customer's name, address, or employment details of which IDCOL becomes aware should be recorded as part of the know your customer process.
- 7.5.9 File copies of supporting evidence should be retained. The relevant details should be recorded on the applicant's file.
- 7.5.10 An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file.

7.6 Corporate Bodies and other Entities

- 7.6.1 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. IDCOL 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.

- 7.6.2 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, wound-up or terminated.
- 7.6.3 Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh.
- 7.6.4 No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.
- 7.6.5 The following documents should normally be obtained from companies:
- i. Certified true copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
 - ii. Certified true copy of the Memorandum and Articles of Association, or by-laws of the client;
 - iii. Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
 - iv. 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;
 - v. Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 20% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
 - vi. 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;
 - vii. Subsequent changes to signatories must be verified;
 - viii. Copies of the list/register of directors;
 - ix. Two recent photographs of the Account operators duly attested by the Company Official / Secretary.
- 7.6.6 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.
- 7.6.7 The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:
- i. All of the directors who will be responsible for the operation of the account / transaction.
 - ii. All the authorized signatories for the account/transaction.
 - iii. All holders of powers of attorney to operate the account/transaction.
 - iv. The beneficial owner(s) of the company.
 - v. The majority shareholders of a private limited company.
- 7.6.8 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.

7.7 Partnerships and Unincorporated Businesses

- 7.7.1 In the case of partnerships and other unincorporated businesses whose partners/directors are not known to IDCOL, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account relationship and conferring authority on those who will operate it should be obtained.
- 7.7.2 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).
- 7.7.3 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.

7.8 Powers of Attorney/ Mandates to Operate Accounts

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

7.9 Identification of Beneficial Owners and Verification of their Identities

7.9.1 What is a beneficial owner?

The term “beneficial ownership,” when used to refer to favorable rights of an account in an AML context (such as the Principles), is usually understood as connecting to ultimate Control over funds in such account, whether through ownership or other means. “Control” in this sense is to be distinguished from mere signature authority or legal title.

The term reflects a recognition that a person in whose name an account is opened with IDCOL is not necessarily the person who ultimately controls such funds.

Beneficial Owner means the individual who –

- i. has effective control of a customer or person on whose behalf a transaction is conducted; or
- ii. owns a prescribed threshold of the customer or person on whose behalf a transaction is conducted.

Therefore the beneficial owner can only be an individual, not a company or organization. There may be more than one beneficial owner associated with the customers. The aim of this task is to identify and verify the identity of all the beneficial owners of customers of IDCOL.

7.9.2 The assessment process to identify beneficial ownership

- i. IDCOL should have to apply the following 3(Three) elements to assess the beneficial ownership:
 - 1. Who owns more than 20 percent of the assets related/connected account?
 - 2. Who has effective control of the account/customer?
 - 3. The persons on whose behalf a transaction is conducted. A beneficial owner is an individual who satisfies any one element, or any combination of the three elements.
- ii. If the customer of IDCOL is an individual, he/she has been treated as the beneficial owner unless there are reasonable grounds to suspect that he/she is operating the activities or controlling the funds on behalf of another individual/entity/organization etc. If the customer is acting on behalf of another individual/entity/organization etc., IDCOL shall have to ensure due diligence to collect the identity of that beneficial owner.
- iii. There shall be individuals who have effective control over the customer, but do not have an ownership interest and are not a person on whose behalf a transaction is conducted;

they will be beneficial owners. Effective control, ownership and persons on whose behalf a transaction is conducted are not mutually exclusive.

7.9.3 **Enhanced Due Diligence**

- i. To start new relationship or to continue pre-existing relationships, IDCOL shall have to identify and verify the identity of the beneficial owner(s). IDCOL should have to establish the customer's ownership structure and understand the ownership at each layer. The beneficial owner is not necessarily one individual; there may be several beneficial owners in a structure. When there are complex ownership layers and no reasonable explanation for them IDCOL should consider the possibility that the structure is being used to hide the beneficial owner(s).
- ii. IDCOL shall to monitor the transactions and to stop at any point in the process or activities of the account. However, if identification and verification of the identity of the beneficial owner(s) is not obtained and due diligence has not been completed IDCOL shall not establish any business relationship or conduct any occasional transaction for the customer. Risk-based approach shall also be applied to verify the identity.
- iii. IDCOL shall consider obtaining an undertaking or declaration from the customer on the identity and the information relating to the beneficial owner. For example, where the customer is a portfolio manager. In that situation, as well as other instances where the customer has a *bonafide* and legitimate interest or duty not to disclose to the FI the identity or particulars of beneficial owners who are known to exist, IDCOL shall consider the application of simplified CDD.
- iv. The Authority recognizes 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 a 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.

7.9.4 **Applying a risk-based approach**

- i. The assessment procedures allows to adopt a risk-based approach to verify beneficial ownership of the accounts/customers. Identifying beneficial ownership of a customer is an obligation that must be satisfied by IDCOL, regardless of the level of risk associated with that account/customer. However, reasonable steps to take to satisfy about identity and information of customers/account is correct. The process for assessing customer risk and identification, must be based on guidelines of AML/CFT risk assessment.
- ii. A risk-based approach allows us some flexibility in FI's obligation to use data, documents or information obtained from a reliable and independent source to verify the identity of the beneficial owner(s) of the customers/accounts. This is applied on case to case basis. For example, a well-known local businessman/individual wants to be customer of IDCOL. IDCOL shall have to identify both the customer and the beneficial owner(s) first and then shall have to obtain standard identity documentation as per account opening instructions and AML/CFT policy of IDCOL. Risk assessment shall also to be made to segregate the account/customer. If the customer/account found as higher risk, IDCOL shall also apply Enhanced Customer Due Diligence, in such case IDCOL also shall have to obtain information relating to the source of funds or wealth of the customer/account. Verification of the identity of the beneficial owner(s) is the last step in the process.

7.9.5 **Suspicious Transaction Report (STR)**

IDCOL shall have to be satisfy of the all level of risk associated with beneficial ownership of account/customer, Where there are reasonable grounds for suspicion of money laundering or terrorist financing, IDCOL should also apply Enhanced Customer Due Diligence and shall report a Suspicious Transaction Report (STR) to the Central Compliance Unit (CCU).

7.9.6 **Record keeping**

Detailed records of all information, decisions, Customer Due Diligence and relevant records shall be maintained. It is important for the FI to record the justification behind any decision that are taken.

7.10 Reliability of Information and Documentation

7.10.1 Where IDCOL obtains information or documents from the customer 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 IDCOL.

7.10.2 Where the customer is unable to produce original documents, IDCOL may consider accepting documents that are certified to be true copies by qualified persons, such as lawyers and accountants.

7.11 Non-Face-to-Face Verification

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

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

- i. telephone contact with the customer through residential or business contact number that can be verified independently;
- ii. Confirmation of the customer's address through an exchange of correspondence or other appropriate method;
- iii. Subject to the customer's consent, telephonic confirmation of the customer's employment status with the customer's employer's personnel department at a listed business number of the employer;
- iv. Confirmation of the customer's salary details by requiring the presentation of recent bank statements from a bank;
- v. Certification of identification documents by lawyers or notary publics presented by the customer; and
- vi. Any other reliable verification checks adopted by IDCOL for non-face-to-face business.

7.12 Timing and Duration of Verification

7.12.1 The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed.

7.12.2 However, if it is necessary for sound business reasons to carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority.

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

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

7.13 Simplified Customer Due Diligence

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

7.13.2 IDCOL 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 IDCOL adopt such lesser or reduced CDD measures, such measures should be commensurate with its assessment of the risks. Examples of when IDCOL might adopt lesser or reduced CDD measures are: - Where reliable information on the customer is publicly available to the FIs; - IDCOL is dealing with another financial institution whose AML/CFT controls is well familiar with by virtue of a previous course of dealings; or -The customer 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.

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

7.13.4 Where the risks of money laundering or terrorist financing are lower, concern of IDCOL could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- ii. Reducing the frequency of customer identification updates.
- iii. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- iv. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.
- v. Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

7.14 Enhanced CDD Measures

7.14.1 IDCOL should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, IDCOL should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, IDCOL should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- i. Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- ii. Obtaining additional information on the intended nature of the business relationship.
- iii. Obtaining information on the source of funds or source of wealth of the customer.
- iv. Obtaining information on the reasons for intended or performed transactions.
- v. Obtaining the approval of senior management to commence or continue the business relationship.
- vi. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- vii. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

7.15 Politically Exposed Persons

“Politically Exposed Persons” (PEPs) is someone who has been entrusted with a prominent public function, or an individual who is closely related to such a person of local government or from 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 terms PEPs defined not only including the senior persons associated with foreign country but also middle-ranking or more junior individuals in the categories defined or officials of local governments.

7.15.1 Identifying PEPs

Politically Exposed Persons (PEPs) as contained in BFIU circular no. 12 dated June 29, 2015 is described as under –

“Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials”.

The description as detailed for PEPs shall equally apply if business relationship is established with the family members and close associates of these persons both from home and abroad who may pose reputational risk to IDCOL.

As per FATF, PEPs refers –

- i. Foreign PEPs are individuals who are or have been entrusted with prominent public functions by 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.
- ii. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
- iii. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

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 PEPs. Another important thing is that not only customer, a PEP but also may be a beneficial of an account.

7.15.2 **Initiating business relationship and Operating the account of PEP(s) –**

A risk management system shall have to be followed to identify risks associated with starting business relationship with PEPs. The following instructions shall have to be followed to ensure Enhanced Due Diligence (EDD), while initiating business relationship with Politically Exposed Persons (PEPs):

- i. Obtain senior management approval for establishing business relationships with such Foreign PEPs. In case of Domestic PEPs prior approval of Senior Management is not required but Enhanced Due Diligence (EDD) should be applied;
- ii. Take reasonable measures to establish the source of wealth and source of funds;
- iii. Ongoing monitoring of the transactions have to be conducted; and
- iv. IDCOL shall have to observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while initiating business with non-residents;
- v. The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

7.15.3 **Risk Assessment**

PEPs accounts must be marked as **High Risk** accounts and consider the followings while opening and maintaining the accounts of any PEPs, IDCOL must:

- i. Whether the customer or the beneficial owner is a Politically Exposed Person;
- ii. Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships with Foreign PEPs;
- iii. Take reasonable measures to establish the source of wealth and source of funds; and Conduct enhanced ongoing monitoring Enhanced Due Diligence (EDD) of the business relationship.

A database of the account of the PEPs to be maintain for ongoing monitoring of the transactions from time to time.

7.16 Other High Risk Categories

7.16.1 Enhanced CDD measures to be applied to other categories of customers apart from PEPs, which IDCOL may consider to present a greater risk of money laundering or terrorist financing. In assessing the risk of money laundering or terrorist financing, IDCOL may take into account factors such as the type of customer, the type of product that the customer purchases, the geographical area of operation of the customer's business.

7.16.2 IDCOL is also required to give particular attention to business relations and transactions with persons from or in countries that have inadequate AML/CFT measures. For this purpose, IDCOL may take a range of steps, including the adoption of measures similar to those for PEPs and other high risk categories.

7.16.3 While the Authority may from time to time circulate names of countries and jurisdictions with inadequate AML/CFT regimes (which can then be used as a reference guide), IDCOL officials are also encouraged to refer, where practicable, to other sources of information to identify countries and jurisdictions that are considered to have inadequate AML/CFT regimes.

7.17 Performance of CDD Measures

7.17.1 Where IDCOL wishes to rely on an intermediary to perform elements of the CDD measures, IDCOL requires 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 been measured and taken in place to comply with the requirements.

- 7.17.2 IDCOL may take a variety of measures, including but not limited to the following in determining whether the intermediary satisfies the requirements:
- i. 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 associated bodies, or assessment reports made under the Financial Sector Assessment Programmed of the International Monetary Fund and the World Bank);
 - ii. Referring to any publicly available reports or material on the quality of that intermediary's compliance with applicable AML/CFT rules;
 - iii. 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;
 - iv. Examining the AML/CFT laws in the jurisdiction where the intermediary operates and determining its comparability with the AML/CFT laws of Bangladesh.
- 7.17.3 To the extent that the performance of CDD is undertaken by the intermediary rather than by IDCOL, it is required to immediately obtain from the intermediary the information relating to CDD obtained by the intermediary.
- 7.17.4 In addition, where the IDCOL relies on the intermediary to undertake the performance of CDD, it should be able to justify that the conditions of above paragraph have been met. IDCOL should take considerable care when deciding if an intermediary is one on whom it can safely rely on to perform the CDD measures.

7.18 Risk Based Approach (RBA)

- 7.18.1 IDCOL understand the Risk Based Approach (RBA) essential for mitigating or minimizing AML/CFT risk. IDCOL management has also concern about the high risk or low risk situation arising from type of product, customer, services, transaction or delivery channel.
- 7.18.2 The central Compliance unit of IDCOL requires to assess AML/CFT risk arises from different type of products, services or delivery channel. Such assessment should be undertaken for each type of existing products, services or delivery channels and newly introduce ones as well.
- i. **Higher Risk scenario**
 The examples below are included for guidance of the staff of IDCOL only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances. Where the risk of money laundering or terrorist financing considered is higher, enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:
 1. **Customer risk factors:**
 - a. The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
 - b. Non-resident customers.
 - c. Legal persons or arrangements that are personal asset-holding vehicles.
 - d. Companies that have nominee shareholders or shares in bearer form.
 - e. Business that are cash-intensive.
 - f. The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
 2. **Country or geographic risk factors:**

- a. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
 - b. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
 - c. Countries identified by credible sources as having significant levels of corruption or other criminal activity.
 - d. Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.
3. **Product, service, transaction or delivery channel risk factors:**
- a. Private banking.
 - b. Anonymous transactions (which may include cash).
 - c. Non-face-to-face business relationships or transactions.
 - d. Payment received from unknown or un-associated third parties

ii. **Lower Risk scenario**

There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by IDCOL, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

1. **Customer risk factors:**
- a. Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
 - b. Public Limited companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
 - c. Public administrations or enterprises.
2. **Product, service, transaction or delivery channel risk factors:**
- a. Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
 - b. Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.
 - c. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
 - d. Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.
3. Country risk factors:

- a. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- b. Countries identified by credible sources as having a low level of corruption or other criminal activity.
- c. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.
- d. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

7.19 Risk grading

- 7.19.1 Relevant officials of IDCOL required to perform due diligence on all prospective clients prior to opening an account or establishing business relationship. This process is completed by fulfilling the documentation requirements and also a 'Know Your Customer' profile which is used to record a client's source of wealth, expected transaction activity at its most basic level.
- 7.19.2 Once the identification procedures have been completed and the client relationship is established, IDCOL should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened. IDCOL will do this firstly by their staff being diligent, reporting suspicious transactions undertaken by the customer, updating the client's KYC profile for any significant changes in their lifestyle (e.g., change of employment status, increase in net worth) and by monitoring the transaction activity over the client's account on a periodic basis.
- 7.19.3 KYC profile gives the basic information about the customer like, Name, Address, Tel/Fax Numbers, line of business, Annual sales. If the customer is a Public Figure, the account will become automatically a High Risk Account.
- 7.19.4 The KYC Profile information will also include the observations of IDCOL's Staff/Officer when they visit the customer's business place like, the business place is owned or rented, the type of clients visited, by what method is the client paid (cheque or cash). The Staff/Officer will record his observations and sign the KYC Profile form.
- 7.19.5 In the case of high net worth Accounts, the information will include net worth of the customer, source of funds etc.
- 7.19.6 The KYC Profile leads to Risk Classification of the Account as High/Low Risk.



- 7.19.7 When opening accounts, the concerned staff/Officer must assess the risk keeping it in mind that the accounts could be used for "money laundering", and must classify the accounts as either High Risk or Low Risk. (Annexure M)
- 7.19.8 KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for "High Risk" accounts. There is no requirement for periodic updating of profiles for "Low Risk" transactional accounts. These should, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern.

7.19.9 IDCOL have to introduce a risk registrar for calculating the risk of existing products, services and delivery channels and also need to be done risk assessment in advance for its future products, services and delivery channels.

7.20 Know Your Customer's Customer (KYCC)

7.20.1 Enhance due diligence is required to be in practice to Know Your Customer's Customer ensuring the highest level of compliance in AML & CFT issues. KYCC has become the most important tool for identification/verification of the customer's business. It is essential to find out the customer's customer to whom they are dealing with. On the other hand, Customers close association or family members or beneficiary of the account should be known in too.

7.20.2 IDCOL should-

- i. Take a list with the true identification like name, address, type of business, etc. of customer's customer;
- ii. Review the given list and check the background of the customer's customer at least half yearly basis if necessary;
- iii. Monitor the transaction occurred by the customer's customer if necessary;
- iv. Monitor the customer's customer business indirectly if necessary.

7.21 Know Your Employee (KYE)

7.21.1 Institutions and businesses learn at great expense that an insider can pose the same ML/TF threat as a customer. It has become clear in the field that having co-equal programs to know your customer and to know your employee is essential/vital. In an effort to identify and anticipate trouble before it costs time, money and reputational damage/risk. IDCOL should develop program to look closely at the people inside their own organizations.

7.21.2 A Know Your Employee (KYE) program means that the institution has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control, and other deterrents/restrictions should be firmly in place

7.21.3 Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. It can be used effectively, the pre-employment background checks/examines may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. IDCOL should verify that contractors are subject to screening procedures.

7.21.4 The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications. The extent of the screening depends on the circumstances, with reasonableness the standard as well as source of income.

Chapter Eight: Record Keeping

8.1 Statutory Requirement

- 8.1.1 The requirement contained in Section 25 (1) of Money Laundering Prevention Act, 2012, to retain correct and full records of customers' identification and transactions while operating an account of a customer, and to retain the records of customers' identification and transactions at least for five years after closing of relationships with the customers are essential/important constituents of the audit trail that the law seeks to establish.
- 8.1.2 FATF recommendation 11 states that financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.
- 8.1.3 The records prepared and maintained by IDCOL on its customer relationship and transactions should be such that:
- i. requirements of legislation and Bangladesh Bank directives are fully met;
 - ii. competent third parties will be able to assess the IDCOL's observance of money laundering policies and procedures;
 - iii. any transactions effected via IDCOL can be reconstructed;
 - iv. any customer can be properly identified and located;
 - v. all suspicious reports received internally and those made to Bangladesh Bank can be identified; and
 - vi. IDCOL can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.
- 8.1.4 Records relating to verification of identity will generally comprise:
- i. a description of the nature of all the evidence received relating to the identity of the verification subject;
 - ii. the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.
- 8.1.5 Records relating to transactions will generally comprise:
- i. details of personal identity, including the names and addresses, etc. pertaining to:
 1. the customer;
 2. the beneficial owner of the account or product;
 3. the non-account holder conducting any significant one-off transaction;
 4. any counter-party;
 - ii. details of transaction including:
 1. nature of such transactions;
 2. volume of transactions customer's instruction(s) and authority(ies);
 3. source(s) of funds;
 4. destination(s) of funds;
 5. book entries;
 6. custody of documentation;
 7. date of the transaction;
 8. form in which funds are offered and paid out;
 9. parties to the transaction;
 10. identity of the person who conducted the transaction on behalf of the customer.

- 8.1.6 These records of identity must be kept for at least five years from the date when the relationship with the customer has ended. This is the date of:
- i. closing of an account
 - ii. providing of any financial services
 - iii. carrying out of the one-off transaction, or the last in a series of linked one-off transactions;
or
 - iv. ending of the business relationship; or
 - v. commencement of proceedings to recover debts payable on insolvency.
- 8.1.7 IDCOL should ensure that records pertaining to the identification of the customer, his/her address (e.g. copies of documents like passport, national ID card, driving license, trade license, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended and should be made available to the competent authorities upon request without delay.

8.2 Retrieval of Records

- 8.2.1 To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of IDCOL, provided that it has reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduced and recollected without undue delay.
- 8.2.2 It is not always necessary to retain documents in their original hard copy form, provided that the procedures are reliable for holding records in electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, IDCOL may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on IDCOL itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.
- 8.2.3 However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

8.3 STR and Investigation

- 8.3.1 Where IDCOL has submitted a report of suspicious transaction to BFIU or where it is known that a customer or any transaction is under investigation, it should not destroy any records related to the customer or transaction without the consent of the BFIU or conclusion of the case even though the five-year limit may have been elapsed. To ensure the preservation of such records IDCOL should maintain a register or tabular records of all investigations and inspection made by the investigating authority or Bangladesh Bank and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:
- i. the date of submission and reference of the STR/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.

8.4 Training Records

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

- i. details of the content of the training programs provided;
- ii. the names of staff who have received the training;
- iii. the date/duration of training;
- iv. the results of any testing carried out to measure staffs understanding of the requirements; and
- v. an on-going training plan.

8.5 Branch Level Record Keeping

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

- i. Information regarding Identification of the customer,
- ii. KYC information of a customer,
- iii. Transaction report,
- iv. Suspicious Transaction/Activity Report generated from the branch,
- v. Exception report,
- vi. Training record,
- vii. Return submitted or information provided to the Head Office or competent authority.

8.6 Sharing of Record/Information of/to a Customer

8.6.1 Under MLPA 2012, and ATA, 2009 (as amended in 2012), IDCOL shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Bank.

Chapter Nine: Transaction Monitoring & Reporting

9.1 Reporting requirements

- 9.1.1 Reporting agencies are required by the AML/CFT legislation in Bangladesh to report to the Bangladesh Financial Intelligence Unit (BFIU) Bangladesh Bank. Most of such reports derive from transaction monitoring. Such as :
- i. Cash Transaction Report (CTR);
 - ii. Suspicious Transaction Report (STR);or
 - iii. Any other threshold based report.

9.2 Cash Transaction Reports (CTRs)

- 9.2.1 IDCOL is required to submit CTR to the BFIU, Bangladesh Bank on monthly basis. CTR is significantly different from abnormal/suspicious transactions reporting (STR). That is, if any customer happens to make transaction above 10 lacs taka or more, there is no scope of treating it as suspicious only for this. But IDCOL has to report CTR to BFIU, Bangladesh Bank for information only.
- 9.2.2 In the case of cash deposit (regardless of amount) of the Govt. accounts or of accounts of the Govt. owned entities need not to be reported. CTR must be submitted in soft copy. So concerned officials of IDCOL are required to submit CTR to the CCU by the 1st week of every month. After receiving such reports, CCU will compile all the CTRs and send it to the BFIU before 21st day of every month.

9.3 Suspicious Transaction Reports (STRs)

- 9.3.1 IDCOL will have regular monthly or fortnightly meeting and have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring for IDCOL is to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts.
- 9.3.2 It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. IDCOL has already developed a corporate compliance culture, and has properly trained, vigilant staff who will form an effective monitoring method through their day-to-day dealing with customers.
- 9.3.3 IDCOL will look for a computer systems specifically designed to assist the detection of fraud and money laundering. Until then, IDCOL will continue detecting fraud and money laundering from the available information in the system.
- 9.3.4 Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. Ideally any deviation from the normally expected TP should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account.
- 9.3.5 On a monthly basis the IDCOL shall prepare an exception report of customers based on Anti-Money Laundering risk assessment exercise.
- 9.3.6 Account Officers/Relationship Managers or other designated staff will review and sign-off on such exception report of customers whose accounts shows one or more individual account transaction during the period that exceeded the “transaction limit” established for that category of customer. The concerned staff will document their review by initial on the report, and where necessary he will prepare internal Suspicious Activity Reports (SARs) with action

plans approval by the BAMLCO/Deputy CAMLCO. A copy of the transaction identified will be attached to the SARs.

- 9.3.7 AMLCO will review the Suspicious Activity Reports (SARs) and responses from the Account Officers /Relationship Managers or other concerned staff. If the explanation for the exception does not appear reasonable then the BAMLCO should review the transactions prior to considering submitting them to the Deputy CAMLCO or CAMLCO.
- 9.3.8 If the BAMLCO and / or AMLCO that believe the transaction should be reported then the AMLCO will supply the relevant details to the Deputy CAMLCO or the CAMLCO.
- 9.3.9 The Deputy CAMLCO and CAMLCO will investigate any reported accounts and will send a status report on any of the accounts reported. No further action should be taken on the account until notification has been received.
- 9.3.10 If, after confirming with the client, the transaction trend is to continue the Account Officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly.

9.4 Recognition of Suspicious Transactions

- 9.4.1 As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. It is more than the absence of certainty that someone is innocent. A person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.
- 9.4.2 Questions that a relevant official must consider when determining whether an established customer's transaction must be suspicious are:
 - i. Is the size of the transaction consistent with the normal activities of the customer?
 - ii. Is the transaction rational in the context of the customer's business or personal activities?
 - iii. Has the pattern of transactions conducted by the customer changed?
 - iv. Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?
- 9.4.3 Examples of what might constitute suspicious transactions are given by types of business in Annexure. **These are not intended to be exhaustive and only provide examples of the most basic way by which money may be laundered.** However, identification of any of the types of transactions listed in Annexure C should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

9.5 Suspicious Activity Reporting Process

- 9.5.1 FIs must establish written internal procedures so that, in the event of a suspicious activity being discovered, all staff is aware of the reporting chain and the procedures to follow. Such procedures should be periodically updated by CCU to reflect any regulatory changes.
- 9.5.2 BAMLCO/Deputy CAMLCO must ensure that staff report all suspicious activities, and that any such report be considered in the light of all other relevant information by the AMLCO, or by another designated person, for the purpose of determining whether or not the information or other matter contained in the report does give rise to a knowledge or suspicion.
- 9.5.3 Where staff continues to encounter suspicious activities on an account, which they have previously reported to the AMLCO, they should continue to make reports to the AMLCO whenever a further suspicious transaction occurs, and the BAMLCO will determine whether a

disclosure in accordance with the regulations is appropriate. In that case attached internal reporting format (Annexure –D) may be used.

9.5.4 All reports of suspicious activities must reach the CAMLCO and only the CAMLCO should have the authority to determine whether a disclosure in accordance with the regulation is appropriate. However, the BAMLCO/Deputy CAMLCO can be permitted to add his/her comments to the suspicion report indicating any evidence as to why he/she believes the suspicion is not justified.

9.5.5 The listed below are the possible suspicious activity which require to be reported to BFIU as per AML Circular:

Bribery/Gratuity, Wire Transfer Fraud, False statement, Check Fraud, Counterfeit debit/credit card, Identity Theft, Check Kiting, Credit/ Debit card fraud, Consumer loan fraud, Commercial loan fraud, Defalcation/Embezzlement, Structuring, Mysterious Disappearance, Computer intrusion, Counterfeit instrument, Terrorist Financing, Counterfeit check.

9.6 Reporting of Suspicious Transactions

9.6.1 There is a statutory obligation for all staff to report suspicions of money laundering. Section 25 (1) of the Act contains the requirement to report to the BFIU, Bangladesh Bank. The actual reporting should be made as per the BFIU Circular No 12 of BFIU (Annexure – F) and an internal reporting will be made using the format as attached Annexure -D , as procedure as laid down in the AML Organizational Structure.

9.6.2 Such unusual or suspicious transactions will be drawn initially to the attention of immediate Supervisory Officer to ensure that there are no known facts that will negate the suspicion before further reporting on to the Anti-Money Laundering Compliance Officer.

9.6.3 Each FI must have a clear instruction for the Officers and Employees to ensure:

- i. That each relevant employee knows to which person they should report suspicions, and
- ii. That there is a clear reporting chain under which those suspicions will be passed without delay to the Chief Anti Money Laundering Compliance Officer (CAMLCO).

9.6.4 Once employees have reported their suspicions to the appropriate person in accordance with an established internal reporting procedure they have fully satisfied the statutory obligations.

9.6.5 IDCOL must refrain from carrying out transactions which they know or suspect to be related to money laundering until they have apprised the Bangladesh Bank. Where it is impossible in the circumstances to refrain from executing a suspicious transaction before reporting to the Bangladesh Bank or where reporting it is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the financial institutions concerned shall apprise the Bangladesh Bank immediately afterwards. While it is impossible to spell out in advance how to deal with every possible contingency, in most cases common sense will suggest what course of action is most appropriate. Where there is doubt, the advice of the Anti Money Laundering Compliance Officers may be sought.

9.6.6 It is the Chief Anti Money Laundering Compliance Officer (CAMLCO) who will have the responsibility for communicating reports of suspicious transactions to the Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank and will provide the liaison between the Bank and the Bangladesh Bank.

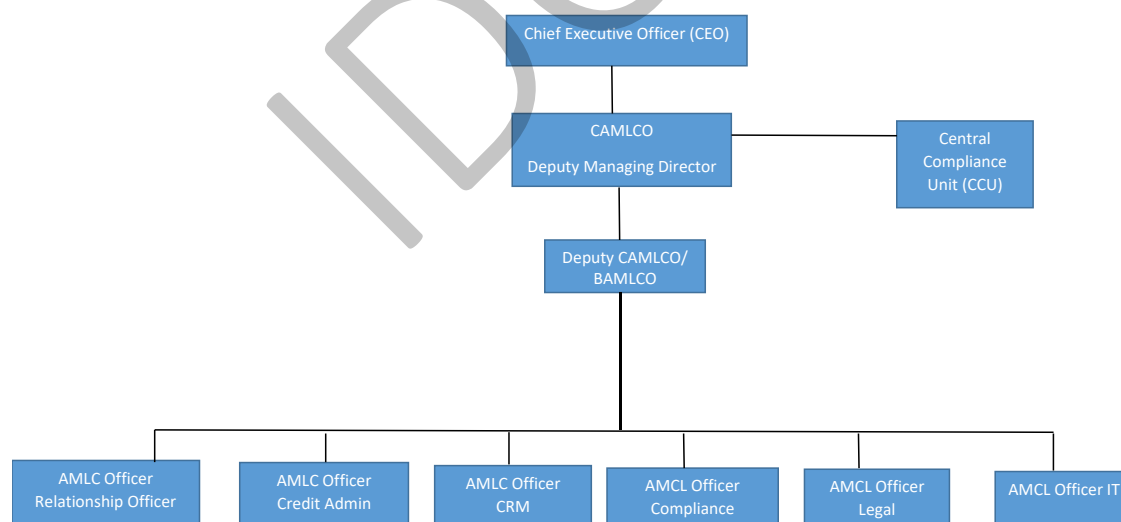
9.6.7 The CAMLCO has a significant degree of responsibility and should be familiar with all aspects of the legislation. He/she is required to determine whether the information or other matters contained in the transaction report he/she has received give rise to a knowledge or suspicion that a customer is engaged in money laundering.

9.6.8 He/She must take steps to validate the suspicion in order to judge whether or not a report should be submitted to Bangladesh Bank. In making this judgment, the CAMLCO should

consider all other relevant information available within the financial institution concerning the person or business to which the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the relationship, and referral to identification records held. If, after completing this review, the CAMLCO decides that there are no facts that would negate the suspicion, then he must disclose the information to Bangladesh Bank.

- 9.6.9 The determination of whether or not to report implies a process with at least some formality attached to it. It does not necessarily imply that the CAMLCO must give reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent for internal procedures to require that written reports are submitted and that he/she should record his/her determination in writing. Clearly in cases where there is a doubt it would be prudent for the CAMLCO to make a report to the Bangladesh Bank.
- 9.6.10 It is therefore imperative that the CAMLCO has reasonable access to information that will enable him/her to undertake his/her responsibility. It is important therefore that the CAMLCO should keep a written record of every matter reported to him, of whether or not the suggestion was negated or reported, and of his reasons for his decision.
- 9.6.11 The CAMLCO will be expected to act honestly and reasonably and to make his determinations in good faith. Provided that the CAMLCO or an authorized deputy does act in good faith in deciding not to pass on any suspicious report, there will be no liability for non-reporting if the judgment is later found to be wrong.
- 9.6.12 Care should be taken to guard against a report being submitted as a matter of routine to Bangladesh Bank without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

9.7 Reporting lines



Relationship Manager or Unit-in-Charge will act as AMLC
AMLC = Anti-Money Laundering Compliance

- 9.7.1 Supervisors should also be aware of their own legal obligations. An additional fact which the supervisor supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the supervisor. The supervisor then has a legal obligation to report to the AMLCO.

- 9.7.2 All suspicions reported to the AMLCO should be documented (in urgent cases this may follow an initial discussion by telephone). In some organizations it may be possible for the person with the suspicion to discuss it with the AMLCO and for the report to be prepared jointly. The report should include the full details of the customer as and full statement as possible of the information giving rise to the suspicion.
- 9.7.3 The AMLCO should acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. “tipping off”. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed.
- 9.7.4 On-going communication between the AMLCO and the reporting person/department is important. IDCOL may wish to consider advising the reporting person, department or the branch of the AMLCO’s decision, particularly if the report is believed to be invalid. Likewise, at the end of an investigation, consideration should be given to advising all the members or the staff concerned of the outcome. It is particularly important that the AMLCO is informed of all communication between the investigating officer and the Branch concerned at all stages of the investigation.
- 9.7.5 Records of suspicions, which were raised internally with the CAMLCO but not disclosed to Bangladesh Bank, should be retained for five years from the date of the transaction. Records of suspicions which the Bangladesh Bank has advised are of no interest should be retained for a similar period. Records of suspicions that assist with investigations should be retained until the Bank is informed by the Bangladesh Bank that they are no longer needed.

9.8 Reporting destinations

- 9.8.1 The national reception point for reporting of suspicions by the CAMLCO is:
The General Manager
Bangladesh Financial Intelligence Unit (BFIU)
Bangladesh Bank
Head Office, Dhaka- 1000.

Chapter Ten: Assessment Procedure

10.1 Self-Assessment Process

10.1.1 IDCOL have to conduct self-assessment program aiming to identify the implementation of AML & CFT policy, rules and laws and instruction issued by BFIU, Bangladesh Bank. The CAMLCO will time to time advise management whether the internal procedures and statutory obligations of the Bank have been properly discharged. The report should provide conclusions to three key questions:

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

10.1.2 Such report should be prepared in line with the BFIU Circular No 12 and as per the checklist provided with by BFIU. The Annexure-G attached herewith for information and necessary action for head office/branches. As per instruction, all branch of IDCOL will take necessary initiatives to overcome the shortcomings immediately, where necessary, Branches will sought for the help of CCU.

10.2 Independent Procedures Testing

10.2.1 Testing of Compliance AML Act and Guideline shall be conducted at least twice a year by Audit Department, and by external auditors. The tests include;

- i. Interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with IDCOL's anti-money laundering procedures;
- ii. A sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- iii. A test of the validity and reasonableness of any exemptions granted by IDCOL; and
- iv. A test of the record keeping system according to the provisions of the Act.

10.2.2 Any deficiencies if be identified would be reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline should be fixed to overcome the deficiencies.

10.2.3 Such report should be prepared in line with the BFIU Circular No 12 and as per the checklist provided with by BFIU. The Annexure-H attached herewith for information and necessary action for all officials. As per instruction all branches (HO to be considered as Principal Branch) of IDCOL will take necessary initiatives to overcome the shortcomings immediately, where necessary, Branch will sought for the help of CCU.

Chapter Eleven: Training and awareness building

11.1 Employee Training and Awareness Program

11.1.1 FATF recommendation 18 suggests that a formal AML/CFT compliance program should include an ongoing employee training program. The importance of a successful training and awareness program cannot be overstated. Employees in different business functions need to understand how IDCOL's policy, procedures, and controls affect them in their day to day activities. As per AML circular, each financial institution shall arrange suitable training for their officials to ensure proper compliance of money laundering and terrorist financing prevention activities.

i. **The Need for Staff Awareness**

The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the seriousness of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities. It is, therefore, important that IDCOL introduce comprehensive measures to ensure that all staff and contractually appointed agents (if there is any) are fully aware of their responsibilities.

ii. **Education and Training Programs**

All relevant staff should be educated in the process of the "Know Your Customer" requirements for money laundering and terrorist financing prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity. Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and IDCOL itself. Some sorts of high-level general awareness raising training are, therefore, also suggested.

iii. **General Training**

A general training program should include the following:

1. General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
2. Legal framework, how AML/CFT related laws apply to IDCOL and its employees;
3. IDCOL's policies and systems with regard to customer identification and verification, due diligence, monitoring;
4. How to react when faced with a suspicious client or transaction;
5. How to respond to customers who want to circumvent reporting requirements;
6. Stressing the importance of not tipping off clients;
7. Suspicious transaction reporting requirements and processes;
8. Duties and accountabilities of employees;

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training should present real life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable, how the pattern of activity was first detected and its ultimate impact on IDCOL.

iv. **Job Specific Training**

The nature of responsibilities/activities performed by the staff of IDCOL is different from one another. So their training on AML/CFT issues should also be different for each category. Job specific AML/CFT trainings are as under:

1. New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so. The new or fresh employee may be trained up within a year.

2. Customer Service/Relationship Managers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to IDCOL's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with nonregular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

3. Processing (Back Office) Staff

The staffs, who receive completed Account Opening, FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the IDCOL's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML/CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

4. Credit Officers

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

5. Audit and compliance staff

These are the people charged with overseeing, monitoring and testing AML/CFT controls, and they should be trained about changes in regulation, money laundering and terrorist financing methods and enforcement, and their impact on the institution.

6. Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering and terrorist financing prevention procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and terrorist financiers; internal reporting procedures and the requirements for verification of identity and the retention of records.

7. Senior Management and Board of Directors

Money laundering and terrorist financing issues and dangers should be regularly and thoroughly communicated to the board. It is important that the Compliance Department has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering and terrorist financing poses to IDCOL. Major AML/CFT compliance related circulars/circular letters issued by Bangladesh Bank should be placed to the board to bring it to the notice of the Board members.

8. AML/CFT Compliance Officer

The CAMLCO/DCAMLCO/AML/CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Bank directives and internal policies and standards.

In addition, the CAMLCO/DCAMLCO AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

11.2 Training Procedures

11.2.1 The trainers can take the following steps to develop an effective training program:

- i. Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- ii. Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick “why are they here” assessment. New hires should receive training different from that given to veteran employees.
- iii. Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- iv. Determine who can best develop and present the training program.

- v. Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- vi. Establish a training calendar that identifies the topics and frequency of each course.
- vii. Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- viii. Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

11.3 Refresher Training

- 11.3.1 In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of IDCOL's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities.
- 11.3.2 Training should be conducted ongoing basis, incorporating trends and developments in IDCOL's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions/unusual activity.

IDCOL

ANNEXURE

IDCOL

Annexure

Annexure –A: Questions for source of wealth.....	3
Wealth Generated From Business Ownership.....	3
Wealth Derived From Being a Top Executive.....	3
Primary Source of Wealth was Through Inheritance.....	3
Wealth Generated From a Profession (Physician, dentist, lawyer, engineer, entertainer etc.).....	3
Wealth Generated From Investments	4
Annexure –B: Identification of Directors & Authorized Signatories.....	5
Annexure –C: Examples of Potentiality Suspicious Transactions	6
Secured and unsecured lending.....	6
Accounts.....	6
International banking/trade finance.....	6
Institution employees and agents.....	6
Cash transactions	6
Annexure –D: Internal Suspicious Activity Report Form.....	8
Annexure –E: FATF Standards and FATF 40 Recommendation	9
Annexure –F: STR Reporting Format.....	10
Annexure –G: Self-Assessment	13
Annexure –H: Independent Testing Procedures.....	17
Annexure – I: Money Laundering Prevention Act and Anti-Terrorist Act.....	23
Anti-terrorism Act 2009	23
Money Laundering Prevention Act 2012_English.....	23
Anti-Terrorism (Amendment) Act 2013	23
Money Laundering Prevention (Amendment) Act, 2015.....	23
Annexure – J: Account Opening Form (Institutions).....	24
Annexure – K: Account Opening Form (Individuals).....	31
Annexure – L: Individual information Form	37
Annexure – M: KYC Form	42
Annexure – N: Signature Mismatch Form.....	45
Annexure – O: AML & BFIU Circulars	47
AML Circular No. 22: "Anti-Terrorism Act, 2009"	47
BFIU Circular No. 02: Regarding "Money Laundering Prevention Act, 2012" and Amendment of "Anti-Terrorism Act, 2012"	47
BFIU Circular No. 04: Regarding Guidance Notes on Prevention of Money Laundering and Terrorist Financing	47

BFIU Circular No. 07: Anti-Terrorism (Amendment) Act, 2013.....	47
BFIU Circular Letter No. 03: Circulation of Money Laundering Prevention Rules, 2013 and Anti-Terrorism Rules, 2013	47
BFIU Circular No. 12: Master Circular regarding Instructions to be followed by the Financial Institutions for the prevention of Money Laundering & Terrorist Financing	47
BFIU Circular Letter No. 04: Money Laundering and Terrorist Financing Risk Assessment Guidelines for Financial Institutions	47
BFIU Circular Letter No. 06: Circulation of Money Laundering Prevention (Amendment) Act, 2015	47
BFIU Circular Letter No. 01: Instructions to be followed for the compliance of Freezing Accounts of listed Individuals or Institutions and Other Issues under the Sanction List of Different Resolutions of United Nations Security Council	47
Booklets	48
Booklet of Financial Action Task Force (FATF)	48
Booklet of Money Laundering Prevention Act and Anti-Terrorist Act.....	48
Booklet of AML & BFIU Circulars.....	48

IDCOL

Annexure –A: Questions for source of wealth

Note: This form must be renewed every year

List of Questions to be used when obtaining source of wealth

Wealth Generated From Business Ownership

- Description and nature of the business and its operations
- Ownership type: private or public?
- What kind of company?
- Percentage of ownership?
- Estimated sales volume?
- Estimated net income?
- Estimated net worth?
- How long the business is going on?
- How was the business established?
- Other owners or partners (yes/no)?
- Names of other owners or partners?
- Percentage owned by other owners or partners?
- Number of employees?
- Number of locations?
- Geographic trade areas of business?
- Details other family members in business?
- Significant revenues from government contract or licenses?

Wealth Derived From Being a Top Executive

- Estimate of compensation?
- What does the company do? (For example, manufacturer, service...)
- Position held (for example, President, CFO/CEO)
- Length of time with company?
- Area of expertise (for example, finance, production, etc...)
- Publicly or privately owned?
- Client's past experience (for example, CFO at another company...)

Primary Source of Wealth was Through Inheritance

- In what business was the wealth generated?
- Inherited from whom?
- Type of asset inherited (for example: land, securities, company trusts...)
- When were the assets inherited?
- How much wealth was inherited?
- Percentage of ownership for a business that is inherited

Wealth Generated From a Profession (Physician, dentist, lawyer, engineer, entertainer etc.)

- What is the profession, including area of specialty (ex: arts, singer, construction, engineer)
- Source of wealth (Ex: lawyer who derived wealth from real estate, Dr. running a clinic...)
- Estimation of income

Wealth Generated From Investments

- Where did the source of wealth come from? (example, invested in shares, bonds, etc.)
- What do they currently invest in? (For example, real estate, stock market...)
- What is the size of the investment?
- Cite notable public transactions if any
- What is the client's role in transaction (ex: takes positions, buy companies, middle man)
- Estimated annual income/capital appreciation?
- How long has the client been an investor?

IDCOL

Annexure –B: Identification of Directors & Authorized Signatories

Identification of Directors & Authorized Signatories (Company letterhead)

Date:

To,
Infrastructure Development Company Limited (IDCOL)
UTC Building(16th floor), 8 Panthapath,
Kawran Bazar, Dhaka 1215.

Sub: Identification of Directors & Authorized signatories.

This is to introduce the following directors of the company & authorized signatories of the account(s) of the company maintained with your institution.

Name Designation	Father's Name Mother's Name	Date of birth Nationality ETIN	Present Address	Permanent Address

We certify that information provided above is true and correct. Please treat this letter together with duly attested photographs of the above individuals attached herewith on separate sheet, as Photo Identification document.

Sincerely.

.....
Chairman/ Company Secretary (Name & Seal)

(Company Stamp)

Annexure –C: Examples of Potentiality Suspicious Transactions

Secured and unsecured lending

- Customers who repay problem loans unexpectedly.
- Request to borrow against assets held by the financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
- Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.
- Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earnings capacity or asset base.

Accounts

- Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.
- Customer's reluctance or refusal to disclose other banking relationship.
- Purpose of maintaining account at FI cannot be adequately explained.
- Reluctance or refusal to provide business financial statements.
- Information provided by the customer does not make sense for the customer's business.
- A visit to the place of business does not result in a comfortable feeling that the business is in the business they claim to be in.
- Paying in large third party cheques endorsed in favor of the customer.
- Companies' representatives avoiding contact with FI.
- Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other product services that would be regarded as valuable.

International banking/trade finance

- Customer introduced by an overseas bank, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.
- Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from: countries which are commonly associated with the production, processing or marketing of drugs; proscribed terrorist organizations; [tax haven countries].
- Customers who show apparent disregard for arrangements offering more favorable terms.

Institution employees and agents

- Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.
- Changes in employee or agent performance, e.g. the salesman selling products for cash have a remarkable or unexpected increase in performance.
- Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

Cash transactions

- Unusual large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

- Customers who constantly pay in cash to cover requests for payment order, money transfers or other negotiable and readily marketable money instruments.

IDCOL

Annexure –D: Internal Suspicious Activity Report Form

Strictly Private & confidential

To	Anti Money Laundering Compliance Officer	Date:
From	Name:	Department:
	Job Title:	SAR Ref No.

Note: This form may be completed in English. For any queries, please contact AMLCO. Please provide full details of the transaction(s) and any other relevant data. Attach copies of relevant documents/transaction notes.

Customer/ Business Name:	Transaction Date(s):
Account Number(s):	Copies of Transactions and Account Details Attached Yes <input type="checkbox"/> No <input type="checkbox"/>
Description of Transaction(s). <i>(Nature of transaction, Origin & destination of Transaction etc.)</i>	
Source of Funds and Purpose of Transaction <i>(If you can, try to tactfully ask the customer)</i>	
Reasons why do you think the transaction is suspicious (Give as much details as possible)	
_____ Signature of IDCOL Staff	
TO BE COMPLETED BY AMLCO.	
ACTION TAKEN TO VALIDATE	
<input type="checkbox"/> Acknowledgement sent to the originator on _____ <input type="checkbox"/> Reviewed account documentation <input type="checkbox"/> Discuss with the relationship manager <input type="checkbox"/> Other.	
AGREED SUSPICIOUS. Yes/No	
COMMENTS / NOTES OF AMLCO	
_____ Signature of AMLCO	Date:

Annexure –E: FATF Standards and FATF 40 Recommendation

Please see the attached booklet of FINANCIAL ACTION TASK FORCE (FATF)

IDCOL

Annexure –F: STR Reporting Format

SUSPICIOUS TRANSACTION REPORT (STR) FORM

A. Reporting Institution :

- 1. Name of the FI:
- 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 and ref. no

C. Suspect Account Details :

- 1. Account Number:
- 2. Name of the account:
- 3. Nature of the account:
- 4. Nature of ownership:
(Individual/proprietorship/partnership/company/other, pls. specify)
- 5. Date of opening/Transaction:
- 6. Address:

D. Account holder details :

- 1.
 - 1. Name of the account holder:
 - 2. Address:
 - 3. Profession:
 - 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. Place of birth:
 - 11. Passport No.
 - 12. National Identification No.
 - 13. Birth Registration No.
 - 14. TIN:
- 2.
 - 1. Name of the account holder:
 - 2. Relation with the account holder mention in sl. no. D1
 - 3. Address:
 - 4. Profession:
 - 5. Nationality:

6. Other account(s) number(if any):	<input type="text"/>
7. Other business:	<input type="text"/>
8. Father's name:	<input type="text"/>
9. Mother's Name:	<input type="text"/>
10. Date of birth:	<input type="text"/>
11. Place of birth:	<input type="text"/>
12. Passport No.	<input type="text"/>
13. National Identification No.	<input type="text"/>
14. Birth Registration No.	<input type="text"/>
15. TIN:	<input type="text"/>

E. Reasons for considering the transaction(s) as 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 summary of suspicion and consequence of events)
(To be filled by the BAMLICIO)

F. Suspicious Activity Information

Summary characterization of suspicious activity:

- | | | |
|---|--|--|
| a. <input type="checkbox"/> Corruption and bribery | k. <input type="checkbox"/> murder, grievous physical injury | u. <input type="checkbox"/> terrorism or financing in terrorist activities |
| b. <input type="checkbox"/> counterfeiting currency | l. <input type="checkbox"/> trafficking of women and children | v. <input type="checkbox"/> adulteration or the manufacture of goods through infringement of title |
| c. <input type="checkbox"/> Counter feiting deeds and documents | m. <input type="checkbox"/> black marketing | w. <input type="checkbox"/> offences relating to the environment |
| d. <input type="checkbox"/> extortion | n. <input type="checkbox"/> smuggling of domestic and foreign currency | x. <input type="checkbox"/> sexual exploitation |
| e. <input type="checkbox"/> fraud | o. <input type="checkbox"/> Theft or robbery or dacoity or piracy or hijacking of aircraft | y. <input type="checkbox"/> insider trading and market manipulation |
| f. <input type="checkbox"/> forgery | p. <input type="checkbox"/> human trafficking | z. <input type="checkbox"/> organized crime, and participation in organized criminal groups |
| | | <input type="checkbox"/> |

- g. illegal trade of firearms
- h. illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication
- i. illegal trade in stolen and other goods
- j. kidnapping, illegal restrain and hostage taking
- q. dowry
- r. smuggling and offences related to customs and excise duties
- s. tax related offences
- t. infringement of intellectual property rights
- aa. racketeering
- bb. Other(Please specify) _____

G. Transaction/Attempted Transaction Details:			
Sl. no.	Date	Amount	Type*

H. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the FI? Yes No

I. Has the FI taken any action in this context? If yes, give details.

J. Documents to be enclosed
1. Account opening form along with submitted documents 2. KYC Profile 3. Account statement for last one year 4. Supporting Voucher/correspondence mention in sl. no. H 5. Others

Signature :
 (CAMLCO or authorized officer of CCU)
 Name :
 Designation :
 Phone :
 Date :

Annexure –G: Self-Assessment

আর্থিক প্রতিষ্ঠানের নাম

---- শাখা।

শাখা কর্তৃক Self Assessment পদ্ধতির মাধ্যমে নিজস্ব অবস্থান নির্ণয়

প্রতিটি আর্থিক প্রতিষ্ঠানের শাখা মানিগভারিং ও সন্ত্রাসী কার্যে অর্থাৎ প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানি গভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থাৎ প্রতিরোধ নীতিমালার আলোকে নিম্নবর্ণিত প্রশ্নমালায় বিস্তারিত উত্তর প্রদানের মাধ্যমে Self Assessment পদ্ধতিতে নিজেদের অবস্থান নির্ণয় করবে :

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
১. শাখায় মোট কর্মকর্তার সংখ্যা কত (পদানুযায়ী)? কতজন কর্মকর্তা মানিগভারিং প্রতিরোধ ও সন্ত্রাসে অর্থাৎ প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? (শতকরা হার)	প্রশিক্ষণ সংক্রান্ত রেকর্ড যাচাই করতে হবে।		
২.ক) শাখার মানিগভারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) জেষ্ঠ্য ও অভিজ্ঞ কি না? বিগত দুই বছরে তিনি মানিগভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থাৎ প্রতিরোধ বিষয়ক কোন প্রশিক্ষণ পেয়েছেন কি না? খ) শাখায় মানি গভারিং প্রতিরোধ কার্যক্রম যথানিয়মে পরিপালিত হচ্ছে এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় মনিটরিং ও পর্যালোচনা করে থাকেন কি না?	BAMLCO কর্তৃক – KYC কার্যক্রমের যথার্থতা মনিটরিং করা হয় কি না? যথাযথভাবে Transaction মনিটরিং এবং সন্দেহজনক সেনদেন রিপোর্ট (ইন্টারনাল রিপোর্টসহ) করা হয় কি না? যথাযথভাবে রেকর্ড সংরক্ষণ করা হয় কি না? STR সনাক্তকরণে ব্যবস্থা নেয়া হয় কি না?		
৩. BAMLCO সহ শাখার কর্মকর্তাগণ মানিগভারিং ও সন্ত্রাসী কার্যে অর্থাৎ প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানি গভারিং প্রতিরোধ ও সন্ত্রাসে অর্থাৎ প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	বিষয়টি যাচাইয়ের পদ্ধতি কী?		
৪. শাখা পর্যায়ে ত্রৈমাসিক ভিত্তিতে মানি গভারিং ও সন্ত্রাসে অর্থাৎ প্রতিরোধ বিষয়ক সভা অনুষ্ঠিত হয় কি না?	সভার আলোচ্যসূচি সকলের অবগতির জন্য বণ্টন করা হয় কি না? সভায় কী কী গুরুত্বপূর্ণ সিদ্ধান্ত গৃহীত হয়েছে? সভায় গৃহীত সিদ্ধান্ত কিভাবে বাস্তবায়িত হয়?		

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
৫. সকল প্রকার হিসাব খোলা ও সোনদেন পরিচালনার ক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং সময়ে সময়ে বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ?	গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয় কিনা? হিসাবের প্রকৃত সুবিধাজোগী (Beneficial Owner) সনাক্ত করা হয় কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরীখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কিনা?		
৬. ক) ঝুঁকির ভিত্তিতে শাখা তাদের গ্রাহকদের শ্রেণীবিন্যাস/শ্রেণীকরণ করে কিনা?	করে থাকলে এ পর্বত কতটি উচ্চ ঝুঁকি সম্পন্ন হিসাব শাখায় খোলা হয়েছে? এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে শাখা কী পদক্ষেপ গ্রহণ করেছে?		
৭. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিলান্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা?	এ বিষয়ক নিজস্ব নীতিমালা গ্রহণ করা হয়েছে কিনা? হলে উক্ত নীতিমালা শাখায় কিভাবে বাস্তবায়িত হচ্ছে?		
৮. শাখা গ্রাহকের KYC Profile এর তথ্য বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা মোতাবেক নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে কিনা?	কী পদ্ধতিতে এক্সপ মূল্যায়ন সম্পাদিত হয়ে থাকে?		

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
৯. সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখা কী ধরনের পদক্ষেপ গ্রহণ করেছে?	জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজলুশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও সেনদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কি না? এরূপ কোন ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা?		
১০. এ যাবৎ শাখা কর্তৃক কতগুলো সন্দেহজনক সেনদেন (STR) শনাক্ত করা হয়েছে?	শাখায় সন্দেহজনক সেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখায় সন্দেহজনক সেনদেন রিপোর্টিং এর জন্য Internal Reporting Mechanism চালু রয়েছে কিনা? শাখা পর্যায়ে নিস্পত্তিকৃত Internal Report সংরক্ষণ করা হয় কিনা?		
১১. মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন, সার্কুলার, প্রশিক্ষণ রেকর্ড, বিবরণী ও অন্যান্য এএমএস/সিএফটি সংক্রান্ত বিষয়াবলীর আলাদা নথি শাখা কর্তৃক সংরক্ষণ করা হয় কিনা? আইন, সার্কুলার ইত্যাদির কপি শাখার	সংরক্ষিত হয়ে থাকলে হ্যাঁ অথবা না হয়ে থাকলে না, আংশিক হলে কী কী সংরক্ষিত আছে তা লিখুন।		

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
সকল কর্মকর্তা/কর্মচারীদের সরবরাহ করা হয় কিনা?			
১২. বিএফআইইউ মান্টার সার্কুলার অনুসারে শাখায় PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা?	উত্তর হ্যাঁ হলে এই হিসাব খোলা ও পরিচালনার ক্ষেত্রে কী কী ধরনের সতর্কতা অবগত করা হচ্ছে?		
১৩. আর্থিক প্রতিষ্ঠানের প্রধান কার্যালয়, বাংলাদেশ ব্যাংক ও বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইউনিট-এর পরিদর্শন প্রতিবেদনে উল্লেখিত মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ পরিপালন বিষয়ক দুর্বলতা/অনিয়মসমূহ নিয়মিত করা হয়েছে কিনা?	না হয়ে থাকলে প্রতিবন্ধকতাসমূহ কী কী?		

শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তার নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ	শাখা ব্যবস্থাপকের নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ
--	---

Annexure –H: Independent Testing Procedures

অভ্যন্তরীণ নিরীক্ষা বিভাগ
আর্থিক প্রতিষ্ঠানের নাম
প্রধান কার্যালয়

Independent Testing Procedures: শাখা পরিদর্শনের চেকলিস্ট

আর্থিক প্রতিষ্ঠানের অভ্যন্তরীণ নিরীক্ষা বিভাগ মানিগভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানি গভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নলিখিত প্রশ্নমালার যথাযথ উত্তর (ডকুমেন্ট ভিত্তিক) অনুসারে কোর প্রদানপূর্বক শাখার মানি গভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রমকে মূল্যায়ন করবে। অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক শাখার উপর প্রণীত বার্ষিক নিরীক্ষা প্রতিবেদনে (প্রযোজ্য ক্ষেত্রে পৃথক পরিদর্শন কর্মসূচীর আওতায় শুধুমাত্র Independent Testing Procedures ভিত্তিক প্রতিবেদন প্রণীত হবে) মানি গভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়ন সংক্রান্ত আলাদা অধ্যায়ে সমুদয় বিষয়াদি সুপারিশসহ সন্নিবেশ করবে।

(যাচাইয়ের মানদণ্ড অনুসারে সম্পূর্ণরূপে পরিপালিত হলে সম্পূর্ণ কোর, আংশিক পরিপালনে আংশিক কোর এবং উত্তর নেতিবাচক হলে শূন্য কোর প্রদান করতে হবে।)

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	কোর	প্রাপ্ত কোর	মন্তব্য
১.	শাখা পরিপালন ইউনিট	১. শাখায় একজন অভিজ্ঞ ও জ্যেষ্ঠ পরিপালন কর্মকর্তা (BAMLCO) রয়েছেন কি?	অফিস অর্ডার দেখুন। শাখার দ্বিতীয় কর্মকর্তা বা অভিজ্ঞ কোন উপস্থিত কর্মকর্তাকে BAMLCO মনোনীত করা সমীচীন হবে।	১		
		২. বিগত দুই বছরে তিনি মানি গভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণে অংশগ্রহণ করেছেন কি? মানিগভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানি গভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে তিনি যথেষ্ট অবহিত কি?	সাক্ষাৎকার ও নথিপত্রের ভিত্তিতে যাচাই করুন।	২		
		৩. মানি গভারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং এর আওতায় জারীকৃত পদিসি এবং/অথবা নির্দেশনা যথানিয়মে পরিপালিত হচ্ছে- এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ার মনিটরিং ও পর্যালোচনা করে থাকেন কি?	BAMLCO কর্তৃক মনিটরিং ও পর্যালোচনার প্রক্রিয়া যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন।	৩		

ক্রমিক নং	অঞ্চল/এবিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	কোর	প্রাপ্ত কোর	মন্তব্য
		৪. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিগভারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা? BAMLCO কর্তৃক শাখায় পরিচালিত উচ্চ ঝুঁকিমুক্ত হিসাবসহ সকল হিসাবের লেনদেন মনিটরিং পর্যাপ্ত কি?	মানিগভারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে শাখার গৃহীত পদক্ষেপ মূল্যায়ন করুন। BAMLCO কর্তৃক উচ্চ ঝুঁকিমুক্ত হিসাবসহ সকল হিসাবের লেনদেন মনিটরিং পদ্ধতি যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন।	৪		
		৫. বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা?	এ ধরনের হিসাব বোনা ও পরিচালনার ক্ষেত্রে বিএফআইইউ মাস্টার সার্কুলার অনুসারে সতর্কতা অবলম্বন করা হচ্ছে কিনা তা যাচাই করুন। তবে PEPs প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব না থাকলেও যদি বিএফআইইউ মাস্টার সার্কুলার এ প্রদত্ত নির্দেশনা বাস্তবায়নের প্রক্রিয়া বিদ্যমান থাকে তাহলে শাখা পূর্ণ নম্বর প্রাপ্ত হবে।	৩		
		৬. বিএফআইইউ প্রদত্ত সেলফ অ্যাসেসমেন্ট শাখা কর্তৃক কতটুকু সঠিক ও কার্যকরভাবে সম্পাদন হচ্ছে?	শাখার সেলফ অ্যাসেসমেন্ট রিপোর্ট পর্যালোচনা করুন। সঠিক ও কার্যকরভাবে সেলফ অ্যাসেসমেন্ট রিপোর্ট গ্রহণ ও বাস্তবায়নের ভিত্তিতে নম্বর প্রদান করুন।	৬		
২.	মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ে কর্মকর্তাদের জ্ঞান ও সচেতনতা বৃদ্ধি এবং ঝুঁকি প্রতিরোধে গৃহীত ব্যবস্থা।	১. শাখায় কতজন কর্মকর্তা মানি গভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? ২. শাখার কর্মকর্তাগণ মানিগভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানি গভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	১০০% কর্মকর্তার প্রশিক্ষণ সম্পন্ন হলে তা সন্তোষজনক বলে বিবেচিত হবে। প্রশিক্ষণের হার অনুসারে নম্বর প্রাপ্ত হবে। শাখার সংশ্লিষ্ট কর্মকর্তাদের সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করুন।	৩ ৪		

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	কোর	প্রাপ্ত কোর	মন্তব্য
		৩. মানি লন্ডারিং ও সন্ত্রাসে অর্পায়ন প্রতিরোধ কার্যক্রম মূল্যায়নের জন্য একটি ত্রৈমাসিক ভিত্তিতে শাখা ব্যবস্থাপকের নেতৃত্বে কর্মকর্তাগণের সভা আয়োজন করা হয় কিনা?	সভার আলোচ্যসূচী সংগ্রহ ও এর কার্যকারিতা পরীক্ষা করুন।	৫		
		৪. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং ব্যাংকের নিজস্ব নীতিমালা অনুযায়ী মানিলান্ডারিং ও সন্ত্রাসে অর্পায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা?		৩		
৩.	গ্রাহক পরিচিতি (KYC) পদ্ধতি	১. সকল প্রকার হিসাব খোলা ও সেন্সেদন পরিচালনার ক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং বিএফআইইউ কর্তৃক জারীকৃত মানস্টার সার্কুলারের নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ?	প্রত্যেক ধরনের ৪/৫ টি হিসাবের নমুনা পরীক্ষা করুন। নিম্নোক্ত বিষয়ে সন্তুষ্টিসাপেক্ষে নম্বর প্রদান করুন- গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয়েছে কিনা? হিসাবের প্রকৃত সুবিধাজোগী (Beneficial Owner) সনাক্ত করা হয়েছে কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির দিগ্বিধে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কি না?	৬		
		২. বিএফআইইউ কর্তৃক জারীকৃত মানস্টার সার্কুলারের নির্দেশনা অনুসারে শাখা যথাযথভাবে ঝুঁকির ভিত্তিতে তাদের গ্রাহকদের শ্রেণীবিন্যাস/ শ্রেণীকরণ করে কি?	বিএফআইইউ কর্তৃক জারীকৃত মানস্টার সার্কুলারের নির্দেশনা পরিপাতিত হয়ে কিনা যাচাই করুন।	৬		
		৩. উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে প্রয়োজনীয় অতিরিক্ত তথ্য সংগ্রহ করা হয় কি?	কি ধরনের তথ্য সংগ্রহ করা হয় এবং তা যথেষ্ট কিনা পরীক্ষা করুন।	৫		
		৪. শাখা কি গ্রাহকের KYC Profile নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে থাকে?	KYC Profile পুনঃমূল্যায়ন ও হালনাগাদ পদ্ধতি মূল্যায়ন করুন।	৫		

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	কোর	প্রাপ্ত কোর	মন্তব্য
৪.	সন্ত্রাস বিরোধী আইন, ২০০৯ এর পরিপালন	সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসে অর্থায়ন প্রতিরোধের দক্ষ্যে শাখা কী ধরনের কার্যকর পদক্ষেপ গ্রহণ করেছে?	নিম্নোক্ত বিষয়ে সন্ত্রাসিলাপেক্ষে নম্বর প্রদান করুন- জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজলুশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তাগিকাত্মক কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তাগিকাত্মক কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তাগিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও সেনাদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কিনা? এরূপ ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা ?	৫		
৫.	সন্দেহজনক সেনাদেন রিপোর্ট (STR) ও নগদ সেনাদেন রিপোর্ট(CTR)	১. শাখার কর্মকর্তাগণ সন্দেহজনক সেনাদেন রিপোর্ট (STR) সম্পর্কে অবহিত আছেন কি? ২. শাখার মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত সন্দেহজনক সেনাদেন চিহ্নিতকরণের কার্যকর পদ্ধতি চাপু আছে কি? এ যাবৎ কতগুলো সন্দেহজনক সেনাদেন (STR) BAMLCO কর্তৃক CCU এর নিকট রিপোর্ট করা হয়েছে?	শাখায় সন্দেহজনক সেনাদেন Reporting এর জন্য Internal Reporting Mechanism চাপু আছে কিনা? তা সর্বত্র কর্মকর্তা জানেন কিনা? শাখায় সন্দেহজনক সেনাদেন সংঘটিত হওয়া সত্ত্বেও যদি BAMLCO কর্তৃক CCU এর নিকট কোন STR না করা হয়ে থাকে তাহলে তা অসন্তোষজনক বিবেচিত হবে। নগ্নি ও সিস্টেম পরীক্ষা করে শাখায় STR সনাক্তকরণের জন্য কোন পদ্ধতির প্রবর্তন করা হয়েছে কিনা তা যাচাই করুন। নিম্নোক্ত বিষয়ে সন্ত্রাসি লাপেক্ষে নম্বর প্রদান করুন- শাখায় সন্দেহজনক সেনাদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখা পর্যায়ে নিম্পত্তিকৃত Internal Report যথাযথভাবে সংরক্ষণ করা হয় কিনা?	৫	৪	

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	স্কোর	প্রাপ্ত স্কোর	মন্তব্য
		৩. শাখা কর্তৃক যথাযথ ও সঠিকরূপে নগদ সেনলদেন রিপোর্ট (CTR) করা হয় কিনা?	এতদসংক্রান্ত নথি পরীক্ষা করুন। (কমপক্ষে এক মাসের নগদ সেনলদেন) ক্যাশ রেজিস্টার/বিবরণী হতে পরীক্ষা করুন এবং এর ভিত্তিতে ঐ মাসে দাখিলকৃত CTR রিপোর্ট পরীক্ষাপূর্বক CTR রিপোর্ট এর সঠিকতার বিষয়ে মূল্যায়ন করুন।	২		
৬.	CCU বরাবর বিবরণী দাখিল	১. শাখা কর্তৃক কতটি বিবরণী (CCU বরাবর দাখিল করা হয়? শাখা কি যথাসময়ে বিবরণী দাখিল করে?	এতদসংক্রান্ত নথি পরীক্ষা করুন। বিলম্বে অথবা বিবরণী দাখিল না করলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
		২. শাখা কর্তৃক নিয়মিতভাবে সেক্স অ্যালোসমেন্ট করা হয় কিনা? প্রস্তুতকৃত বিবরণী যথাযথ কিনা?	এতদসংক্রান্ত বিবরণী পরীক্ষা করুন। তথ্যাদি সঠিক ও পরিপূর্ণ না হলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
৭.	রেকর্ড সংরক্ষণ	১. গ্রাহক পরিচিতি (KYC) এবং সেনলদেন সম্পর্কিত রেকর্ড যথাযথভাবে সংরক্ষণের বিধান আছে কি?	৫টি বন্ধ হিসাব পরীক্ষা করুন। এক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন এর বিধান যথাযথভাবে অনুসরণ করা হয়েছে কিনা যাচাই করুন।	৪		
		২. নিয়ন্ত্রণকারী কর্তৃপক্ষ বা CCU এর চাহিদা মোতাবেক রেকর্ডসমূহ সরবরাহ করা হয় কি?	এতদসংক্রান্ত নথি পরীক্ষা করুন। যথাসময়ে ও যথাযথ তথ্য সরবরাহ না করলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
৮.	AML/CFT সম্পর্কিত শাখার সার্বিক কার্যক্রম	১. শাখা ব্যবস্থাপক (BAMLCO না হলে) মানি লন্ডারিং ও সন্ত্রাসে অর্পায়ন প্রতিরোধ বিষয়ক কর্মসূচী বাস্তবায়নে যথাযথ ভূমিকা পালন করে কি?	শাখায় আয়োজিত সভার আলোচনাসূচি ও শাখা ব্যবস্থাপকের সাথে সাক্ষাৎকার এবং এ বিষয়ে শাখার পরিপালন অবস্থার ভিত্তিতে মূল্যায়ন করুন।	৫		
		২. পূর্ববর্তী অভ্যন্তরীণ ও বহিঃ নিরীক্ষা প্রতিবেদন পরীক্ষাকালে AML/CFT বিষয়ক কোন অনিয়ম ও দুর্বলতার উল্লেখ আছে কিনা এবং শাখা কোন সংশোধনমূলক ব্যবস্থা গ্রহণ করেছে কিনা?	সর্বশেষ নিরীক্ষা সংক্রান্ত রিপোর্ট পরীক্ষা করুন এবং কি ধরনের সংশোধনমূলক ব্যবস্থা নেওয়া হয়েছে যাচাই করুন।	৪		
		৩. শাখার সার্বিক কার্যক্রম সন্তোষজনক কি?	শাখার মানি লন্ডারিং ও সন্ত্রাসে অর্পায়ন প্রতিরোধ সংক্রান্ত সার্বিক কার্যক্রম এবং শাখা ব্যবস্থাপকের পারফরম্যান্সের ভিত্তিতে মূল্যায়ন করুন।	৬		
			মোট	১০০		

শাখার সার্বিক মূল্যায়ন :

কোর	রেটিং
৯০ ⁺ -১০০	শক্তিশালী (Strong)
৭০ ⁺ -৯০	সন্তোষজনক (Satisfactory)
৫৫ ⁺ -৭০	মোটামুটি ভাল (Fair)
৪০ ⁺ -৫৫	প্রান্তিক (Marginal)
৪০ ও এর নীচে	অসন্তোষজনক (Unsatisfactory)

IDCOL

Annexure – I: Money Laundering Prevention Act and Anti-Terrorist Act

Anti-terrorism Act 2009

Money Laundering Prevention Act 2012_English

Anti-Terrorism (Amendment) Act 2013

Money Laundering Prevention (Amendment) Act, 2015

Please see the attached booklet of Money Laundering Prevention Act and Anti-Terrorist Act

IDCOL

Annexure – J: Account Opening Form (Institutions)



Account Opening Form Corporate Account

Date:

For Office Use Only:

Account Number:

Unique Customer ID Number

The Executive Director and CEO
Infrastructure Development Company Limited

Dear Sir,

I/We hereby request you to kindly open an Account in the books of your institution as follows. I/We furnish our detailed information hereunder

01. **Account Title:** (In English)
(Please use block letters)
(In Bangla)

02. **Nature of Business:** (Please put a ✓ mark where applicable)

- | | | | |
|--|--|--|--|
| <input type="checkbox"/> Private Limited | <input type="checkbox"/> Public Limited | <input type="checkbox"/> Partnership | <input type="checkbox"/> Sole Proprietorship |
| <input type="checkbox"/> NGO/NPO | <input type="checkbox"/> Government Organization | <input type="checkbox"/> School/College/Club/Society | <input type="checkbox"/> Joint Venture |
| <input type="checkbox"/> Multinational | <input type="checkbox"/> Trustee Organization | | |
| <input type="checkbox"/> Others (Please Specify) | | | |

03. **Type of Industry:** (Please put a ✓ mark where applicable)

- | | | | |
|--|----------------------------------|--------------------------------|--------------------------------------|
| <input type="checkbox"/> Manufacturing | <input type="checkbox"/> Service | <input type="checkbox"/> Trade | <input type="checkbox"/> Agriculture |
| <input type="checkbox"/> Others (Please Specify) | | | |

04. **Size of Workforce:**

Management and executives Workers and others

05. **Size of Asset Base:**

Replacement cost of total assets (Excluding land and factory building) BDT millions

Value of land BDT millions Value of factory building BDT millions

06. **Type of Account:** (Please put a ✓ mark where applicable)

- | | | |
|--|-------------------------------|--------------------------------|
| <input type="checkbox"/> Deposit | <input type="checkbox"/> Loan | <input type="checkbox"/> Grant |
| <input type="checkbox"/> Others (Please Specify) | | |

07. **Declaration Related to Account Operation:** (Please put a ✓ mark where applicable)

- | | | | |
|--|---|--|--|
| <input type="checkbox"/> Sole operation | <input type="checkbox"/> Combined Operation | <input type="checkbox"/> Any one person will operate | <input type="checkbox"/> Others (Please Specify) |
| <input type="checkbox"/> Special Instructions (If any) | | | |



08. Company Address

Registered Address:

Upazila/Thana District Postal Code

Country

Business/Office Address:

Upazila/Thana District Postal Code

Country

Factory Address:

Upazila/Thana District Postal Code

Country

09. Contact Details: Phone: Fax: E-mail:

Website:

10. Trade License Number: **Date:**

Issuing Authority:

11. Registration/Incorporation Number:

Registration Authority: **Country:**

12. Tax Identification Number (e-TIN only):

13. VAT Registration Number:

14. Nature of Business (Please provide detailed description):

.....

.....

15. The Project and its Development History (Please provide detailed description):.....

.....

.....

.....

.....

.....

.....



16. Deposit Related Information :

Amount: *In words:*

Period: Year Months Days

Date of maturity:

Currency:

Interest rate: (% per annum)

Cheque/ pay order number: Date:

Name of bank and branch:

Renewal/encashment Instructions (*Please put a ✓ mark where applicable*):

Renew both principal and interest Renew principal only Not applicable

17. Special Scheme Related Information:

Name of scheme: Period of scheme:

Initial deposit amount: Amount of installment: Number of installments: *Per year*

Installment start date: Maturity date:

Payable at maturity: Payable per month/installment:

18. Debt Product Related Information:

Type of facility (*Please put a ✓ mark where applicable*): Term Loan Short Term Loan Others (*Please specify*)

Loan Amount: Tenor: Grace Period:

Other Details:

19. Source of Funds (*Please put a ✓ mark where applicable*):

Salary Own Business Commission Inheritance/Gift/Return on Investment

Please provide detailed description of the source of funds

.....

.....

.....

.....



20. Declaration and Signature:

I/We declare that all information provided in this application and in documents submitted is true, accurate and complete. I/We understand that withholding of information or giving false information will result in refusal of my application.

I/We authorise IDCOL to verify any information provided by me/us.

I/We authorize permission to any person, employee, agent, representative, adviser, subsidiary, affiliate, firm or corporation of IDCOL to release, collect, receive, store, transfer and use any information provided by me/us, or any information obtained in connection with this application, and to disclose such information to its authorised representatives or regulatory bodies or the government or otherwise for the purpose of this application, where IDCOL reasonably considers it is necessary to make such disclosure. I/We waive any and all claims with respect to providing this information. I/We hereby release IDCOL from all liability for any damage or issuing of this information.

I/We declare that I/we have fully read and understood the terms and conditions of the IDCOL Environmental and Social Safeguards/Management Framework.

I/We understand that all fees paid to IDCOL are non-refundable under any circumstances, except as required by law.

I/We declare that I/we have fully read and understood the terms and conditions set out in this disclaimer.

(Please attach an attested true copy photograph)

(Please attach an attested true copy photograph)

(Please attach an attested true copy photograph)

(Signature with date)

(Signature with date)

(Signature with date)

Name and designation:

Name and designation:

Name and designation:

.....
.....

.....
.....

.....
.....



For Office Use Only

Product Code:	Sector Code:
----------------------	---------------------

Type of Company (Please put a ✓ mark where applicable):

Is the company a SME? Yes No

If the company is a SME, please put ✓ mark where applicable in the following boxes showing enterprise type

Small Medium Micro Cottage

Woman Entrepreneur (Please put a ✓ mark where applicable):

Is there a woman entrepreneur? Yes No

Comments:

Account opening officer: Signature (with Seal) : Name and designation: Date :	Checked and Authorized by: Signature (with Seal) : Name and designation: Date :
---	---



Account Opening Documentation Checklist

- General Requirements**
- Completed account opening form
 - Proof of address verification: Utility bill (Gas/Electricity/Water)/BTCL Telephone Bill/House Rent /Lease agreement/Proof of personal visit by the RM
 - CIB undertaking form
 - Completed KYC Profile form
- Additional Documentary Requirements**
- Sole Proprietorship**
- Photograph of applicant (2 copies, attested)
 - Photograph of all authorized signatories (2 copies)
 - Trade license (valid up-to-date copy) and TIN certificate (if any)
 - Permission under 18-A from Bangladesh Bank (For GSA and Agents only)
 - Photo identification (National ID/Voter ID card/Current valid passport/ Valid driving license. Where photograph is also attested/Employee photo ID card of any multinational or listed (with stock exchange) company or organization)
- Partnership concern**
- Trade license (valid up-to-date copy)
 - TIN certificate
 - Certified true copy of partnership deed of the partnership concern (if registered)
 - Notarized copy of partnership deed of the partnership concern (if unregistered)
 - Certificate of registration of the partnership concern
 - Partners' letter of authority for opening the account and authorization for its operation, duly certified by the managing partner
 - List of partners with their addresses
 - Permission under 18A from Bangladesh Bank (for GSA and Agents only)
 - Where a third party is authorized to operate a partnership account, a mandate form must be signed by all the partners and the signature of the third party should be attested thereon
 - Copy of the latest report and account (audited where applicable)
 - An explanation of the nature of the business or partnership should also be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose
 - 2 copies of photograph and identification document of all partners and all authorized signatories
- Limited company (incorporated in Bangladesh)**
- Trade license (valid up-to-date copy), TIN certificate
 - Certified true copy of the Memorandum or Articles of Association or By-Laws of the company
 - Certified true copy of certificate of incorporation
 - Certified true copy the certificate of commencement of business (In case of public limited company)
 - Extract of resolution of the board/general meeting of the company for opening the account and authorization for its operation duly certified by the Chairman/Managing director of the company, clearly mentioning the operating instruction
 - List/register of directors
 - Permission under 18A from Bangladesh Bank (for GSA and Agents only)
 - An 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 statement when available
 - 2 copies photographs and identification document of:
 - 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 power of attorney to operate the account/transaction
 - The beneficial owner(s) of the company
 - The major shareholders holding 20% or more shares in the company
 - RJSC certified up-to-date Schedule X
 - RJSC certified up-to-date Form VI
 - RJSC certified up-to-date Form XII
 - Certificate of name change (if applicable)



- VAT registration certificate
 - Latest credit rating report
- Association/club/charity/trust/school/college /society
- Certified true copy of the constitution/by-laws/trust deed/memorandum and articles of association
 - Trust deed and rules (for trusts)
 - Certificate of registration/recognition
 - List of members of the governing body/executive committee with their addresses
 - Extract of resolution of the governing body/executive committee/ for opening the account and authorization for its operation duly certified by the Chairman/secretary of the association/club/charity/trust/school/college
 - 2 copies of photographs and identification of all authorized signatories
- NGO/unincorporated associations
- Certified true copy of the constitution/by-laws/rules of charter
 - Certificate of registration from NGO bureau
 - List of members of the governing body/executive committee with their addresses
 - Extract of resolution of the governing body/executive committee for opening the account and authorization for its operation or power of attorney
 - Form QA-22 signed in duplicate by all signatories (foreign entity)
 - 2 copies of photographs and identification document of all authorized signatories
- Limited company/LLCs/others (incorporated outside Bangladesh)
- Memorandum and Articles of Association of the company (*)
 - certificate of incorporation (*)
 - certificate of commencement of business (in case of public limited company) (*)
 - Extract of resolution of the board/general meeting of the company for opening the account and authorization for its operation duly certified by the Chairman/Managing director of the company, clearly mentioning the operating instruction
 - List of all authorized signatories and directors (*)
 - Permission under 18B from Bangladesh Bank (**)
 - Permission from Ministry of Industry (**)
 - Certificate of filing with Register of Joint Stock Companies (**)
 - Form QA-22 signed in duplicate by all signatories
 - BOI registration certificate
 - Latest credit rating report
 - 2 copies photographs and identification document of:
 - 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 power of attorney to operate the account/transaction
 - The beneficial owner(s) of the company
 - The major shareholders holding 20% or more shares in the company
- (*) These items should be certified by the authorities where the company is registered and counter certified by Bangladesh Mission overseeing the country of the Ministry Foreign Affairs in Dhaka
 (**) These are not required if the application is for a non-resident account by a limited liability company incorporated overseas

Note: In addition to the documents mentioned above, IDCOL reserves the right to require additional documents during its due diligence process

Annexure – K: Account Opening Form (Individuals)



Account Opening Form Personal Account

Date:

For Office Use Only:

Account Number:

Unique Customer ID Number

The Executive Director and CEO
Infrastructure Development Company Limited

Dear Sir,

I/We hereby request you to kindly open an Account in the books of your institution as follows. I/We furnish our detailed information hereunder

01. Name of Applicant(s): *(In English, please use block letters)*
- (In Bangla)*

First Applicant	
Second Applicant	
Third Applicant	
Fourth Applicant	

02. Type of Account: *(Please put a ✓ mark where applicable)*

- Deposit Loan Others *(Please Specify)*

03. Declaration Related to Account Operation: *(Please put a ✓ mark where applicable)*

- Sole operation Combined Operation Any one person will operate Others *(Please Specify)*
- Special Instructions (if any)

04. Deposit Related Information :

Amount: *In words:*

Period: Year Months Days

Date of maturity:

Currency:

Interest rate: *(% per annum)*

Cheque/ pay order number: Date:

Name of bank and branch:

Renewal/encashment Instructions *(Please put a ✓ mark where applicable):*

- Renew both principal and interest Renew principal only Not applicable

05. Special Scheme Related Information:

Name of scheme: Period of scheme:



Initial deposit amount: Amount of installment: Number of installments: Per year
 Installment start date: Maturity date:
 Payable at maturity: Payable per month/installment:

06. Source of Funds (Please put a ✓ mark where applicable):

- Salary Own Business Commission Inheritance/Gift/Return on Investment
- Please provide detailed description of the source of funds
-
-
-
-

07. Please Fill-in if One or More Applicant is Minor(s):

I, being the lawful Guardian of the following applicant, hereby declare that the applicant is a minor. His/her necessary information has been furnished above. The account will be operated under my signature being lawful Guardian until the minor becomes adult or any other declaration is given by me.

(Please attach an attested true copy photograph)	(Please attach an attested true copy photograph)	(Please attach an attested true copy photograph)
--	--	--

Name of the minor: 1 2 3

Name of the guardian: 1 2 3

Relationship with the minor: 1 2 3

08. Nomination:

I/We hereby nominate the following person as my/our nominee to whom the balance of my/our account would be paid in the event of my/our death. I/We reserve the right to charge/cancel this nomination any time. The nominee will be responsible for distributing the balance of my /our account among my/our heirs as per preset law. I/We also agree that Infrastructure Development Company Limited will no way be responsible for such payment as per my/our instruction or distribution as per law.

Name of the Nominee(s) and % Share of Inheritance:

Nominee 1 Nominee 2

Father's Name:

Nominee 1 Nominee 2

Mother's Name:

Nominee 1 Nominee 2

Spouse's Name:

Nominee 1 Nominee 2

Date of Birth:



Nominee 1 Nominee 2

Occupation:

Nominee 1 Nominee 2

National ID Card No. (if any):

Nominee 1 Nominee 2

Relationship with Applicant:

Nominee 1 Nominee 2

(Please attach an attested true copy photograph of nominee 1)

(Please attach an attested true copy photograph of nominee 1)

(Name and signature with date)

(Name and signature with date)

Permanent Address:

Nominee 1

 Upazila/Thana District Postal Code
 Country
 Phone no. Mobile no. E-mail

Nominee 2

 Upazila/Thana District Postal Code
 Country
 Phone no. Mobile no. E-mail

Note: If the nominee(s) is a non-resident Bangladeshi and the balance of the account becomes payable to him/her, then all formalities as detailed in Foreign Exchange Regulations Act, 1947 will be applicable for remitting fund abroad



09. Mailing Address:

.....

 Upazila/Thana District Postal Code
 Country
 Phone no. Mobile no. E-mail

10. Declaration and Signature:

I/We declare that all information provided in this application and in documents submitted is true, accurate and complete. I/We understand that withholding of information or giving false information will result in refusal of my application.

I/We authorise IDCOL to verify any information provided by me/us.

I/We authorize permission to any person, employee, agent, representative, adviser, subsidiary, affiliate, firm or corporation of IDCOL to release, collect, receive, store, transfer and use any information provided by me/us, or any information obtained in connection with this application, and to disclose such information to its authorised representatives or regulatory bodies or the government or otherwise for the purpose of this application, where IDCOL reasonably considers it is necessary to make such disclosure. I/We waive any and all claims with respect to providing this information. I/We hereby release IDCOL from all liability for any damage or issuing of this information.

I/We declare that I/we have fully read and understood the terms and conditions of the IDCOL Environmental and Social Safeguards/Management Framework.

I/We understand that all fees paid to IDCOL are non-refundable under any circumstances, except as required by law.

I/We declare that I/we have fully read and understood the terms and conditions set out in this disclaimer.

(Please attach an attested true copy photograph)

(Please attach an attested true copy photograph)

(Please attach an attested true copy photograph)

(Signature with date)

Name and designation:

.....

(Signature with date)

Name and designation:

.....

(Signature with date)

Name and designation:

.....



For Office Use Only

Product Code:	Sector Code:
---------------	--------------

Woman Entrepreneur (Please put a ✓ mark where applicable):

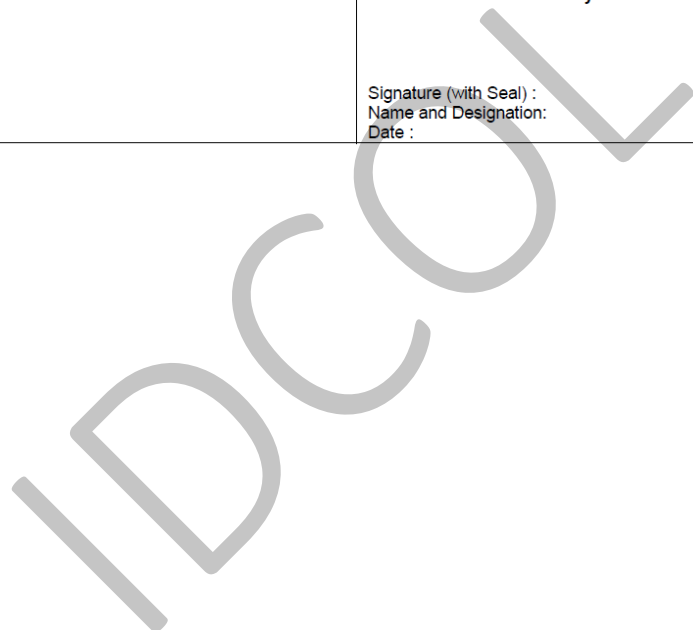
Is there a woman entrepreneur?

Yes

No

Comments:

Account opening officer: Signature (with Seal) : Name and Designation: Date :	Checked and Authorized by: Signature (with Seal) : Name and Designation: Date :
--	--





Account Opening Documentation Checklist

Documents Required

- Completed account opening form
- Completed KYC Profile form
- CIB undertaking
- Proof of address verification: Utility bill (Gas/Electricity/Water)/BTCL Telephone Bill/House Rent /Lease agreement/Proof of personal visit by the RM
- Photograph of applicant (2 copies, attested)
- Photograph of nominee(s) (2 copies, attested)
- Certified true copy of passport
- Certified true copy of the national ID card
- Certified true copy of birth registration certificate
- Copy of e-Tin certificate
- Certified true copy of driving license
- Employee photo ID card of any multinational or listed (with stock exchange) company or Organization
- Signature cards (if applicable)
- List of companies where individual holds directorship position along with shareholding proportion (if applicable)
- Certified true copies of up-to-date IT 10 B/IT 10 BB forms
- Certified true copy of up-to-date net worth statement

Note: In addition to the documents mentioned above, IDCOL reserves the right to require additional documents during its due diligence process

Annexure – L: Individual information Form



Individual Information Form

Date:

For Office Use Only:

Account Number:

Unique Customer ID Number

01. **Name of Customer** *(In English, please use block letters)*

(In Bangla)

02. **Relation with the Account:** *(Please put a ✓ mark where applicable)*

- | | | | |
|---|--|--|---|
| <input type="checkbox"/> 1 st Applicant | <input type="checkbox"/> 2 nd Applicant | <input type="checkbox"/> 3 rd Applicant | <input type="checkbox"/> Director |
| <input type="checkbox"/> Partner | <input type="checkbox"/> Attorney Holder | <input type="checkbox"/> Signatory | <input type="checkbox"/> Ultimate Beneficiary |
| <input type="checkbox"/> Others <i>(Please Specify)</i> | | | |

03. **Father's Name** *(In English)*

(Please use block letters)

(In Bangla)

04. **Mother's Name** *(In English)*

(Please use block letters)

(In Bangla)

05. **Husband/Wife's Name** *(In English)*

(Please use block letters)

(In Bangla)

06. **Nationality**

07. **Date and Place of Birth**

08. **Sex** Male Female Others *(please specify)*

09. **Occupation:** *(Please put a ✓ mark where applicable)*

- | | | | |
|---|---|---|---|
| <input type="checkbox"/> Salaried | <input type="checkbox"/> Self-employed | <input type="checkbox"/> Retired | <input type="checkbox"/> Housewife |
| <input type="checkbox"/> Politician | <input type="checkbox"/> Student | <input type="checkbox"/> Jewelry/gems trade | <input type="checkbox"/> Real estate agent |
| <input type="checkbox"/> Promoter of Construction project | <input type="checkbox"/> Owner of bar/nightclub/ Restaurant/residential hotel | <input type="checkbox"/> Cash investor | <input type="checkbox"/> Share/stock broker |
| <input type="checkbox"/> Others <i>(Please Specify)</i> | | | |



Country

20. Business Address (In English)

(In Bangla)

Upazila/Thana District Postal Code

Country

21. Contact Details Phone: (Home)..... (Office) (Mobile)

E-mail: Fax:

22. Credit Card Related Information Issuing institution and card number (If card user)

1.

2.

3.

23. Residence Status Resident

Non-resident

24. FATCA Compliance (Where applicable)

Please write "Yes" or "No" for each of the following questions.

Are you a U.S resident?

Are you a U.S citizen?

Do you hold a U.S permanent resident card (green card)?

Do You have a U.S residence address or a U.S correspondence address (including a U.S P.O Box) or a U.S telephone number?

Prior consent from U.S citizen clients for reporting customer's account information to IRS (Internal Revenue Services) under FATCA obligations:

"Subject to applicable laws, I hereby consent for Infrastructure Development Company Limited to share my information with domestic or overseas regulators, or tax authorities where necessary to establish my tax liability in any jurisdiction. Where required by domestic or overseas regulators or tax authorities, I consent and agree that Infrastructure Development Company Limited may withhold from my account(s) such amounts as may be required according to applicable laws regulations and directives"

Name:

Signature:

Date:



25. Declaration and Signature:

I/We declare that all information provided in this application and in documents submitted is true, accurate and complete. I/We understand that withholding of information or giving false information will result in refusal of my application.

I/We authorise IDCOL to verify any information provided by me/us.

I/We authorize permission to any person, employee, agent, representative, adviser, subsidiary, affiliate, firm or corporation of IDCOL to release, collect, receive, store, transfer and use any information provided by me/us, or any information obtained in connection with this application, and to disclose such information to its authorised representatives or regulatory bodies or the government or otherwise for the purpose of this application, where IDCOL reasonably considers it is necessary to make such disclosure. I/We waive any and all claims with respect to providing this information. I/We hereby release IDCOL from all liability for any damage or issuing of this information.

I/We declare that I/we have fully read and understood the terms and conditions of the IDCOL Environmental and Social Safeguards/Management Framework.

I/We understand that all fees paid to IDCOL are non-refundable under any circumstances, except as required by law.

I/We declare that I/we have fully read and understood the terms and conditions set out in this disclaimer.

(Please attach an attested true copy photograph)

(Signature with date)

Name and designation:

.....
.....



Documentation Checklist

Documents Required

- CIB undertaking
- Photocopy of National ID Card
- TIN certificate
- Photocopy of passport
- Photocopy of driving license
- Photocopy of birth registration certificate
- Up-to date IT 10 B form
- Shareholding interest in other companies (if applicable)
- Up to date net worth statement
- Photograph of applicant (2 copies, attested)

Note: In addition to the documents mentioned above, IDCOL reserves the right to require additional documents during its due diligence process

IDCOL

Annexure – M: KYC Form



KNOW YOUR CUSTOMER (KYC) PROFILE FORM

(To be used for Opening of Individual and Company Accounts)

Source: Circular No. 02/2015 from Bangladesh Financial Intelligence Unit, Bangladesh Bank.

01. Account Name :		
02. Account Holder's Name :		
03. Account Type and Number :		
04. Unique Customer Identification Code :		
05. Name and Designation of Officer Opening the Account :		
06. Nature of Business :		
07. Birth Certificate No.:	Photocopy Obtained? Yes / No (If Applicable)
08. Passport No. :	Photocopy Obtained? Yes / No (If Applicable)
09. Voter ID Card No. :	Photocopy Obtained? Yes / No (If Applicable)
10. National ID Card No. :	Photocopy Obtained? Yes / No (If Applicable)
11. TIN No. (e-tin only) :	Photocopy Obtained? Yes / No (If Applicable)
12. VAT Registration No. :	Photocopy Obtained? Yes / No (If Applicable)
13. Driving License No. :	Photocopy Obtained? Yes / No (If Applicable)
14. Registration/ Incorporation No. :	Photocopy Obtained? Yes / No (If Applicable)
15. Who is the Beneficial Owner of the account (Detailed information of the shareholder controlling the company and the single shareholder holding 20% or more share) :		
16. What is the source of fund?		
17. Confirmation of whether or not the amount of transaction is commensurate with the nature of business described when the relationship was established.		



18. Overall Risk Assessment :

High

Low

Comments* :

*(*In the comments section, it is mandatory to comment on the client's risk based on subjective judgment. In determining client's risk, nature of client's occupation should be analyzed in details. E.g. in case client's occupation is business, nature of business, magnitude of funds, area of business, size of business, ultimate beneficial ownership of the account, etc. should be kept in consideration in classifying the account as bearing high or low risk. Even in case of service as a profession, risk should be determined in terms of nature of service and responsibilities associated. Regular monitoring is required if the client is highly risky)*

19. In case of a company, does any director of the company/member of executive committee have directorship in any Bank/FI? Yes / No

If yes, please provide details:

20. In case of a company, is/was there any legal proceedings against any director/member of executive committee? Yes / No

If yes, please provide details:

21. In case of a company, is/was there any cases pending against any director/ member of Executive Committee? Yes / No

If yes, please provide details:

22. Has the address(es) of the Account holder been verified? Yes / No

If Yes, How verified?

23. Has any one of the items 7-14 above been verified? Yes / No

If Yes, How verified?

24. For Politically Exposed Persons/Directors/Member of Executive Committee (PEPs) : (Ref.: AML Circular No. 14)



A. Obtained Approval from Senior Management? <i>Yes / No</i>
B. Sources of Fund :
C. Face to Face Interview with the Customer : <i>Yes / No</i>

Account opening officer: Signature (with Seal) : Name and designation: Date :	Checked and Authorized by: Signature (with Seal) : Name and designation: Date :
---	---

25. When was the Account related information Reviewed & Updated last?

Reviewed & Updated by : Signature : Name and designation: Date :



Annexure – N: Signature Mismatch Form

Date:

To,
Infrastructure Development Company Limited (IDCOL)
UTC Building(16th floor), 8 Panthapath,
Kawran Bazar, Dhaka 1215.

Subject: Clarification of Signature Mismatch

Dear Sir / Madam,

I,resident of

.....

.....

..... bearing National ID / Passport / Others (.....) No.

..... hereby declare that as per National ID / Passport / Others
(.....), my signature is:

--

Please be notified that, for the purpose of loan documentation and/or any kind of transactions with IDCOL, the sample signatures provide below along with due attestations will be used:

Sl. No.	Signature
1	
2	
3	

The above sample signatures have been provided in the presence of the following person:

<p>.....</p> <p>(Signature)</p> <p>Name: Designation: Infrastructure Development Company Limited</p>
--

Please also be notified that, all of my signatures provided above are valid & authentic and identify me as same person legally.

.....
(Signature)

Name:

The proof of identification attached is:

NID Passport Others (.....)

IDCOL

Annexure – O: AML & BFIU Circulars

AML Circular No. 22: "Anti-Terrorism Act, 2009"

BFIU Circular No. 02: Regarding "Money Laundering Prevention Act, 2012" and Amendment of "Anti-Terrorism Act, 2012"

BFIU Circular No. 04: Regarding Guidance Notes on Prevention of Money Laundering and Terrorist Financing

BFIU Circular No. 07: Anti-Terrorism (Amendment) Act, 2013

BFIU Circular Letter No. 03: Circulation of Money Laundering Prevention Rules, 2013 and Anti-Terrorism Rules, 2013

BFIU Circular No. 12: Master Circular regarding Instructions to be followed by the Financial Institutions for the prevention of Money Laundering & Terrorist Financing

BFIU Circular Letter No. 04: Money Laundering and Terrorist Financing Risk Assessment Guidelines for Financial Institutions

BFIU Circular Letter No. 06: Circulation of Money Laundering Prevention (Amendment) Act, 2015

BFIU Circular Letter No. 01: Instructions to be followed for the compliance of Freezing Accounts of listed Individuals or Institutions and Other Issues under the Sanction List of Different Resolutions of United Nations Security Council

Please see the attached booklet of AML & BFIU Circulars

Booklets

Booklet of Financial Action Task Force (FATF)

Booklet of Money Laundering Prevention Act and Anti-Terrorist Act

Booklet of AML & BFIU Circulars

IDCOL

FATF



INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING OF
TERRORISM & PROLIFERATION

The FATF Recommendations

February 2012

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING
OF TERRORISM & PROLIFERATION

THE FATF RECOMMENDATIONS

FEBRUARY 2012

Updated October 2016



FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2012), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, updated October 2016, FATF, Paris, France,
www.fatf-gafi.org/recommendations.html

© 2016 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

CONTENTS

List of the FATF Recommendations	4
Introduction	7
FATF Recommendations	11
Interpretive Notes	31
Note on the legal basis of requirements on financial institutions and DNFBPs	111
Glossary	113
Table of Acronyms	128
Annex I: FATF Guidance Documents	129
Annex II: Information on updates made to the FATF Recommendations	131

THE FATF RECOMMENDATIONS

Number	Old Number ¹	
A – AML/CFT POLICIES AND COORDINATION		
1	-	Assessing risks & applying a risk-based approach *
2	R.31	National cooperation and coordination
B – MONEY LAUNDERING AND CONFISCATION		
3	R.1 & R.2	Money laundering offence *
4	R.3	Confiscation and provisional measures *
C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION		
5	SRII	Terrorist financing offence *
6	SRIII	Targeted financial sanctions related to terrorism & terrorist financing *
7		Targeted financial sanctions related to proliferation *
8	SRVIII	Non-profit organisations *
D – PREVENTIVE MEASURES		
9	R.4	Financial institution secrecy laws
		<i>Customer due diligence and record keeping</i>
10	R.5	Customer due diligence *
11	R.10	Record keeping
		<i>Additional measures for specific customers and activities</i>
12	R.6	Politically exposed persons *
13	R.7	Correspondent banking *
14	SRVI	Money or value transfer services *
15	R.8	New technologies
16	SRVII	Wire transfers *
		<i>Reliance, Controls and Financial Groups</i>
17	R.9	Reliance on third parties *
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries *
19	R.21	Higher-risk countries *
		<i>Reporting of suspicious transactions</i>
20	R.13 & SRIV	Reporting of suspicious transactions *
21	R.14	Tipping-off and confidentiality
		<i>Designated non-financial Businesses and Professions (DNFBPs)</i>
22	R.12	DNFBPs: Customer due diligence *
23	R.16	DNFBPs: Other measures *

E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *

F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES

Regulation and Supervision

26	R.23	Regulation and supervision of financial institutions *
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs

Operational and Law Enforcement

29	R.26	Financial intelligence units *
30	R.27	Responsibilities of law enforcement and investigative authorities *
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers *

General Requirements

33	R.32	Statistics
34	R.25	Guidance and feedback

Sanctions

35	R.17	Sanctions
-----------	------	-----------

G – INTERNATIONAL COOPERATION

36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation *
39	R.39	Extradition
40	R.40	Other forms of international cooperation *

1. The 'old number' column refers to the corresponding 2003 FATF Recommendation.

* Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.

Version as adopted on 15 February 2012.

INTRODUCTION

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

Following the conclusion of the third round of mutual evaluations of its members, the FATF has reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.

The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.

Combating terrorist financing is a very significant challenge. An effective AML/CFT system, in general, is important for addressing terrorist financing, and most measures previously focused on terrorist financing are now integrated throughout the Recommendations, therefore obviating the need for the Special Recommendations. However, there are some Recommendations that are unique to terrorist financing, which are set out in Section C of the FATF Recommendations. These are: Recommendation 5 (the criminalisation of terrorist financing); Recommendation 6 (targeted financial sanctions related to terrorism & terrorist financing); and Recommendation 8 (measures to prevent the misuse of non-profit organisations). The proliferation of weapons of mass destruction is also a significant security concern, and in 2008 the FATF's mandate was expanded to include dealing with the financing of proliferation of weapons of mass destruction. To combat this threat, the FATF has adopted a new Recommendation (Recommendation 7) aimed at ensuring consistent and effective implementation of targeted financial sanctions when these are called for by the UN Security Council.

The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs, and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank – on the basis of the FATF's common assessment methodology. Some Interpretive Notes and definitions in the glossary include examples which illustrate how the requirements could be applied. These examples are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

The FATF also produces Guidance, Best Practice Papers, and other advice to assist countries with the implementation of the FATF standards. These other documents are not mandatory for assessing compliance with the Standards, but countries may find it valuable to have regard to them when considering how best to implement the FATF Standards. A list of current FATF Guidance and Best

Practice Papers, which are available on the FATF website, is included as an annex to the Recommendations.

The FATF is committed to maintaining a close and constructive dialogue with the private sector, civil society and other interested parties, as important partners in ensuring the integrity of the financial system. The revision of the Recommendations has involved extensive consultation, and has benefited from comments and suggestions from these stakeholders. Going forward and in accordance with its mandate, the FATF will continue to consider changes to the standards, as appropriate, in light of new information regarding emerging threats and vulnerabilities to the global financial system.

The FATF calls upon all countries to implement effective measures to bring their national systems for combating money laundering, terrorist financing and the financing of proliferation into compliance with the revised FATF Recommendations.

THE FATF RECOMMENDATIONS

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach *

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence *

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures *

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of *bona fide* third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence *

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing *

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation *

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. 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.

8. Non-profit organisations *

Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

- (a) by terrorist organisations posing as legitimate entities;
- (b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
- (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence *

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

- (i) establishing business relations;
- (ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- (iii) there is a suspicion of money laundering or terrorist financing; or
- (iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

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

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons *

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

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

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking *

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

- (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- (b) assess the respondent institution's AML/CFT controls;
- (c) obtain approval from senior management before establishing new correspondent relationships;
- (d) clearly understand the respective responsibilities of each institution; and
- (e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services *

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTs) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTs without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTs provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTs provider and its agents operate. Countries should take measures to ensure that MVTs providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

16. Wire transfers *

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties *

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

The criteria that should be met are as follows:

- (a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.
- (b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- (c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.
- (d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries *

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries *

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions *

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

- (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and
- (b) prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence *

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

- (a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.
- (b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.
- (c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

- (d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:
- buying and selling of real estate;
 - managing of client money, securities or other assets;
 - management of bank, savings or securities accounts;
 - organisation of contributions for the creation, operation or management of companies;
 - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
- (e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:
- acting as a formation agent of legal persons;
 - acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
 - providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
 - acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
 - acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures *

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

- (a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
- (b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

- (c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons *

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements *

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs *

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

- (a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:
 - casinos should be licensed;

- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
 - competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.
- (b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a “fit and proper” test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units *

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary,

cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers *

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

- (a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.
- (b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.
- (c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
- (d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).
- (e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

- (a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and
- (b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation *

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

- (a) ensure money laundering and terrorist financing are extraditable offences;
- (b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;
- (c) not place unreasonable or unduly restrictive conditions on the execution of requests; and
- (d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation *

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing

cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

INTERPRETIVE NOTES TO THE FATF RECOMMENDATIONS

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH)

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.
2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

A. Obligations and decisions for countries

3. **Assessing risk** - Countries¹ should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.
4. **Higher risk** - Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.
5. **Lower risk** - Countries may decide to allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 3.

Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified customer due diligence (CDD) measures, provided that the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 7 below, are met.

6. **Exemptions** - Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:
 - (a) there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or
 - (b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.

¹ Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

7. **Supervision and monitoring of risk** - Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.

B. Obligations and decisions for financial institutions and DNFBPs

8. **Assessing risk** - Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.
9. **Risk management and mitigation** - Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.
10. **Higher risk** - Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks.
11. **Lower risk** - Where lower risks are identified, countries may allow financial institutions and DNFBPs to take simplified measures to manage and mitigate those risks.
12. When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

INTERPRETIVE NOTE TO RECOMMENDATION 3 (MONEY LAUNDERING OFFENCE)

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).
2. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.
3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.
4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.
5. Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.
6. Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.
7. Countries should ensure that:
 - (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.
 - (b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.
 - (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of

liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

- (d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

INTERPRETIVE NOTE TO RECOMMENDATIONS 4 AND 38 (CONFISCATION AND PROVISIONAL MEASURES)

Countries should establish mechanisms that will enable their competent authorities to effectively manage and, when necessary, dispose of, property that is frozen or seized, or has been confiscated. These mechanisms should be applicable both in the context of domestic proceedings, and pursuant to requests by foreign countries.

INTERPRETIVE NOTE TO RECOMMENDATION 5 (TERRORIST FINANCING OFFENCE)

A. Objectives

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.

B. Characteristics of the terrorist financing offence

2. Terrorist financing offences should extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.
3. Terrorist financing includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.
4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with this Recommendation.
5. Terrorist financing offences should extend to any funds or other assets, whether from a legitimate or illegitimate source.
6. Terrorist financing offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).
7. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.
8. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.
9. Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.
10. It should also be an offence to attempt to commit the offence of terrorist financing.
11. It should also be an offence to engage in any of the following types of conduct:
 - (a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

- (b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;
 - (c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.
12. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

INTERPRETIVE NOTE TO RECOMMENDATION 6 (TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING)

A. OBJECTIVE

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person² or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions³; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).
2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)⁴. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

² Natural or legal person.

³ Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

⁴ Based on requirements set, for instance, in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention)* and the *United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention)*, which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the *International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention)* contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

B. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their own motion, or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.
4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions⁵. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list-based programmes, pursuant to those Security Council resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:
 - (a) Countries should identify a competent authority or a court as having responsibility for:
 - (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;
 - (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and

⁵ The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

- (iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.
- (b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination whether they are satisfied, according to applicable (supra-) national principles, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2011), as set forth in Section E.
- (c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.
- (d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.
- (e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:
 - (i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;

- (ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;
 - (iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and
 - (iv) specify whether their status as a designating state may be made known.
- (f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:
- (i) follow the procedures for listing, as adopted by the 1988 Committee;
 - (ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and
 - (iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.
- (g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

- (h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.
6. Countries should establish the necessary legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:
- (a) Countries⁶ should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.
- (b) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or

⁶ In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

- (c) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.
- (d) Countries should require financial institutions and DNFBPs⁷ to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.
- (e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

- 7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.
- 8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.
- 9. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of

⁷ Security Council resolutions apply to all natural and legal persons within the country.

such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to resolution 1373 (2001) and as set out in resolution 1963 (2010).
11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.
12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:
 - (a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions**⁸:
 - (i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof⁹; or

⁸ Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

⁹ OP2 of resolution 1617 (2005) further defines the criteria for being “associated with” Al-Qaida or Usama bin Laden.

- (ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.
- (b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions:**
 - (i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or
 - (ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.
- (c) **Security Council resolution 1373 (2001):**
 - (i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;
 - (ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c) (i) of this subparagraph; or
 - (iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c) (i) of this subparagraph.

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions¹⁰ to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person¹¹ or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.¹²
2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.¹³ The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

B DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations

¹⁰ Recommendation 7 is focused on targeted financial sanctions. However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions and vigilance provisions). With respect to other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs. With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction, the FATF has also issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

¹¹ Natural or legal person.

¹² Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Recommendation, (February 2012), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010).

¹³ Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and Security Council resolution 1540 (2004). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

to the relevant Security Council Committees. However, in practice, the Committees primarily depend upon requests for designation by Member States. Security Council resolutions 1718 (2006) and 1737 (2006) provide that the relevant Committees shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by these resolutions.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:
 - (a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:
 - (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions¹⁴, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and
 - (ii) proposing to the 1737 Sanctions Committee, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 1737 (2006) and its successor resolutions¹⁵, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).
 - (b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 1737 (2006), and their successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.
 - (c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

¹⁴ Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009).

¹⁵ Recommendation 7 is applicable to all current and future successor resolutions to S/RES/1737 (2006). At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1737 (2006) are: resolution 1747 (2007), resolution 1803 (2008), and resolution 1929 (2010).

- (d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.
- (e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the 1737 Sanctions Committee, pursuant to resolution 1737 (2006) and its successor resolutions, providing as much detail as possible on:
 - (i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and
 - (ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).
- (f) having procedures to be able, where necessary, to operate *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

- 5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:
 - (a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council; and
 - (b) in the case of resolution 1737 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1737 Sanctions Committee of the Security Council,

when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations.

- 6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:
 - (a) Countries¹⁶ should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated

¹⁶ In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU regulations (as amended). EU member states may have to take additional measures to implement the

persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

- (b) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).
- (c) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.
- (d) Countries should require financial institutions and DNFBPs¹⁷ to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.
- (e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 7.
- (f) Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBPs with the relevant laws or enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

D DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

- 7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer

freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

¹⁷ Security Council resolutions apply to all natural and legal persons within the country.

exists. Such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e., a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.
9. Where countries have determined that the exemption conditions set out in resolution 1718 (2006) and resolution 1737 (2006) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.
10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 1737 (2006) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.
11. Freezing action taken pursuant to resolution 1737 (2006) shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:
 - (a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in the relevant Security Council resolution;
 - (b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity designated pursuant to resolution 1737 (2006); and
 - (c) the relevant countries have submitted prior notification to the 1737 Sanctions Committee of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.¹⁸
12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBS immediately upon taking such action, and providing adequate

¹⁸ In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, adopted in September 2007.

guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolution are:

(a) **Resolution 1718 (2006):**

- (i) Any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programs;
- (ii) any person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programs, including through illicit means;
- (iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)¹⁹; or
- (iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)²⁰.

(b) **Resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010):**

- (i) any person or entity engaged in Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
- (ii) any person or entity directly associated with or providing support for Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
- (iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i) and/or subsection 13(b)(ii), or by entities owned or controlled by them;
- (iv) any person or entity acting on behalf or at the direction of the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929 (2010);
- (v) any entity owned or controlled, including through illicit means, by the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929 (2010)²¹;

¹⁹ The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee.

²⁰ Ibid.

²¹ Ibid.

- (vi) any person or entity acting on behalf or at the direction of the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929 (2010);
- (vii) entities owned or controlled, including through illicit means, by the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929 (2010); or
- (viii) any person or entity determined by the United Nations Security Council or the Committee to have assisted designated persons or entities in evading sanction of, or in violating the provisions of, S/RES/1737 (2006), S/RES/1747 (2007), S/RES/1803 (2008), or S/RES/1929 (2010).

INTERPRETIVE NOTE TO RECOMMENDATION 8 (NON-PROFIT ORGANISATIONS)

A. INTRODUCTION

1. Given the variety of legal forms that non-profit organisations (NPOs) can have, depending on the country, the FATF has adopted a functional definition of NPO. This definition is based on those activities and characteristics of an organisation which put it at risk of terrorist financing abuse, rather than on the simple fact that it is operating on a non-profit basis. For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”. Without prejudice to Recommendation 1, this Recommendation only applies to those NPOs which fall within the FATF definition of an NPO. It does not apply to the entire universe of NPOs.
2. NPOs play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The FATF recognises the vital importance of NPOs in providing these important charitable services, as well as the difficulty of providing assistance to those in need, often in high risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognises the intent and efforts to date of NPOs to promote transparency within their operations and to prevent terrorist financing abuse, including through the development of programmes aimed at discouraging radicalisation and violent extremism. The ongoing international campaign against terrorist financing has identified cases in which terrorists and terrorist organisations exploit some NPOs in the sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. As well, there have been cases where terrorists create sham charities or engage in fraudulent fundraising for these purposes. This misuse not only facilitates terrorist activity, but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting NPOs from terrorist financing abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs and the donor community. Measures to protect NPOs from potential terrorist financing abuse should be targeted and in line with the risk-based approach. It is also important for such measures to be implemented in a manner which respects countries’ obligations under the Charter of the United Nations and international human rights law.
3. Some NPOs may be vulnerable to terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. In some cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate some NPOs and misuse funds and operations to cover for, or support, terrorist activity.

B. OBJECTIVES AND GENERAL PRINCIPLES

4. The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:
- (a) A risk-based approach applying focused measures in dealing with identified threats of terrorist financing abuse to NPOs is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to terrorist financing abuse, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.
 - (b) Flexibility in developing a national response to terrorist financing abuse of NPOs is essential, in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.
 - (c) Past and ongoing terrorist financing abuse of NPOs requires countries to adopt effective and proportionate measures, which should be commensurate to the risks identified through a risk-based approach.
 - (d) Focused measures adopted by countries to protect NPOs from terrorist financing abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote accountability and engender greater confidence among NPOs, across the donor community and with the general public, that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of NPOs are integral to ensuring they cannot be abused for terrorist financing.
 - (e) Countries are required to identify and take effective and proportionate action against NPOs that either are exploited by, or knowingly supporting, terrorists or terrorist organisations taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should, to the extent reasonably possible, minimise negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.
 - (f) Developing cooperative relationships among the public and private sectors and with NPOs is critical to understanding NPOs' risks and risk mitigation strategies, raising awareness, increasing effectiveness and fostering capabilities to combat terrorist

financing abuse within NPOs. Countries should encourage the development of academic research on, and information-sharing in, NPOs to address terrorist financing related issues.

C. MEASURES

5. Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), countries should identify which subset of organisations fall within the FATF definition of NPO. In undertaking this exercise, countries should use all relevant sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse.²² It is also crucial to identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs. Countries should review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified. These exercises could take a variety of forms and may or may not be a written product. Countries should also periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures.
6. There is a diverse range of approaches in identifying, preventing and combating terrorist financing abuse of NPOs. An effective approach should involve all four of the following elements: (a) sustained outreach, (b) targeted risk-based supervision or monitoring, (c) effective investigation and information gathering and (d) effective mechanisms for international cooperation. The following measures represent examples of specific actions that countries should take with respect to each of these elements, in order to protect NPOs from potential terrorist financing abuse.
 - (a) Sustained outreach concerning terrorist financing issues
 - (i) Countries should have clear policies to promote accountability, integrity and public confidence in the administration and management of NPOs.
 - (ii) Countries should encourage and undertake outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.
 - (iii) Countries should work with NPOs to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect them from terrorist financing abuse.

²² For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

(iv) Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

(b) Targeted risk-based supervision or monitoring of NPOs

Countries should take steps to promote effective supervision or monitoring. A “one-size-fits-all” approach would be inconsistent with the proper implementation of a risk-based approach as stipulated under Recommendation 1 of the FATF Standards. In practice, countries should be able to demonstrate that risk-based measures apply to NPOs at risk of terrorist financing abuse. It is also possible that existing regulatory or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a jurisdiction, although terrorist financing risks to the sector should be periodically reviewed. Appropriate authorities should monitor the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them.²³ Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.²⁴ The following are some examples of measures that could be applied to NPOs, in whole or in part, depending on the risks identified:

- (i) NPOs could be required to license or register. This information should be available to competent authorities and encouraged to be available to the public.²⁵
- (ii) NPOs could be required to maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information could be publicly available either directly from the NPO or through appropriate authorities.
- (iii) NPOs could be required to issue annual financial statements that provide detailed breakdowns of incomes and expenditures.
- (iv) NPOs could be required to have appropriate controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPO’s stated activities.
- (v) NPOs could be required to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries²⁶ and associate NPOs and that

²³ In this context, rules and regulations may include rules and standards applied by self-regulatory organisations and accrediting institutions.

²⁴ The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

²⁵ Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations²⁷. However, NPOs should not be required to conduct customer due diligence. NPOs could be required to take reasonable measures to document the identity of their significant donors and to respect donor confidentiality. The ultimate objective of this requirement is to prevent charitable funds from being used to finance and support terrorists and terrorist organisations.

- (vi) NPOs could be required to maintain, for a period of at least five years, records of domestic and international transactions that are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the organisation, and could be required to make these available to competent authorities upon appropriate authority. This also applies to information mentioned in paragraphs (ii) and (iii) above. Where appropriate, records of charitable activities and financial operations by NPOs could also be made available to the public.
- (c) Effective information gathering and investigation
- (i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.
 - (ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.
 - (iii) Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.
 - (iv) Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action.

²⁶ The term beneficiaries refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.

²⁷ This does not mean that NPOs are expected to identify each specific individual, as such a requirement would not always be possible and would, in some instances, impede the ability of NPOs to provide much-needed services

- (d) Effective capacity to respond to international requests for information about an NPO of concern. Consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

D. RESOURCES FOR SUPERVISION, MONITORING, AND INVESTIGATION

7. Countries should provide their appropriate authorities, which are responsible for supervision, monitoring and investigation of their NPO sector, with adequate financial, human and technical resources.

Glossary of specific terms used in this Recommendation

Appropriate authorities	refers to competent authorities, including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions.
Associate NPOs	includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.
Beneficiaries	refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
Non-profit organisation or NPO	refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.
Terrorist financing abuse	refers to the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING-OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:
 - (a) normally seek to identify and verify the identity²⁸ of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and
 - (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.
2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.
3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements²⁹, financial institutions should be required to identify and verify the identity of

²⁸ Reliable, independent source documents, data or information will hereafter be referred to as "identification data."

²⁹ In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue

the customer, and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

- (a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:
 - (i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.
 - (ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).
 - (iii) The address of the registered office, and, if different, a principal place of business.
- (b) Identify the beneficial owners of the customer and take reasonable measures³⁰ to verify the identity of such persons, through the following information:
 - (i) For legal persons³¹:
 - (i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest³² in a legal person; and

to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

³⁰ In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

³¹ Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

³² A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

- (i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.
 - (i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.
- (ii) For legal arrangements:
- (ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries³³, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);
 - (ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:
- (a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;
 - (b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the

³³ For beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.
8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.
9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:
 - Non face-to-face business.
 - Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers³⁴ on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

H. RISK BASED APPROACH³⁵

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:³⁶

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.

³⁴ Existing customers as at the date that the national requirements are brought into force.

³⁵ The RBA does not apply to the circumstances when CDD should be required but may be used to determine the extent of such measures.

³⁶ Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
 - Countries identified by credible sources as having significant levels of corruption or other criminal activity.
 - Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.
- (c) Product, service, transaction or delivery channel risk factors:
- Private banking.
 - Anonymous transactions (which may include cash).
 - Non-face-to-face business relationships or transactions.
 - Payment received from unknown or un-associated third parties

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.
17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:
- (a) Customer risk factors:
- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
 - Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
 - Public administrations or enterprises.
- (b) Product, service, transaction or delivery channel risk factors:
- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
 - Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

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

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
 - Reducing the frequency of customer identification updates.
 - Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
 - Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

23. Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

INTERPRETIVE NOTE TO RECOMMENDATION 12 (POLITICALLY EXPOSED PERSONS)

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

- a) inform senior management before the payout of the policy proceeds; and
- b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

INTERPRETIVE NOTE TO RECOMMENDATION 13 (CORRESPONDENT BANKING)

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

INTERPRETIVE NOTE TO RECOMMENDATION 14 (MONEY OR VALUE TRANSFER SERVICES)

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

INTERPRETIVE NOTE TO RECOMMENDATION 16 (WIRE TRANSFERS)

A. OBJECTIVE

1. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:
 - (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;
 - (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and
 - (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.
2. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

B. SCOPE

3. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers , including serial payments, and cover payments.
4. Recommendation 16 is not intended to cover the following types of payments:
 - (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.
 - (b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

5. Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:
 - (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.
 - (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

C. CROSS-BORDER QUALIFYING WIRE TRANSFERS

6. Information accompanying all qualifying wire transfers should always contain:
 - (a) the name of the originator;
 - (b) the originator account number where such an account is used to process the transaction;
 - (c) the originator's address, or national identity number, or customer identification number³⁷, or date and place of birth;
 - (d) the name of the beneficiary; and
 - (e) the beneficiary account number where such an account is used to process the transaction.
7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.
8. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

D. DOMESTIC WIRE TRANSFERS

9. Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter

³⁷ The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

10. The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS

Ordering financial institution

11. The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.
12. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.
13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.
14. The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.

Intermediary financial institution

15. For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it
16. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.
17. An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.
18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

Beneficiary financial institution

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.
20. For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.
21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTs) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTs provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTs provider:
 - (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and
 - (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Glossary of specific terms used in this Recommendation

Accurate	is used to describe information that has been verified for accuracy.
Batch transfer	is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
Beneficiary Financial Institution	refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.
Cover Payment	refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

Glossary of specific terms used in this Recommendation

Cross-border wire transfer	refers to any <i>wire transfer</i> where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of <i>wire transfer</i> in which at least one of the financial institutions involved is located in a different country.
Domestic wire transfers	refers to any <i>wire transfer</i> where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of <i>wire transfer</i> that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of <i>wire transfer</i> that takes place entirely within the borders of the European Economic Area (EEA) ³⁸ .
Intermediary financial institution	refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
Ordering financial institution	refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
Originator	refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
Qualifying wire transfers	means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.
Required	is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the <i>required originator information</i> . Subparagraphs 6(d) and 6(e) set out the <i>required beneficiary information</i> .
Serial Payment	refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering

³⁸ An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

Glossary of specific terms used in this Recommendation

	financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).
Straight-through processing	refers to payment transactions that are conducted electronically without the need for manual intervention.
Unique transaction reference number	refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
Wire transfer	refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. ³⁹

³⁹ It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).

INTERPRETIVE NOTE TO RECOMMENDATION 17 (RELIANCE ON THIRD PARTIES)

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.
2. For the purposes of Recommendation 17, the term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.
3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

INTERPRETIVE NOTE TO RECOMMENDATION 18 (INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES)

1. Financial institutions' programmes against money laundering and terrorist financing should include:
 - (a) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;
 - (b) an ongoing employee training programme; and
 - (c) an independent audit function to test the system.
2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.
3. Compliance management arrangements should include the appointment of a compliance officer at the management level.
4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place.
5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including, as appropriate, requesting the financial group to close down its operations in the host country.

INTERPRETIVE NOTE TO RECOMMENDATION 19 (HIGHER-RISK COUNTRIES)

1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.
2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:
 - (a) Requiring financial institutions to apply specific elements of enhanced due diligence.
 - (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.
 - (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
 - (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.
 - (e) Limiting business relationships or financial transactions with the identified country or persons in that country.
 - (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.
 - (g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.
 - (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.
 - (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries

INTERPRETIVE NOTE TO RECOMMENDATION 20 (REPORTING OF SUSPICIOUS TRANSACTIONS)

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.
2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.
3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.
4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called “indirect reporting”), is not acceptable.

INTERPRETIVE NOTE TO RECOMMENDATIONS 22 AND 23 (DNFBPS)

1. The designated thresholds for transactions are as follows:
 - Casinos (under Recommendation 22) - USD/EUR 3,000
 - For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions, so long as these businesses or professions are included in laws or enforceable means covering the underlying activities.

INTERPRETIVE NOTE TO RECOMMENDATION 22 (DNFBPS – CUSTOMER DUE DILIGENCE)

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.
2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

INTERPRETIVE NOTE TO RECOMMENDATION 23 (DNFBPS – OTHER MEASURES)

1. Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.
3. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.
4. Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

INTERPRETIVE NOTE TO RECOMMENDATION 24 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS)

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information⁴⁰) that are created⁴¹ in the country. Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. It is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective.
2. As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:
 - (a) identify and describe the different types, forms and basic features of legal persons in the country.
 - (b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;
 - (c) make the above information publicly available; and
 - (d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country.

A. BASIC INFORMATION

3. In order to determine who the beneficial owners of a company are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.
4. All companies created in a country should be registered in a company registry.⁴² Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company⁴³ as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

⁴⁰ Beneficial ownership information for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (e.g. 25%).

⁴¹ References to creating a legal person, include incorporation of companies or any other mechanism that is used.

⁴² "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

⁴³ The information can be recorded by the company itself or by a third person under the company's responsibility.

- (a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors; and
 - (b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder⁴⁴ and categories of shares (including the nature of the associated voting rights).
5. The company registry should record all the basic information set out in paragraph 4(a) above.
6. The company should maintain the basic information set out in paragraph 4(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

B. BENEFICIAL OWNERSHIP INFORMATION

7. Countries should ensure that either: (a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority.
8. In order to meet the requirements in paragraph 7, countries should use one or more of the following mechanisms:
 - (a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;
 - (b) Requiring companies to take reasonable measures⁴⁵ to obtain and hold up-to-date information on the companies' beneficial ownership;
 - (c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22⁴⁶; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators); (iii) information held by the company as required above in Section A; and (iv) available information on companies listed on a stock exchange, where disclosure requirements (either by stock exchange rules or through law or enforceable means) impose requirements to ensure adequate transparency of beneficial ownership.

⁴⁴ This is applicable to the nominal owner of all registered shares.

⁴⁵ Measures taken should be proportionate to the level of risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders.

⁴⁶ Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

9. Regardless of which of the above mechanisms are used, countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner. This should include:
 - (a) Requiring that one or more natural persons resident in the country is authorised by the company⁴⁷, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or
 - (b) Requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or
 - (c) Other comparable measures, specifically identified by the country, which can effectively ensure cooperation.
10. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

C. TIMELY ACCESS TO CURRENT AND ACCURATE INFORMATION

11. Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis. Countries should require that any available information referred to in paragraph 7 is accurate and is kept as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.
12. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.
13. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above.

D. OBSTACLES TO TRANSPARENCY

14. Countries should take measures to prevent the misuse of bearer shares and bearer share warrants, for example by applying one or more of the following mechanisms: (a) prohibiting

⁴⁷ Members of the company's board or senior management may not require specific authorisation by the company.

them; (b) converting them into registered shares or share warrants (for example through dematerialisation); (c) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary; or (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity.

15. Countries should take measures to prevent the misuse of nominee shares and nominee directors, for example by applying one or more of the following mechanisms: (a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or (b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request.

E. OTHER LEGAL PERSONS

16. In relation to foundations, Anstalt, and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures.
17. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and current by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and current beneficial ownership information for such legal persons.

F. LIABILITY AND SANCTIONS

18. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. INTERNATIONAL COOPERATION

19. Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor

the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

INTERPRETIVE NOTE TO RECOMMENDATION 25 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS)

1. Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.
2. All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when, as a trustee, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust⁴⁸; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.
3. Countries are encouraged to ensure that other relevant authorities, persons and entities hold information on all trusts with which they have a relationship. Potential sources of information on trusts, trustees, and trust assets are:
 - (a) Registries (e.g. a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets.
 - (b) Other competent authorities that hold information on trusts and trustees (e.g. tax authorities which collect information on assets and income relating to trusts).
 - (c) Other agents and service providers to the trust, including investment advisors or managers, lawyers, or trust and company service providers.
4. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the information held by trustees and other parties, in particular information held by financial institutions and DNFBPs on: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.
5. Professional trustees should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust ceases. Countries are encouraged to require non-professional trustees and the other authorities, persons and entities mentioned in paragraph 3 above to maintain the information for at least five years.

⁴⁸ Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

6. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and be as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.
7. Countries should consider measures to facilitate access to any information on trusts that is held by the other authorities, persons and entities referred to in paragraph 3, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.
8. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 2 and 6 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

Other Legal Arrangements

9. As regards other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified above in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities.

International Cooperation

10. Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

Liability and Sanctions

11. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 2, 6 and (where applicable) 5; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.⁴⁹ Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to

⁴⁹ This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

grant to competent authorities timely access to information regarding the trust referred to in paragraphs 1 and 5.

INTERPRETIVE NOTE TO RECOMMENDATION 26 (REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS)

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.
2. Adopting a risk-based approach to supervising financial institutions' AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group (or groups, when applicable for Core Principles institutions). The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile, and on the money laundering and terrorist financing risks present in the country.
3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.
4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.
5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

Resources of supervisors

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and

autonomy to ensure freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPS)

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.
2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.
3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.
4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS)

A. GENERAL

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

B. FUNCTIONS

(a) Receipt

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

(b) Analysis

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

(c) Dissemination

4. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination.
 - **Spontaneous dissemination:** The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
 - **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

C. ACCESS TO INFORMATION**(a) Obtaining Additional Information from Reporting Entities**

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

(b) Access to Information from other sources

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

D. INFORMATION SECURITY AND CONFIDENTIALITY

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

E. OPERATIONAL INDEPENDENCE

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.
9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.
10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.
11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

F. UNDUE INFLUENCE OR INTERFERENCE

12. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

G. EGMONT GROUP

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

H. LARGE CASH TRANSACTION REPORTING

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

INTERPRETIVE NOTE TO RECOMMENDATION 30 (RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES)

1. There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation.
2. A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to:
 - identifying the extent of criminal networks and/or the scale of criminality;
 - identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and
 - developing evidence which can be used in criminal proceedings.
3. A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.
4. Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing cases to postpone or waive the arrest of suspected persons and/or the seizure of the money, for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.
5. Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.
6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.
7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.
8. Law enforcement authorities and prosecutorial authorities should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the

staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INTERPRETIVE NOTE TO RECOMMENDATION 32 (CASH COURIERS)

A. OBJECTIVES

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical cross-border transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

B. THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.
 - (a) *Written declaration system for all travellers:* In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a “yes” or “no” box).
 - (b) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

- (c) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the “red channel” (goods to declare) and the “green channel” (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

C. ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

5. Whichever system is implemented, countries should ensure that their system incorporates the following elements:
- (a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.
 - (b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs and their intended use.
 - (c) Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious cross-border transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way.
 - (d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.
 - (e) In the following two cases, competent authorities should be able to stop or restrain cash or BNIs for a reasonable time, in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.
 - (f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of

money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

- (g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

D. SANCTIONS

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.
7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

E. GOLD, PRECIOUS METALS AND PRECIOUS STONES

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

Glossary of specific terms used in this Recommendation

False declaration	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is

Glossary of specific terms used in this Recommendation

asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

Physical cross-border transportation

refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.

Related to terrorist financing or money laundering

when used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

INTERPRETIVE NOTE TO RECOMMENDATION 38 (MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION)

1. Countries should consider establishing an asset forfeiture fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes. Countries should take such measures as may be necessary to enable them to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions.
2. With regard to requests for cooperation made on the basis of non-conviction based confiscation proceedings, countries need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.

INTERPRETIVE NOTE TO RECOMMENDATION 40 (OTHER FORMS OF INTERNATIONAL COOPERATION)

A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION

Obligations on requesting authorities

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.

Unduly restrictive measures

2. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:
 - (a) the request is also considered to involve fiscal matters; and/or
 - (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or
 - (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or
 - (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

Safeguards on information exchanged

3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.
4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry⁵⁰, consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of

⁵⁰ Information may be disclosed if such disclosure is required to carry out the request for cooperation.

information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.

Power to search for information

5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

B. PRINCIPLES APPLICABLE TO SPECIFIC FORMS OF INTERNATIONAL COOPERATION

6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.

Exchange of information between FIUs

7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.
8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.
9. FIUs should have the power to exchange:
 - (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and
 - (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors⁵¹

10. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

⁵¹ This refers to financial supervisors which are competent authorities.

11. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:
 - (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors.
 - (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.
 - (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.
12. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.
13. Any dissemination of information exchanged or use of that information for supervisory and non-supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

Exchange of information between law enforcement authorities

14. Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.
15. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.
16. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or

multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

Exchange of information between non-counterparts

17. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.
18. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS

1. All requirements for financial institutions or DNFBPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).
2. In Recommendations 10, 11 and 20, the term “*law*” refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country’s constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.
3. The term “*Enforceable means*” refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).
4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:
 - (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:
 - (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;
 - (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).
 - (b) The document/mechanism must be issued or approved by a competent authority.
 - (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:
 - (i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

- (ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and
 - (iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.
- 5. In all cases it should be apparent that financial institutions and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to “accounts” should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, <i>agent</i> means any natural or legal person providing MVTs on behalf of an MVTs provider, whether by contract with or under the direction of the MVTs provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	<i>Bearer negotiable instruments (BNIs)</i> includes monetary instruments in bearer form such as: traveller’s cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee’s name omitted.
Bearer shares	<i>Bearer shares</i> refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	<i>Beneficial owner</i> refers to the natural person(s) who ultimately ⁵² owns or controls a customer ⁵³ and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiaries	Please refer to the IN to Recommendation 8.
Beneficiary	The meaning of the term <i>beneficiary</i> in the FATF Recommendations depends on the context: <ul style="list-style-type: none"> ■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or

⁵² Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

⁵³ This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
	<p>statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.</p> <ul style="list-style-type: none"> ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. <p>Please also refer to the Interpretive Notes to Recommendation 16.</p>
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Competent authorities	<p><i>Competent authorities</i> refers to all public authorities⁵⁴ with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.</p>
Confiscation	<p>The term <i>confiscation</i>, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or</p>

⁵⁴ This includes financial supervisors established as independent non-governmental authorities with statutory powers.

Terms	Definitions
	forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	<i>Core Principles</i> refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	<i>Correspondent banking</i> is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to <i>country</i> or <i>countries</i> apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN. to Recommendation 16.
Criminal activity	<i>Criminal activity</i> refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Please refer to the IN to Recommendation 16.
Currency	<i>Currency</i> refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	<p><i>Designated categories of offences</i> means:</p> <ul style="list-style-type: none"> ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods;

Terms	Definitions
	<ul style="list-style-type: none"> ■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. <p>When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.</p>
Designated non-financial businesses and professions	<p><i>Designated non-financial businesses and professions</i> means:</p> <ul style="list-style-type: none"> a) Casinos⁵⁵ b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses,

⁵⁵ References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

Terms	Definitions
	<p>nor to professionals working for government agencies, who may already be subject to AML/CFT measures.</p> <p>f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:</p> <ul style="list-style-type: none"> ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.
<p>Designated person or entity</p>	<p>The term <i>designated person or entity</i> refers to:</p> <ul style="list-style-type: none"> (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution

Terms	Definitions
	<p>1718 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the “<i>Security Council Committee established pursuant to resolution 1718 (2006)</i>” (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and</p> <p>(v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 1737 (2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the “<i>Security Council Committee established pursuant to paragraph 18 of resolution 1737 (2006)</i>” (the 1737 Sanctions Committee) pursuant to resolution 1737 (2006) and its successor resolutions.</p>
Designation	<p>The term <i>designation</i> refers to the identification of a person⁵⁶ or entity that is subject to targeted financial sanctions pursuant to:</p> <ul style="list-style-type: none"> ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and its successor resolutions; ■ Security Council resolution 1737 (2006) and its successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction.
Domestic Wire Transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term <i>ex parte</i> means proceeding without prior notification and participation

⁵⁶ Natural or legal.

Terms	Definitions
	of the affected party.
Express trust	<i>Express trust</i> refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	Please refer to the IN to Recommendation 32.
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	<i>Financial group</i> means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	<p><i>Financial institutions</i> means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:</p> <ol style="list-style-type: none"> 1. Acceptance of deposits and other repayable funds from the public.⁵⁷ 2. Lending.⁵⁸ 3. Financial leasing.⁵⁹ 4. Money or value transfer services.⁶⁰ 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: <ul style="list-style-type: none"> (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);

⁵⁷ This also captures private banking.

⁵⁸ This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

⁵⁹ This does not extend to financial leasing arrangements in relation to consumer products.

⁶⁰ It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	<p>(b) foreign exchange;</p> <p>(c) exchange, interest rate and index instruments;</p> <p>(d) transferable securities;</p> <p>(e) commodity futures trading.</p> <p>8. Participation in securities issues and the provision of financial services related to such issues.</p> <p>9. Individual and collective portfolio management.</p> <p>10. Safekeeping and administration of cash or liquid securities on behalf of other persons.</p> <p>11. Otherwise investing, administering or managing funds or money on behalf of other persons.</p> <p>12. Underwriting and placement of life insurance and other investment related insurance⁶¹.</p> <p>13. Money and currency changing.</p>
Foreign counterparts	<p>Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).</p>
Freeze	<p>In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority.</p> <p>For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court.</p> <p>In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third</p>

⁶¹ This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Terms	Definitions
	<p>parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.</p>
Fundamental principles of domestic law	<p>This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.</p>
Funds	<p>The term <i>funds</i> refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.</p>
Funds or other assets	<p>The term <i>funds or other assets</i> means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.</p>
Identification data	<p>The term <i>identification data</i> refers to reliable, independent source documents, data or information.</p>
Intermediary financial institution	<p>Please refer to the IN to Recommendation 16.</p>
International organisations	<p>International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe,</p>

Terms	Definitions
	institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Legal arrangements	<i>Legal arrangements</i> refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	<i>Legal persons</i> refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a <i>money laundering offence</i> refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	<i>Money or value transfer services (MVTS)</i> refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including <i>hawala</i> , <i>hundi</i> , and <i>fei-chen</i> .
Non-conviction based confiscation	<i>Non-conviction based confiscation</i> means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisations	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through	Please refer to the IN to Recommendation 13.

Terms	Definitions
accounts	
Physical cross-border transportation	Please refer to the IN. to Recommendation 32.
Politically Exposed Persons (PEPs)	<p><i>Foreign PEPs</i> are individuals who are or have been entrusted with prominent public functions by 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.</p> <p><i>Domestic PEPs</i> are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.</p> <p><i>Persons who are or have been entrusted with a prominent function by an international organisation</i> refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.</p> <p>The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p>
Proceeds	<i>Proceeds</i> refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	<i>Property</i> means assets of every kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Please refer to the IN to Recommendation 16.
Reasonable measures	The term <i>Reasonable Measures</i> means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Required	Please refer to the IN to Recommendation 16.
Risk	All references to <i>risk</i> refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.

Terms	Definitions
Satisfied	Where reference is made to a financial institution being <i>satisfied</i> as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term <i>seize</i> means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Please refer to the IN. to Recommendation 16.
Settlor	<i>Settlers</i> are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	<i>Shell bank</i> means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. <i>Physical presence</i> means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word <i>should</i> has the same meaning as <i>must</i> .
Straight-through processing	Please refer to the IN. to Recommendation 16.
Supervisors	<i>Supervisors</i> refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions (“ <i>financial supervisors</i> ” ⁶²) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include

⁶² Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Terms	Definitions
	<p>certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.</p>
Targeted financial sanctions	<p>The term <i>targeted financial sanctions</i> means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.</p>
Terrorist	<p>The term <i>terrorist</i> refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.</p>
Terrorist act	<p>A <i>terrorist act</i> includes:</p> <ul style="list-style-type: none"> (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an 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 organisation to do or to abstain from doing any act.
Terrorist	<p><i>Terrorist financing</i> is the financing of terrorist acts, and of terrorists and terrorist organisations.</p>

Terms	Definitions
financing	
Terrorist financing abuse	Please refer to the IN to Recommendation 8.
Terrorist financing offence	References (except in Recommendation 4) to a <i>terrorist financing offence</i> refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organisation	The term <i>terrorist organisation</i> refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term <i>third parties</i> includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.
Trustee	The terms <i>trust</i> and <i>trustee</i> should be understood as described in and consistent with Article 2 of the <i>Hague Convention on the law applicable to trusts and their recognition</i> ⁶³ . Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family).
Unique transaction	Please refer to the IN. to Recommendation 16.

⁶³ Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

- a) the assets constitute a separate fund and are not a part of the trustee's own estate;*
- b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;*
- c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.*

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

Terms	Definitions
reference number	
Without delay	The phrase <i>without delay</i> means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee or the 1737 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase <i>without delay</i> means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase <i>without delay</i> should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for <i>Combating the financing of terrorism</i>)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IN	Interpretive Note
ML	Money Laundering
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SR.	Special Recommendation
SRB	Self-Regulatory Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

ANNEX I: FATF GUIDANCE DOCUMENTS

Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons (June 1998).

Guidance for Financial Institutions in Detecting Terrorist Financing (April 2002).

International Best Practices: Combating the Abuse of Non-Profit Organisations (October 2002).

International Best Practices: Combating the Abuse of Alternative Remittance Systems (June 2003).

The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (June 2007).

Guidance on the Risk-Based Approach (June 2007 - October 2009). Nine documents including RBA Guidance for:

- the Financial Sector;
- Real Estate Agents;
- Accountants;
- TCSPs;
- Dealers in precious metals and stones;
- Casinos;
- Legal Professionals;
- Money Service Businesses; and
- the Life Insurance Sector.

The Implementation of Activity-Based Financial Prohibitions of United Nations Security Council Resolution 1737 (October 2007).

Capacity Building for Mutual Evaluations and Implementation of the FATF Standards within Low Capacity Countries (February 2008).

Best Practices Paper on Trade Based Money Laundering (June 2008).

The Implementation of Financial Provisions of UN Security Council Resolution 1803 (October 2008).

International Best Practices: Freezing of Terrorist Assets (June 2009).

International Best Practices: Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments (February 2010).

Best Practices Paper on Recommendation 2: Sharing among domestic competent authorities information related to the financing of proliferation (March 2012)

Financial Investigations Guidance (July 2012)

Best Practices: Managing the Anti-Money Laundering and Counter-Terrorist Financing Policy Implications of Voluntary Tax Compliance Programmes (October 2012).

Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery (October 2012).

Revised FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (February 2013).

Guidance on National Risk Assessment (February 2013).

Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services (June 2013).

Guidance on the Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (June 2013).

Guidance on Politically Exposed Persons (Recommendations 12 and 22) (June 2013).

International Best Practices on Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6) (June 2013).

Best Practices Paper: The Use of the FATF Recommendations to Combat Corruption (October 2013).

Guidance on Transparency and Beneficial Ownership (October 2014).

Risk-Based Approach for the Banking Sector (October 2014).

Best Practices on Combating the Abuse of Non-Profit Organisations (June 2015).

Guidance for a Risk-Based Approach to Virtual Currencies (June 2015).

Guidance for a risk-based approach for the effective supervision and enforcement by AML/CFT supervisors of the financial sector and law enforcement (October 2015).

Guidance on AML/CFT-related data and statistics (October 2015)

Guidance for a Risk-Based Approach for Money or Value Transfer Services (February 2016)

ANNEX II: INFORMATION ON UPDATES MADE TO THE FATF RECOMMENDATIONS

The following amendments have been made to the FATF Recommendations since the text was adopted in February 2012.

Date	Type of amendments	Sections subject to amendments
Feb 2013	Alignment of the Standards between R.37 and R.40	<ul style="list-style-type: none"> ■ R.37(d) – page 27 <p>Insertion of the reference that DNFBP secrecy or confidentiality laws should not affect the provision of mutual legal assistance, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.</p>
Oct 2015	Revision of the Interpretive Note to R. 5 to address the foreign terrorist fighters threat	<ul style="list-style-type: none"> ■ INR.5 (B.3) – page 37 <p>Insertion of B.3 to incorporate the relevant element of UNSCR 2178 which addresses the threat posed by foreign terrorist fighters. This clarifies that Recommendation 5 requires countries to criminalise financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.</p> <p>Existing B.3-11 became B.4-12.</p>
Jun 2016	Revision of R. 8 and the Interpretive Note to R. 8	<ul style="list-style-type: none"> ■ R.8 and INR.8 – pages 13 and 54-59 <p>Revision of the standard on non-profit organisation (NPO) to clarify the subset of NPOs which should be made subject to supervision and monitoring. This brings INR.8 into line with the FATF Typologies Report on Risk of Terrorist Abuse of NPOs (June 2014) and the FATF Best Practices on Combatting the Abuse of NPOs (June 2015) which clarify that not all NPOs are high risk and intended to be addressed by R.8, and better align the implementation of R.8/INR.8 with the risk-based approach.</p>

Date	Type of amendments	Sections subject to amendments
Oct 2016	Revision of the Interpretive Note to R. 5 and the Glossary definition of 'Funds or other assets'	■ INR. 5 and Glossary – pages 37 and 121 Revision of the INR.5 to replace “ <i>funds</i> ” with “ <i>funds or other assets</i> ” throughout INR.5, in order to have the same scope as R.6. Revision of the Glossary definition of “ <i>funds or other assets</i> ” by adding references to oil and other natural resources, and to other assets which may potentially be used to obtain funds.

FATF



www.fatf-gafi.org

February 2012

বাংলাদেশ গেজেট



অতিরিক্ত সংখ্যা
কর্তৃপক্ষ কর্তৃক প্রকাশিত

মঙ্গলবার, ফেব্রুয়ারী ২৪, ২০০৯

বাংলাদেশ জাতীয় সংসদ

ঢাকা, ২৪শে ফেব্রুয়ারী, ২০০৯/১২ই ফাল্গুন, ১৪১৫

সংসদ কর্তৃক গৃহীত নিম্নলিখিত আইনটি ২৪শে ফেব্রুয়ারী, ২০০৯ (১২ই ফাল্গুন, ১৪১৫) তারিখে রাষ্ট্রপতির সম্মতি লাভ করিয়াছে এবং এতদ্বারা এই আইনটি সর্বসাধারণের অবগতির জন্য প্রকাশ করা যাইতেছেঃ-

২০০৯ সনের ১৬ নং আইন

কতিপয় সন্ত্রাসী কার্য প্রতিরোধ এবং উহাদের কার্যকর শাস্তির বিধানসহ আনুষঙ্গিক বিষয়াদি
সম্পর্কে বিধান প্রণয়নকল্পে প্রণীত আইন

যেহেতু কতিপয় সন্ত্রাসী কার্য প্রতিরোধ এবং উহাদের কার্যকর শাস্তির বিধানসহ আনুষঙ্গিক বিষয়াদি সম্পর্কে বিধান প্রণয়ন করা সমীচীন ও প্রয়োজনীয়;

সেহেতু নিম্নরূপ আইন করা হইল :-

প্রথম অধ্যায়

প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম, ব্যাপ্তি ও প্রবর্তন।- (১) এই আইন সন্ত্রাস বিরোধী আইন, ২০০৯ নামে অভিহিত হইবে।

(২) সমগ্র বাংলাদেশে ইহার প্রয়োগ হইবে।

(৩) ইহা ১১ জুন ২০০৮ তারিখে কার্যকর হইয়াছে বলিয়া গণ্য হইবে।

২। সংজ্ঞা।- বিষয় বা প্রসঙ্গের পরিপন্থী কোন কিছু না থাকিলে, এই অধ্যাদেশে,-

(১) “অপরাধ” অর্থ এই আইনের অধীন দণ্ডনীয় কোন অপরাধ;

(২) “আগ্নেয়াস্ত্র” অর্থ যে কোন ধরণের পিস্তল, রিভলভার, রাইফেল, বন্দুক বা কামান, এবং অন্য যে কোন আগ্নেয়াস্ত্র ও উহার অন্তর্ভুক্ত হইবে;

(৩) “আদালত” অর্থ দায়রা জজ এর বা, ক্ষেত্রমত, অতিরিক্ত দায়রা জজ এর আদালত;

(৪) “কারাদণ্ড” অর্থ দণ্ডবিধির ধারা ৫৩ তে উল্লিখিত যে কোন বর্ণনার কারাদণ্ড;

(৫) “ফৌজদারী কার্যবিধি” বা “কার্যবিধি” অর্থ Code of Criminal Procedure, 1898 (Act V of 1898);

(৬) “তফসিল” অর্থ এই আইনের তফসিল;

- (৭) “দণ্ডবিধি” অর্থ Penal Code, 1860 (Act XLV of 1860);
- (৮) “দাহ্য পদার্থ” অর্থ এমন কোন পদার্থ যাহাতে আগুন ধরাইবার বা আগুন তীব্রতর করিবার বা ছড়াইবার স্বাভাবিক উচ্চ প্রবণতা রহিয়াছে, যেমন- অকটেন, পেট্রোল, ডিজেল, রূপান্তরিত প্রাকৃতিক গ্যাস (সি.এন.জি), গান পাউডার, এবং অন্য যে কোন দাহ্য পদার্থও উহার অন্তর্ভুক্ত হইবে;
- (৯) “বাংলাদেশ ব্যাংক” অর্থ Bangladesh Bank Order, 1972 (P.O. No. 127 of 1972) এর অধীন প্রতিষ্ঠিত বাংলাদেশ ব্যাংক;
- (১০) “ব্যাংক” অর্থ ব্যাংক কোম্পানী আইন, ১৯৯১ (১৯৯১ সনের ১৪ নং আইন) এর অধীন প্রতিষ্ঠিত কোন ব্যাংক; এবং অন্য কোন আইনের অধীনে ঋণ গ্রহণ, বিতরণ এবং অর্থের বিনিময় করিতে অনুমতিপ্রাপ্ত কোন আর্থিক বা বাণিজ্যিক প্রতিষ্ঠানও ইহার অন্তর্ভুক্ত হইবে;
- (১১) “বিচারক” অর্থ দায়রা জজ, অতিরিক্ত দায়রা জজ বা, ক্ষেত্রমত, সন্ত্রাস বিরোধী বিশেষ ট্রাইব্যুনাল এর বিচারক;
- (১২) “বিশেষ ট্রাইব্যুনাল” অর্থ ধারা ২৮ এর অধীন গঠিত কোন সন্ত্রাস বিরোধী বিশেষ ট্রাইব্যুনাল;
- (১৩) “বিস্ফোরক দ্রব্য” অর্থ—
- (ক) গানপাউডার, নাইট্রো-গ্লিসারিন, ডিনামাইট, গান-কটন, ব্লাসটিং পাউডার, ফুঁসে উঠা (fulminate) পারদ বা অন্য কোন ধাতু, রঙ্গিন আগুন (colored fire) এবং বিস্ফোরণের মাধ্যমে কার্যকর প্রভাব, বা আতসবাজির প্রভাব সৃষ্টির লক্ষ্যে ব্যবহৃত বা উৎপাদিত অন্য যে কোন দ্রব্য যাহা উপরি-উল্লিখিত পদার্থসমূহের সদৃশ হউক বা না হউক; এবং
- (খ) বিস্ফোরক সামগ্রী তৈরীর যে কোন পদার্থ ও কোন বিস্ফোরক পদার্থের মাধ্যমে বা সহযোগে বিস্ফোরণ সৃষ্টি, বা ব্যবহারের অভিপ্রায়ে রূপান্তরিত করিবার, বা সহায়তার জন্য ব্যবহৃত, কোন যন্ত্র, হাতিয়ার, যন্ত্রপাতি বা বস্তুসহ অনুরূপ যন্ত্র, যন্ত্রপাতি বা হাতিয়ারের কোন অংশ এবং ফিউজ, রকেট, পারকাশন ক্যাপস, ডেটোনেটর, কার্টিজ ও যে কোন ধরণের গোলাবারুদও ইহার অন্তর্ভুক্ত হইবে;
- (১৪) “সম্পত্তি” অর্থ বস্তুগত বা অবস্তুগত, স্থাবর বা অস্থাবর, দৃশ্যমান বা অদৃশ্য যে কোন ধরণের সম্পত্তি ও উক্ত সম্পত্তি হইতে উদ্ভূত লাভ, এবং কোন অর্থ বা অর্থে রূপান্তরযোগ্য বিনিময় দলিলও (negotiable instrument) ইহার অন্তর্ভুক্ত হইবে;
- (১৫) “সাক্ষ্য আইন” অর্থ Evidence Act, 1872 (Act I of 1872)।

৩। অন্যান্য শব্দ ও অভিব্যক্তির প্রযোজ্যতা।— (১) এই অধ্যাদেশে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা এই অধ্যাদেশে দেওয়া হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি ফৌজদারী কার্যবিধি বা, ক্ষেত্রমত, দণ্ডবিধিতে যে অর্থে ব্যবহৃত হইয়াছে সেই অর্থে প্রযোজ্য হইবে।

(২) অপরাধ ও শাস্তির দায় দায়িত্ব সংক্রান্ত দণ্ডবিধির সাধারণ বিধানাবলী, যতদূর সম্ভব, এই আইনের অন্যান্য বিধানের সহিত অসঙ্গতিপূর্ণ না হইলে, এই আইনের অধীন অপরাধসমূহের ক্ষেত্রে প্রযোজ্য হইবে।

৪। আইনের প্রাধান্য।— ফৌজদারী কার্যবিধি বা আপাততঃ বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এই আইনের বিধানাবলী কার্যকর থাকিবে।

৫। অতিরিক্তিক প্রয়োগ।— (১) যদি কোন ব্যক্তি বাংলাদেশের বাহিরে বাংলাদেশের কোন নাগরিক বা বাংলাদেশের সম্পদের বিরুদ্ধে কোন অপরাধ সংঘটন করে, যাহা বাংলাদেশে সংঘটিত হইলে এই আইনের অধীন শাস্তিযোগ্য হইত, তাহা হইলে উক্ত অপরাধ বাংলাদেশে সংঘটিত হইয়াছিল বলিয়া গণ্য হইবে এবং উক্ত ব্যক্তি ও অপরাধের ক্ষেত্রে এই আইনের বিধানাবলী প্রযোজ্য হইবে।

(২) যদি কোন ব্যক্তি বাংলাদেশের বাহির হইতে বাংলাদেশের অভ্যন্তরে কোন অপরাধ সংঘটন করে, তাহা হইলে উক্ত অপরাধের সম্পূর্ণ প্রক্রিয়া বাংলাদেশে সংঘটিত হইয়াছিল বলিয়া গণ্য হইবে এবং উক্ত ব্যক্তি ও অপরাধের ক্ষেত্রে এই আইনের বিধানাবলী প্রযোজ্য হইবে।

(৩) যদি কোন ব্যক্তি বাংলাদেশের অভ্যন্তর হইতে বাংলাদেশের বাহিরে কোন অপরাধ সংঘটন করে, তাহা হইলে উক্ত অপরাধ ও উহা সংঘটনের সম্পূর্ণ প্রক্রিয়া বাংলাদেশে সংঘটিত হইয়াছিল বলিয়া গণ্য হইবে এবং উক্ত ব্যক্তি ও অপরাধের ক্ষেত্রে এই আইনের বিধানাবলী প্রযোজ্য হইবে।

দ্বিতীয় অধ্যায়

অপরাধ ও দণ্ড

৬। সন্ত্রাসী কার্য।— (১) কেহ বাংলাদেশের অখন্ডতা, সংহতি, নিরাপত্তা বা সার্বভৌমত্ব বিপন্ন করিবার জন্য জনসাধারণ বা জনসাধারণের কোন অংশের মধ্যে আতংক সৃষ্টির মাধ্যমে সরকার বা অন্য কোন ব্যক্তিকে কোন কার্য করিতে বা করা হইতে বিরত রাখিতে বাধ্য করিবার উদ্দেশ্যে—

(ক) কোন ব্যক্তিকে হত্যা, গুরুতর আঘাত, আটক বা অপহরণ করিলে, বা কোন ব্যক্তির কোন সম্পত্তির ক্ষতিসাধন করিলে; অথবা

(খ) দফা (ক) এর উদ্দেশ্য সাধনকল্পে কোন বিস্ফোরক দ্রব্য, দাহ্য বস্তু, আগ্নেয়াস্ত্র বা অন্য কোন প্রকার রাসায়নিক দ্রব্য ব্যবহার করিলে বা নিজ দখলে রাখিলে;

তিনি “সন্ত্রাসী কার্য” সংঘটনের অপরাধ করিবেন।

(২) কেহ সন্ত্রাসী কার্য সংঘটন করিয়া থাকিলে, তিনি মৃত্যুদণ্ড বা যাবজ্জীবন কারাদণ্ড বা অনূর্ধ্ব বিশ বৎসর এবং অন্যান্য তিন বৎসর পর্যন্ত যে কোন মেয়াদের সশ্রম কারাদণ্ডে দণ্ডিত হইবেন, এবং ইহার অতিরিক্ত অর্ধদণ্ডও আরোপ করা যাইবে।

৭। সন্ত্রাসী কার্যে অর্থ যোগান সংক্রান্ত অপরাধ।— (১) যদি কোন ব্যক্তি অন্য কোন ব্যক্তিকে অর্থ, সেবা বা অন্য কোন সম্পত্তি সরবরাহ করেন বা সরবরাহ করিতে প্ররোচিত করেন এবং কোন সন্ত্রাসী কার্যের উদ্দেশ্যে উহা ব্যবহারের ইচ্ছা পোষণ করেন, বা ইহা সন্দেহ করিবার যুক্তিসঙ্গত কারণ থাকে যে, উহা সন্ত্রাসী কার্যে ব্যবহার করা হইবে বা হইতে পারে, তাহা হইলে তিনি সন্ত্রাসী কর্মকাণ্ডে অর্থ যোগানের অপরাধ সংঘটন করিবেন।

(২) যদি কোন ব্যক্তি অর্থ, সেবা বা অন্য কোন সম্পত্তি গ্রহণ করেন এবং কোন সন্ত্রাসী কার্যের উদ্দেশ্যে ব্যবহারের ইচ্ছা পোষণ করেন, বা ইহা সন্দেহ করিবার যুক্তিসঙ্গত কারণ থাকে যে, উহা সন্ত্রাসী কার্যে ব্যবহার করা হইবে বা হইতে পারে, তাহা হইলে তিনি সন্ত্রাসী কর্মকাণ্ডে অর্থ যোগানের অপরাধ সংঘটন করিবেন।

(৩) যদি কোন ব্যক্তি অর্থ, সেবা বা অন্য সম্পত্তির ব্যবস্থা করেন এবং কোন সন্ত্রাসী কার্যের উদ্দেশ্যে উহা ব্যবহারের ইচ্ছা পোষণ করেন, বা সন্দেহ করিবার যুক্তিসঙ্গত কারণ থাকে যে, উহা সন্ত্রাসী কার্যে ব্যবহার করা হইবে বা হইতে পারে, তাহা হইলে তিনি সন্ত্রাসী কর্মকাণ্ডে অর্থ যোগানের অপরাধ সংঘটন করিবেন।

(৪) উপ-ধারা (১) হইতে (৩) এ বর্ণিত অপরাধে কোন ব্যক্তি দোষী সাব্যস্ত হইলে, উক্ত ব্যক্তি অনধিক বিশ বৎসর ও অন্যান্য তিন বৎসর পর্যন্ত যে কোন মেয়াদের কারাদণ্ডে দণ্ডিত হইবেন, এবং ইহার অতিরিক্ত অর্ধদণ্ডও আরোপ করা যাইবে।

৮। নিষিদ্ধ সংগঠনের সদস্যপদ।— যদি কোন ব্যক্তি ধারা ১৮ এর অধীন কোন নিষিদ্ধ সংগঠনের সদস্য হন বা সদস্য বলিয়া দাবী করেন, তাহা হইলে তিনি অপরাধ সংঘটন করিবেন এবং উক্তরূপ অপরাধ সংঘটনের জন্য তিনি অনধিক ছয় মাস পর্যন্ত যে কোন মেয়াদের কারাদণ্ড, অথবা অর্ধদণ্ড, অথবা উভয় দণ্ডে দণ্ডিত হইবেন।

৯। নিষিদ্ধ সংগঠনের সমর্থন।— (১) যদি কোন ব্যক্তি ধারা ১৮ এর অধীন কোন নিষিদ্ধ সংগঠনকে সমর্থন করিবার উদ্দেশ্যে কাহাকেও অনুরোধ বা আহ্বান করেন, অথবা নিষিদ্ধ সংগঠনকে সমর্থন বা উহার কর্মকাণ্ডকে গতিশীল ও উৎসাহিত করিবার উদ্দেশ্যে কোন সভা আয়োজন, পরিচালনা বা পরিচালনায় সহায়তা করেন, অথবা বক্তৃতা প্রদান করেন, তাহা হইলে তিনি অপরাধ সংঘটন করিবেন।

(২) যদি কোন ব্যক্তি কোন নিষিদ্ধ সংগঠনের জন্য সমর্থন চাহিয়া অথবা উহার কর্মকাণ্ডকে সক্রিয় করিবার উদ্দেশ্যে কোন সভায় বক্তৃতা করেন অথবা রেডিও, টেলিভিশন অথবা কোন মুদ্রণ বা ইলেকট্রনিক মাধ্যমে কোন তথ্য সম্প্রচার করেন, তাহা হইলে তিনি অপরাধ সংঘটন করিবেন।

(৩) যদি কোন ব্যক্তি উপ-ধারা (১) অথবা (২) এর অধীন কোন অপরাধে দোষী সাব্যস্ত হন, তাহা হইলে তিনি অনধিক সাত বৎসর ও অনূন্য দুই বৎসর পর্যন্ত যে কোন মেয়াদের কারাদণ্ডে দণ্ডিত হইবেন এবং ইহার অতিরিক্ত অর্থদণ্ডও আরোপ করা যাইবে।

১০। অপরাধ সংঘটনের ষড়যন্ত্রের (criminal conspiracy) শাস্তি।—যদি কোন ব্যক্তি এই আইনের অধীন অপরাধ সংঘটনের ষড়যন্ত্র করেন, তাহা হইলে তিনি উক্ত অপরাধের জন্য নির্ধারিত সর্বোচ্চ শাস্তির দুই তৃতীয়াংশ মেয়াদের যে কোন কারাদণ্ডে, অথবা অর্থদণ্ডে, অথবা উভয় দণ্ডে দণ্ডিত হইবেন; এবং যদি উক্ত অপরাধের জন্য নির্ধারিত শাস্তি মৃত্যুদণ্ড হয়, তাহা হইলে অপরাধের শাস্তি যাবজ্জীবন কারাদণ্ড অথবা অনূর্ধ্ব চৌদ্দ বৎসরের কারাদণ্ড হইবে, কিন্তু উহা পাঁচ বৎসরের কম হইবে না।

১১। অপরাধ সংঘটনের প্রচেষ্টার (attempt) শাস্তি।— যদি কোন ব্যক্তি এই আইনের অধীন অপরাধ সংঘটনের চেষ্টা করেন, তাহা হইলে তিনি উক্ত অপরাধের জন্য নির্ধারিত সর্বোচ্চ শাস্তির দুই তৃতীয়াংশ মেয়াদের যে কোন কারাদণ্ডে, অথবা অর্থদণ্ডে, অথবা উভয় দণ্ডে দণ্ডিত হইবেন; এবং যদি উক্ত অপরাধের জন্য নির্ধারিত শাস্তি মৃত্যুদণ্ড হয়, তাহা হইলে অপরাধের শাস্তি যাবজ্জীবন কারাদণ্ড অথবা অনূর্ধ্ব চৌদ্দ বৎসরের কারাদণ্ড হইবে, কিন্তু উহা পাঁচ বৎসরের কম হইবে না।

১২। অপরাধে সহায়তার (abetment) শাস্তি।— যদি কোন ব্যক্তি এই আইনের অধীন শাস্তিযোগ্য কোন অপরাধ সংঘটনের সহায়তা করেন, তাহা হইলে তিনি উক্ত অপরাধের জন্য নির্ধারিত দণ্ডে দণ্ডিত হইবেন।

১৩। সন্ত্রাসী কর্মকাণ্ড প্ররোচিত (instigation) করিবার শাস্তি।— যদি কোন ব্যক্তি তাহার স্বৈচ্ছাধীন কর্মকাণ্ড অথবা অংশ গ্রহণের মাধ্যমে কোন দলিল প্রস্তুত বা বিতরণ করেন, অথবা কোন মুদ্রণ বা ইলেকট্রনিক মাধ্যমে কোন তথ্য সম্প্রচার করিয়া, অথবা কোন সরঞ্জাম, সহায়তা বা প্রযুক্তি বা প্রশিক্ষণ প্রদানের মাধ্যমে কোন ব্যক্তি বা সংগঠনকে এইরূপ অবগত থাকিয়া সহায়তা প্রদান করেন যে, উক্ত দলিল, সরঞ্জাম, সহায়তা বা প্রযুক্তি বা প্রশিক্ষণ এই আইনের অধীন কোন অপরাধ সংঘটনের কাজে ব্যবহৃত হইবে বা উক্ত ব্যক্তি বা সংগঠন উহাদের অনুরূপ অপরাধ সংঘটনের প্রচেষ্টায় ব্যবহার করিবে, তাহা হইলে তিনি সন্ত্রাসী কর্মকাণ্ড প্ররোচিত করিয়াছেন বলিয়া গণ্য হইবেন; এবং সংশ্লিষ্ট অপরাধের জন্য নির্ধারিত সর্বোচ্চ শাস্তির দুই তৃতীয়াংশ মেয়াদের কারাদণ্ডে, অথবা অর্থদণ্ডে, অথবা উভয় দণ্ডে তাহাকে দণ্ডিত করা যাইবে; এবং যদি উক্ত অপরাধের জন্য নির্ধারিত শাস্তি মৃত্যুদণ্ড হয়, তাহা হইলে অপরাধের শাস্তি যাবজ্জীবন কারাদণ্ড অথবা অনূর্ধ্ব চৌদ্দ বৎসরের কারাদণ্ড হইবে, কিন্তু উহা পাঁচ বৎসরের কম হইবে না।

১৪। অপরাধীকে আশ্রয়প্রদান।— (১) যদি কোন ব্যক্তি, অন্য কোন ব্যক্তি এই আইনের অধীন অপরাধ সংঘটন করিয়াছেন জানিয়াও বা উক্ত ব্যক্তি অপরাধী ইহা বিশ্বাস করিবার যুক্তিসঙ্গত কারণ থাকা সত্ত্বেও, শাস্তি হইতে রক্ষা করিবার অভিপ্রায়ে উক্ত ব্যক্তিকে আশ্রয়দান করেন বা লুকাইয়া রাখেন তাহা হইলে তিনি—

(ক) উক্ত অপরাধের শাস্তি মৃত্যুদণ্ড হইলে অনধিক পাঁচ বৎসরের কারাদণ্ডে দণ্ডিত হইবেন, এবং ইহার অতিরিক্ত অর্থদণ্ডও আরোপ করা যাইবে; অথবা

(খ) উক্ত অপরাধের শাস্তি যাবজ্জীবন কারাদণ্ড বা যে কোন মেয়াদের কারাদণ্ড হইলে, অনধিক তিন বৎসরের কারাদণ্ডে দণ্ডিত হইবেন; এবং ইহার অতিরিক্ত অর্থদণ্ডও আরোপ করা যাইবে।

(২) উপ-ধারা (১) এর অধীন আশ্রয়দান বা লুকাইয়া রাখিবার অপরাধ স্বামী, স্ত্রী, পুত্র, কন্যা, পিতা বা মাতা কর্তৃক হইলে, এই ধারার বিধান প্রযোজ্য হইবে না।

তৃতীয় অধ্যায়

বাংলাদেশ ব্যাংকের ক্ষমতা

১৫। বাংলাদেশ ব্যাংকের ক্ষমতা।— (১) বাংলাদেশ ব্যাংক এই আইনের অধীন কোন অপরাধ সংঘটনের উদ্দেশ্যে কোন ব্যাংকিং চ্যানেলের মাধ্যমে লেনদেন প্রতিরোধ ও সনাক্ত করিতে প্রয়োজনীয় পদক্ষেপ গ্রহণ করিতে পারিবে এবং এতদুদ্দেশ্যে উহার নিম্নবর্ণিত ক্ষমতা ও কর্তৃত্ব থাকিবে—

(ক) কোন ব্যাংক হইতে সন্দেহজনক লেনদেনে সম্পর্কিত প্রতিবেদন তলব এবং অনুরূপ প্রতিবেদন, আইনের অধীনে প্রকাশের অনুমোদন না থাকিলে, গোপন রাখা;

- (খ) সকল পরিসংখ্যান ও রেকর্ড সংকলন ও সংরক্ষণ করা;
- (গ) সকল সন্দেহজনক লেনদেন সম্পর্কিত রিপোর্টের ডাটা-বেজ সৃষ্টি ও রক্ষণাবেক্ষণ করা;
- (ঘ) সন্দেহজনক লেনদেন সম্পর্কিত প্রতিবেদন বিশ্লেষণ করা;
- (ঙ) কোন লেনদেন সন্ধানী কার্যের সহিত সম্পৃক্ত মর্মে সন্দেহ করিবার যুক্তিসঙ্গত কারণ থাকিলে সংশ্লিষ্ট ব্যাংককে উক্ত লেনদেনের হিসাব ত্রিশ দিনের জন্য বন্ধ রাখিবার উদ্দেশ্যে লিখিত আদেশ জারী করা এবং এইরূপে জারীকৃত আদেশ অতিরিক্ত ত্রিশ দিনের জন্য বর্ধিত করা;
- (চ) ব্যাংকের কার্যাবলী পরিবীক্ষণ ও তদারক করা;
- (ছ) সন্ধানী কার্যে অর্থ যোগান প্রতিহত করিবার উদ্দেশ্যে প্রতিরোধমূলক পদক্ষেপ গ্রহণে ব্যাংকসমূহের নিকট নির্দেশনা জারী করা;
- (জ) সন্ধানী কার্যের সহিত জড়িত সন্দেহজনক লেনদেন সনাক্তের উদ্দেশ্যে ব্যাংকসমূহ পরিদর্শন করা; এবং
- (ঝ) সন্ধানী কার্যে অর্থযোগানের সহিত জড়িত সন্দেহজনক লেনদেন সনাক্ত ও প্রতিরোধের উদ্দেশ্যে ব্যাংকের কর্মকর্তা ও কর্মচারীগণকে প্রশিক্ষণ প্রদান করা।

(২) বাংলাদেশ ব্যাংক, সন্ধানী কার্যে অর্থযোগানের সহিত জড়িত সন্দেহজনক কোন লেনদেনের বিষয় কোন ব্যাংক বা ইহার গ্রাহককে সনাক্ত করিবার সঙ্গে সঙ্গে, উহা যথাযথ আইন প্রয়োগকারী সংস্থাকে অবহিত করিবে এবং অনুসন্ধান ও তদন্ত কার্যে উক্ত আইন প্রয়োগকারী সংস্থাকে প্রয়োজনীয় সকল প্রকার সহযোগিতা প্রদান করিবে।

(৩) সংশ্লিষ্ট ব্যাংকের প্রধান নির্বাহী কর্মকর্তার সম্মতি কিংবা বাংলাদেশ ব্যাংকের অনুমোদন ব্যতিরেকে কোন ব্যাংকের কোন দলিল বা নথিতে কোন আইন প্রয়োগকারী সংস্থার প্রবেশাধিকার থাকিবে না।

১৬। ব্যাংকের দায়িত্ব।- (১) কোন ব্যাংকিং চ্যানেলের মাধ্যমে এই আইনের অধীন কোন অপরাধের সহিত জড়িত অর্থ লেনদেন প্রতিরোধ ও সনাক্ত করিবার লক্ষ্যে প্রত্যেক ব্যাংক যথাযথ সতর্কতা ও দায়িত্বশীলতার সহিত প্রয়োজনীয় ব্যবস্থা গ্রহণ করিবে।

(২) প্রত্যেক ব্যাংকের পরিচালনা পরিষদ (Board of Directors) উহার কর্মকর্তাদের দায়িত্ব সম্পর্কিত নির্দেশনা অনুমোদন ও জারী করিবে, এবং ধারা ১৫ এর অধীন বাংলাদেশ ব্যাংক কর্তৃক জারীকৃত নির্দেশনা, যাহা ব্যাংকসমূহের জন্য প্রযোজ্য, প্রতিপালন করা হইতেছে কিনা উহা নিশ্চিত করিবে।

(৩) কোন ব্যাংক ধারা ১৫ এর অধীন বাংলাদেশ ব্যাংক কর্তৃক জারীকৃত নির্দেশনা পালন করিতে ব্যর্থ হইলে, উক্ত ব্যাংক বাংলাদেশ ব্যাংক কর্তৃক নির্ধারিত ও নির্দেশিত অনধিক দশ লক্ষ টাকা জরিমানা পরিশোধ করিতে বাধ্য থাকিবে।

চতুর্থ অধ্যায়

সন্ধানী সংগঠন

১৭। সন্ধানী কার্যের সহিত জড়িত সংগঠন।- এই আইনের উদ্দেশ্য পূরণকল্পে, কোন সংগঠন সন্ধানী কার্যের সহিত জড়িত বলিয়া গণ্য হইবে, যদি উহা-

- (ক) সন্ধানী কার্য সংঘটিত করে বা উক্ত কার্যে অংশ গ্রহণ করে;
- (খ) সন্ধানী কার্যের জন্য প্রস্তুতি গ্রহণ করে;
- (গ) সন্ধানী কার্য সংঘটনে সাহায্য করে বা উৎসাহ প্রদান করে;
- (ঘ) সন্ধানী কার্যের সহিত জড়িত কোন সংগঠনকে সমর্থন এবং সহায়তা প্রদান করে; অথবা
- (ঙ) অন্য কোনভাবে সন্ধানী কার্যের সহিত জড়িত থাকে।

১৮। সংগঠন নিষিদ্ধকরণ।- (১) এই আইনের উদ্দেশ্য পূরণকল্পে, সরকার কোন সংগঠনকে সন্ধানী কার্যের সহিত জড়িত রহিয়াছে মর্মে যুক্তিসঙ্গত কারণের ভিত্তিতে, আদেশ দ্বারা, তফসিলে তালিকাভুক্ত করিয়া, নিষিদ্ধ করিতে পারিবে।

(২) সরকার, আদেশ দ্বারা, যে কোন সংগঠনকে তফসিলে সংযোজন বা তফসিল হইতে বাদ দিতে অথবা অন্য কোনভাবে তফসিল সংশোধন করিতে পারিবে।

১৯। পুনঃপরীক্ষা (Review)।- (১) ধারা ১৮ এর অধীন সরকার কর্তৃক প্রদত্ত আদেশ দ্বারা সংক্ষুব্ধ সংগঠন, আদেশ প্রদানের তারিখ হইতে ত্রিশ দিনের মধ্যে, উহার বিরুদ্ধে লিখিতভাবে, যুক্তি উপস্থাপনপূর্বক, সরকারের নিকট পুনঃনিরীক্ষার জন্য আবেদন করিতে পারিবে এবং সরকার, আবেদনকারীর শুনানী গ্রহণপূর্বক, আবেদন প্রাপ্তির তারিখ হইতে নব্বই দিবসের মধ্যে উহা নিষ্পন্ন করিবে।

(২) উপ-ধারা (১) এর অধীন পুনঃনিরীক্ষার আবেদন নামঞ্জুর করা হইলে, উক্ত সংক্ষুব্ধ সংগঠন আবেদন নামঞ্জুর হইবার তারিখ হইতে ত্রিশ দিনের মধ্যে হাইকোর্ট বিভাগে আপীল দায়ের করিতে পারিবে।

(৩) সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, উপ-ধারা (১) এর অধীন দায়েরকৃত পুনঃনিরীক্ষার দরখাস্তসমূহ নিষ্পত্তির জন্য একটি তিন সদস্য বিশিষ্ট পুনঃনিরীক্ষা কমিটি (Review Committee) গঠন করিবে।

২০। নিষিদ্ধ সংগঠনের বিরুদ্ধে ব্যবস্থা গ্রহণ।- (১) কোন সংগঠনকে নিষিদ্ধ করা হইলে সরকার, এই অধ্যাদেশে বর্ণিত অন্যান্য ব্যবস্থা গ্রহণ ছাড়াও, নিম্নবর্ণিত পদক্ষেপ গ্রহণ করিবে, যথা :-

- (ক) উহার কার্যালয়, যদি থাকে, বন্ধ করিয়া দিবে;
- (খ) উহার ব্যাংক হিসাব, যদি থাকে, অবরুদ্ধ (freeze) করিবে এবং অন্যান্য হিসাব আটক করিবে;
- (গ) সকল প্রকারের প্রচারপত্র, পোস্টার, ব্যানার, অথবা মুদ্রিত, ইলেকট্রনিক, ডিজিটাল বা অন্যান্য উপকরণ বাজেয়াপ্ত করিবে; এবং
- (ঘ) নিষিদ্ধ সংগঠন বা উহার পক্ষে বা সমর্থনে যে কোন প্রেস বিবৃতির প্রকাশনা, মুদ্রণ বা প্রচারণা, সংবাদ সম্মেলন বা জনসম্মুখে বক্তৃতা প্রদান নিষিদ্ধ করিবে।

(২) নিষিদ্ধ সংগঠন উহার আয় ও ব্যয়ের হিসাব পেশ করিবে এবং এতদুদ্দেশ্যে সরকার কর্তৃক মনোনীত উপযুক্ত কর্তৃপক্ষের নিকট আয়ের সকল উৎস প্রকাশ করিবে।

(৩) যদি দেখা যায় যে নিষিদ্ধ সংগঠনের তহবিল এবং পরিসম্পদ (asset) অবৈধভাবে অর্জিত হইয়াছে অথবা এই আইনের অধীন কোন অপরাধ সংঘটনে ব্যবহৃত হইয়াছে, তাহা হইলে উক্ত তহবিল এবং পরিসম্পদ রাষ্ট্রের অনুকূলে বাজেয়াপ্ত হইবে।

পঞ্চম অধ্যায়

অপরাধের তদন্ত

২১। পুলিশ কর্তৃক সাক্ষীকে পরীক্ষা সম্পর্কিত বিশেষ বিধান।- (১) যদি কোন পুলিশ কর্মকর্তা এই আইনের অধীনে কোন মামলার তদন্তকালে ঘটনা এবং পরিস্থিতি সম্পর্কে অবহিত এইরূপ কোন ব্যক্তিকে জিজ্ঞাসাবাদ করিবার প্রয়োজন মনে করেন এবং, যদি উক্ত ব্যক্তি ঘটনার বিবরণ লিখিতভাবে প্রদান করিতে যথেষ্ট সক্ষম মর্মে পুলিশ কর্মকর্তার জানা থাকে বা বিশ্বাস করিবার কারণ থাকে, তাহা হইলে উক্ত পুলিশ কর্মকর্তা, উক্ত ব্যক্তির সম্মতিতে, ঘটনার বিবরণ উক্ত ব্যক্তির নিকট হইতে লিখিতভাবে গ্রহণ করিতে পারিবেন।

(২) উক্ত ব্যক্তি তাহার বক্তব্য বা ঘটনার বিবরণ স্বহস্তে কলম দ্বারা লিপিবদ্ধ ও স্বাক্ষর করিবেন।

২২। ম্যাজিস্ট্রেট কর্তৃক সাক্ষীর বিবৃতি রেকর্ড সম্পর্কিত বিশেষ বিধান।- যে কোন মেট্রোপলিটন ম্যাজিস্ট্রেট, প্রথম শ্রেণীর ম্যাজিস্ট্রেট, অথবা এতদুদ্দেশ্যে বিশেষভাবে ক্ষমতাপ্রাপ্ত দ্বিতীয় শ্রেণীর ম্যাজিস্ট্রেট যদি অবগত থাকেন বা তাহার বিশ্বাস করিবার যুক্তি সংগত কারণ থাকে যে, মামলার ঘটনা ও পরিস্থিতি সম্পর্কে অবহিত কোন ব্যক্তি তাহার বিবৃতি লিখিতভাবে প্রদান করিতে যথেষ্ট সমর্থ, তাহা হইলে তিনি উক্ত ব্যক্তিকে তাহার বিবৃতি কলম দ্বারা স্বহস্তে লিখিতভাবে প্রদান করিতে নির্দেশ প্রদান করিতে পারিবেন।

২৩। অভিযুক্ত ব্যক্তির স্বীকারোক্তি রেকর্ড সম্পর্কিত বিশেষ বিধান।- যে কোন মেট্রোপলিটন ম্যাজিস্ট্রেট, প্রথম শ্রেণীর ম্যাজিস্ট্রেট, অথবা এতদুদ্দেশ্যে বিশেষভাবে ক্ষমতাপ্রাপ্ত দ্বিতীয় শ্রেণীর ম্যাজিস্ট্রেট অভিযুক্ত ব্যক্তি কর্তৃক স্বীকারোক্তিমূলক কোন বক্তব্য রেকর্ডকালে, যদি উক্ত ব্যক্তি ঘটনা সম্পর্কে লিখিতভাবে বিবৃতি প্রদান করিতে সক্ষম ও আগ্রহী হন, তাহা হইলে উক্ত ব্যক্তিকে তাহার স্বীকারোক্তিমূলক বক্তব্য স্বহস্তে কলম দ্বারা লিপিবদ্ধ করিতে অনুমতি প্রদান করিবেন।

২৪। তদন্তের সময়সীমা।-- (১) কোন পুলিশ কর্মকর্তা এই আইনের অধীন কোন মামলার তদন্ত কার্যবিধির ধারা ১৫৪ এর অধীন তথ্য প্রাপ্তি অথবা লিপিবদ্ধ করিবার তারিখ হইতে ত্রিশ দিনের মধ্যে সম্পন্ন করিবেন।

(২) যদি কোন পুলিশ কর্মকর্তা উপ-ধারা (১) এ উল্লিখিত সময়ের মধ্যে তদন্ত সম্পন্ন করিতে না পারেন, তাহা হইলে, মামলার ডায়রীতে লিখিতভাবে কারণ লিপিবদ্ধ করিয়া অনধিক পনের দিন সময় বৃদ্ধি করিতে পারিবেন।

(৩) যদি উক্ত পুলিশ কর্মকর্তা উপ-ধারা (২) এ উল্লিখিত সময়ের মধ্যে তদন্ত সম্পন্ন করিতে না পারেন, তাহা হইলে উক্ত তদন্তকারী কর্মকর্তা সংশ্লিষ্ট জেলার পুলিশ সুপারিনটেনডেন্টের অথবা, ক্ষেত্রমত, মেট্রোপলিটন এলাকায় সংশ্লিষ্ট ডেপুটি পুলিশ কমিশনারের লিখিত অনুমোদনক্রমে, অতিরিক্ত অনধিক ত্রিশদিন সময় বৃদ্ধি করিতে পারিবে।

(৪) যদি উক্ত পুলিশ কর্মকর্তা উপ-ধারা (৩) এ উল্লিখিত অতিরিক্ত বর্ধিত সময়ের মধ্যে তদন্ত সম্পন্ন করিতে না পারেন, তাহা হইলে তিনি অবিলম্বে কারণ উল্লেখপূর্বক সংশ্লিষ্ট জেলার পুলিশ সুপারিনটেনডেন্টকে অথবা, ক্ষেত্রমত, মেট্রোপলিটন এলাকায় সংশ্লিষ্ট ডেপুটি পুলিশ কমিশনারকে কারণ উল্লেখপূর্বক ঘটনা সম্পর্কে অবহিত করিবেন, এবং উল্লিখিত কারণ সন্তোষজনক না হইলে তাহার বিরুদ্ধে বিভাগীয় শাস্তিমূলক ব্যবস্থা গ্রহণ করা হইবে।

২৫। কতিপয় মামলার তদন্তের ক্ষেত্রে সময়সীমা বৃদ্ধি।-- (১) ধারা ২৫ এর উপ-ধারা (৩) এ নির্ধারিত অতিরিক্ত সময়সীমার মধ্যে এজাহার (FIR) এ উল্লিখিত অপরাধীর পরিচয় অনুদঘাটিত থাকায় এবং উক্ত অপরাধীকে সনাক্তকরণের অসমর্থতার কারণে কোন পুলিশ কর্মকর্তা তদন্তকার্য সম্পন্ন করিতে ব্যর্থ হইলে, ধারা ২৫ এ উল্লিখিত অতিরিক্ত বর্ধিত সময়সীমার পরবর্তীতে যে কোন সময় কোন পুলিশ রিপোর্ট অথবা নূতনভাবে পুলিশ রিপোর্ট অথবা অতিরিক্ত পুলিশ রিপোর্ট প্রদানের ক্ষেত্রে উহা বাধা বলিয়া গণ্য হইবে না।

(২) যদি কোন পুলিশ কর্মকর্তা অপরাধ সংশ্লিষ্ট সাক্ষ্য বা কোন রিপোর্ট সরবরাহ করিবার জন্য ধারা ২৫ এর উপ-ধারা (৩) এর অধীন অতিরিক্ত বর্ধিত সময় সীমার মধ্যে মেডিকেল, ফরেনসিক, আঙ্গুলের ছাপ, রাসায়নিক বা অন্য কোন বিশেষজ্ঞ সাক্ষীর, যাহার উপর তাহার নিয়ন্ত্রণ নাই এবং যাহা ব্যতীত মামলা সম্পর্কে কোন কার্যকর রিপোর্ট তৈরি করা সম্ভব হয় না, অসমর্থতার কারণে তদন্তকার্য সম্পন্ন করিতে ব্যর্থ হন, তাহা হইলে উক্ত উল্লিখিত অতিরিক্ত বর্ধিত সময়সীমার পরবর্তী যে কোন সময় পুলিশ রিপোর্ট পেশ করিতে উহা বাধা বলিয়া গণ্য হইবে না।

২৬। পুনঃসমর্পণ (Remand)।--(১) যেক্ষেত্রে কোন ব্যক্তিকে গ্রেপ্তার করা হয় এবং তদন্তের জন্য আটক রাখা হয়, সেইক্ষেত্রে তদন্ত কর্মকর্তা অভিযুক্ত ব্যক্তিকে পুলিশের হেফাজতে পুনঃসমর্পণের জন্য উপযুক্ত ম্যাজিস্ট্রেটের নিকট আবেদন করিতে পারিবেন।

(২) উপ-ধারা (১) এর অধীন আবেদন বিবেচনাক্রমে ম্যাজিস্ট্রেট অভিযুক্তকে পুলিশের হেফাজতে পুনঃসমর্পণ করিতে পারিবেন, এবং এইরূপ পুনঃসমর্পণের মেয়াদ একাদিক্রমে বা সর্বমোট দশ দিনের অধিক হইবে না :

তবে শর্ত থাকে যে, যদি তদন্তকারী কর্মকর্তা ম্যাজিস্ট্রেটের নিকট ইহা সন্তোষজনকভাবে প্রমাণ করিতে সমর্থ হন যে, অভিযুক্ত ব্যক্তিকে অধিকতর মেয়াদের জন্য পুনঃসমর্পণ করা হইলে অতিরিক্ত সাক্ষ্য পাওয়া যাইতে পারে, তাহা হইলে ম্যাজিস্ট্রেট অনধিক পাঁচ দিন পর্যন্ত পুনঃসমর্পণের মেয়াদ বৃদ্ধি করিতে পারিবেন।

ষষ্ঠ অধ্যায়

দায়রা জজ কর্তৃক বিচার

২৭। দায়রা জজ বা অতিরিক্ত দায়রা জজ কর্তৃক অপরাধের বিচার সম্পর্কিত বিধান।-- (১) ফৌজদারী কার্যবিধি অথবা আপাততঃ বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এতদুদ্দেশ্যে বিশেষ ট্রাইব্যুনাল গঠিত না হওয়া পর্যন্ত এই আইনের অধীন অপরাধসমূহ দায়রা জজ কর্তৃক বা, দায়রা জজ কর্তৃক অতিরিক্ত দায়রা জজের নিকট স্থানান্তরিত হইবার ক্ষেত্রে, অতিরিক্ত দায়রা জজ কর্তৃক, বিচার্য হইবে।

(২) দায়রা জজ বা অতিরিক্ত দায়রা জজ এই আইনের অধীন অপরাধ বিচারের সময় দায়রা আদালতে বিচারের ক্ষেত্রে প্রযোজ্য ফৌজদারী কার্যবিধির অধ্যায় ২৩ এ বর্ণিত পদ্ধতি অনুসরণ করিবেন।

(৩) এই অধ্যায়ের উদ্দেশ্য পূরণকল্পে, এই আইনের অধীন অপরাধসমূহ দায়রা আদালত কর্তৃক বিচার্য বলিয়া গণ্য হইবে, এবং যে দায়রা ডিভিশনের অধিক্ষেত্রে উক্ত অপরাধ বা উহার অংশবিশেষ সংঘটিত হইয়াছে, উক্ত অধিক্ষেত্রের দায়রা জজের নিকট অপরাধের কার্যধারা রুজু করা যাইবে।

সপ্তম অধ্যায়

বিশেষ ট্রাইব্যুনাল কর্তৃক বিচার

২৮। সন্ত্রাস বিরোধী বিশেষ ট্রাইব্যুনাল গঠন।-- (১) সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের অধীন সংঘটিত অপরাধের দ্রুত ও কার্যকর বিচারের উদ্দেশ্যে, এক বা একাধিক সন্ত্রাস বিরোধী বিশেষ ট্রাইব্যুনাল গঠন করিতে পারিবে।

(২) উপ-ধারা (১) এর অধীন গঠিত বিশেষ ট্রাইব্যুনাল, সুপ্রীম কোর্টের সহিত পরামর্শক্রমে সরকার কর্তৃক নিযুক্ত একজন দায়রা জজ অথবা একজন অতিরিক্ত দায়রা জজের সমন্বয়ে গঠিত হইবে; এবং অনুরূপভাবে নিযুক্ত একজন বিচারক “বিচারক, সন্ত্রাস বিরোধী বিশেষ ট্রাইব্যুনাল” নামে অভিহিত হইবেন।

(৩) এই ধারার অধীন গঠিত কোন বিশেষ ট্রাইব্যুনালকে সমগ্র বাংলাদেশের স্থানীয় অধিক্ষেত্র অথবা এক বা একাধিক দায়রা ডিভিশনের অধিক্ষেত্র প্রদান করা যাইতে পারে; এবং উক্ত ট্রাইব্যুনাল কেবল এই আইনের অধীন অপরাধের মামলার বিচার করিবে, যাহা উক্ত ট্রাইব্যুনালে দায়ের বা স্থানান্তরিত হইবে।

(৪) সরকার কর্তৃক কোন বিশেষ ট্রাইব্যুনালকে সমগ্র বাংলাদেশের অথবা এক বা একাধিক দায়রা ডিভিশনের সমন্বয়ে গঠিত উহার অংশ বিশেষের, স্থানীয় অধিক্ষেত্র ন্যস্ত করিবার কারণে একজন দায়রা জজ বা অতিরিক্ত দায়রা জজ কর্তৃক এই আইনের অধীন অপরাধের বিচারের এখতিয়ার ক্ষুণ্ণ হইবে না, এবং সরকার কর্তৃক, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, অনুরূপ কোন আদেশ প্রদান না করা হইলে দায়রা আদালতে নিষ্পত্তাধীন এই আইনের অধীন অপরাধের কোন মামলা বিশেষ স্থানীয় অধিক্ষেত্র সম্পন্ন বিশেষ ট্রাইব্যুনালে বদলী হইবে না।

(৫) কোন বিশেষ ট্রাইব্যুনাল, ভিন্নরূপ সিদ্ধান্ত গ্রহণ না করিলে, যে সাক্ষীর সাক্ষ্য গ্রহণ করা হইয়াছে উক্ত সাক্ষীর সাক্ষ্য পুনঃগ্রহণ, বা পুনঃশুনানী গ্রহণ করিতে, অথবা উপ-ধারা (৪) এর অধীন গৃহীত কার্যধারা পুনরায় আরম্ভ করিতে বাধা থাকিবে না, তবে ইতোমধ্যে যে সাক্ষ্য গ্রহণ বা উপস্থাপন করা হইয়াছে উক্ত সাক্ষ্যের ভিত্তিতে কার্য করিতে এবং মামলা যে পর্যায়ে ছিল সেই পর্যায়ে হইতে বিচারকার্য অব্যাহত রাখিতে পারিবে।

(৬) সরকার, আদেশ দ্বারা, যে স্থান বা সময় নির্ধারণ করিবে সেই স্থান বা সময়ে বিশেষ ট্রাইব্যুনাল আসন গ্রহণ করিতে পারিবে এবং উহার কার্যক্রম পরিচালনা করিতে পারিবে।

২৯। বিশেষ ট্রাইব্যুনালের পদ্ধতি।--(১) সাব-ইন্সপেক্টর পদমর্যাদার নিম্নে নহেন এরূপ কোন পুলিশ কর্মকর্তার লিখিত রিপোর্ট ব্যতীত বিশেষ ট্রাইব্যুনাল কোন অপরাধ বিচারার্থ গ্রহণ করিবে না।

(২) বিশেষ ট্রাইব্যুনাল এই আইনের অধীন অপরাধের বিচারকালে দায়রা আদালতে বিচারের জন্য, ফৌজদারী কার্যবিধির অধ্যায় ২৩ এ বর্ণিত পদ্ধতি, এই আইনের বিশেষ বিধানাবলীর সহিত অসংগতিপূর্ণ না হওয়া সাপেক্ষে, অনুসরণ করিবে।

(৩) কোন বিশেষ ট্রাইব্যুনাল, ন্যায় বিচারের স্বার্থে প্রয়োজনীয় না হলে, এবং কারণ লিখিতভাবে লিপিবদ্ধ না করিয়া, কোন মামলার বিচারকার্য স্থগিত করিতে পারিবেন না।

(৪) যেক্ষেত্রে বিশেষ ট্রাইব্যুনালের বিশ্বাস করিবার কারণ থাকে যে, অভিযুক্ত ব্যক্তি পলাতক রহিয়াছেন বা আত্মগোপন করিয়াছেন যে কারণে তাহাকে গ্রেপ্তার করিয়া বিচারের জন্য উপস্থিত করা সম্ভব নহে এবং তাহাকে অবিলম্বে গ্রেপ্তারের অবকাশ নাই, সেক্ষেত্রে উক্ত ট্রাইব্যুনাল, আদেশ দ্বারা, বহুল প্রচারিত অন্যান্য দুইটি বাংলা দৈনিক সংবাদপত্রে, অনুরূপ ব্যক্তিকে আদেশে উল্লিখিত সময়ের মধ্যে হাজির হইবার নির্দেশ প্রদান করিতে পারিবে, এবং উক্ত ব্যক্তি অনুরূপ নির্দেশ পালন করিতে ব্যর্থ হইলে তাহার অনুপস্থিতিতেই বিচার করা হইবে।

(৫) বিশেষ ট্রাইব্যুনালের সামনে অভিযুক্ত ব্যক্তি উপস্থিত হইবার বা জামিনে মুক্তি পাইবার পর পলাতক হইলে অথবা উহার সম্মুখে উপস্থিত হইতে ব্যর্থ হইলে, উপ-ধারা (৪) এ উল্লিখিত পদ্ধতি প্রযোজ্য হইবে না, এবং উক্ত ট্রাইব্যুনাল উহার সিদ্ধান্ত লিপিবদ্ধ করিয়া অনুরূপ ব্যক্তির অনুপস্থিতিতেই বিচার করিবে।

(৬) কোন বিশেষ ট্রাইব্যুনাল, উহার নিকট পেশকৃত আবেদনের ভিত্তিতে, বা উহার নিজ উদ্যোগে, কোন পুলিশ কর্মকর্তাকে এই আইনের অধীন সংঘটিত অপরাধ সংশ্লিষ্ট যে কোন মামলা পুনঃতদন্তের, এবং তদকর্তৃক নির্ধারিত সময়ের মধ্যে রিপোর্ট প্রদানের নির্দেশ প্রদান করিতে পারিবে।

৩০। বিশেষ ট্রাইব্যুনালের কার্যক্রমে কার্যবিধির প্রয়োগ।-- (১) ফৌজদারী কার্যবিধির বিধানাবলী, যতদূর সম্ভব, এই আইনের বিধানাবলীর সহিত অসংগতপূর্ণ না হওয়া সাপেক্ষে, বিশেষ ট্রাইব্যুনালের কার্যক্রমে প্রযোজ্য হইবে, এবং আদি এখতিয়ার প্রয়োগকারী দায়রা আদালতের সকল ক্ষমতা উক্ত বিশেষ ট্রাইব্যুনালের থাকিবে।

(২) বিশেষ ট্রাইব্যুনালে সরকার পক্ষে মামলা পরিচালনাকারী ব্যক্তি পাবলিক প্রসিকিউটর বলিয়া গণ্য হইবেন।

৩১। আপীল এবং মৃত্যুদণ্ড অনুমোদন।-- (১) বিশেষ ট্রাইব্যুনাল কর্তৃক প্রদত্ত কোন আদেশ, রায় অথবা দণ্ড প্রদানের তারিখ হইতে ত্রিশ দিনের মধ্যে উহার বিরুদ্ধে হাইকোর্ট বিভাগে আপীল দায়ের করা যাইবে।

(২) এই আইনের অধীন কোন বিশেষ ট্রাইব্যুনাল মৃত্যুদণ্ড প্রদান করিলে, অবিলম্বে কার্যধারাটি হাইকোর্ট বিভাগে অনুমোদনের জন্য প্রেরণ করিতে হইবে এবং উক্ত বিভাগ কর্তৃক অনুমোদিত না হওয়া পর্যন্ত মৃত্যুদণ্ড কার্যকর করা যাইবে না।

৩২। জামিন সংক্রান্ত বিধান।-- এই আইনের অধীন শাস্তিযোগ্য কোন অপরাধে অভিযুক্ত ব্যক্তিকে ম্যাজিস্ট্রেট বা বিচারক জামিনে মুক্তি প্রদান করিবেন না, যদি না --

(ক) রাষ্ট্রপক্ষকে অনুরূপ জামিনের আদেশের উপর শুনানীর সুযোগ প্রদান করা হয়; এবং

(খ) বিচারক সন্তুষ্ট হন যে অভিযুক্ত ব্যক্তি বিচারে দোষী সাব্যস্ত নাও হইতে পারেন মর্মে বিশ্বাস করিবার যুক্তিসঙ্গত কারণ রহিয়াছে এবং তিনি অনুরূপ সন্তুষ্টির কারণসমূহ লিখিতভাবে লিপিবদ্ধ করেন।

৩৩। বিশেষ ট্রাইব্যুনাল কর্তৃক মামলা নিষ্পত্তির নির্ধারিত সময়সীমা।-- (১) বিশেষ ট্রাইব্যুনালের বিচারক মামলার অভিযোগপত্র গঠনের তারিখ হইতে ছয় মাসের মধ্যে মামলার বিচার কার্য সমাপ্ত করিবেন।

(২) বিচারক উপ-ধারা (১) এর অধীন নির্ধারিত সময়ের মধ্যে কোন মামলা সমাপ্ত করিতে ব্যর্থ হইলে, তিনি উহার কারণ লিখিতভাবে লিপিবদ্ধ করিয়া অনধিক তিন মাস সময়সীমা বৃদ্ধি করিতে পারিবেন।

(৩) বিচারক উপ-ধারা (২) এ নির্ধারিত বর্ধিত সময়ের মধ্যে বিচার কার্য সমাপ্ত করিতে ব্যর্থ হইলে, তিনি, অনুরূপ ব্যর্থতার কারণ লিখিতভাবে উল্লেখ করিয়া হাইকোর্ট বিভাগ এবং সরকারকে অবহিত করিয়া, পুনরায় অনধিক তিন মাস সময়সীমা বৃদ্ধি করিতে পারিবেন।

অষ্টম অধ্যায়

সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ধৃত সম্পদ

৩৪। সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদের দখল।-- (১) কোন ব্যক্তি সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ধৃত কোন সম্পদ ভো বা দখল করিতে পারিবেন না।

(২) সন্ত্রাসী বা অন্য কোন ব্যক্তি এবং এই আইনের অধীন অভিযুক্ত বা দণ্ডপ্রাপ্ত হউক বা না হউক, এইরূপ অন্য কোন ব্যক্তির দখলে থাকা সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ, সরকারের অনুকূলে বাজেয়াপ্তযোগ্য হইবে।

ব্যাখ্যা।-- সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ অর্থ এই আইনের অধীন অপরাধ সংঘটনের মাধ্যমে অর্জিত বা লব্ধ কোন অর্থ, সম্পত্তি বা সম্পদ।

৩৫। সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ বাজেয়াপ্ত।-- যেক্ষেত্রে বিচারক এই মর্মে সন্তুষ্ট হন যে, কোন সম্পত্তি সন্ত্রাসী কার্য হইতে উদ্ধৃত হইবার কারণে জন্ম বা ক্রোক করা হয়, সেইক্ষেত্রে, তিনি যে ব্যক্তির দখল হইতে উক্ত সম্পত্তি জন্ম বা ক্রোক করা হইয়াছিল, সেই ব্যক্তি এই আইনের অধীন অভিযুক্ত হউক বা না হউক, উহা বাজেয়াপ্ত করিবার আদেশ প্রদান করিতে পারিবেন।

৩৬। সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ বাজেয়াপ্তকরণের পূর্বে কারণ দর্শাইবার নোটিশ জারী।-- (১) সন্ত্রাসী কর্মকাণ্ড-লব্ধ বাজেয়াপ্ত করিবার আদেশ প্রদানের পূর্বে, যে ব্যক্তির নিয়ন্ত্রণ অথবা দখলে উক্ত সম্পদ থাকে, উক্ত ব্যক্তিকে লিখিত নোটিশ প্রদানপূর্বক বাজেয়াপ্ত করিবার কারণ অবহিত না করিয়া এবং নোটিশে প্রদত্ত সময়সীমার মধ্যে লিখিত

জবাব প্রদানের সুযোগ এবং শুনানীর যুক্তিসঙ্গত সময় প্রদান ব্যতিরেকে কোন সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ বাজেয়াপ্ত করিবার আদেশ প্রদান করা যাইবে না।

(২) উপ-ধারা (১) এর অধীন কোন বাজেয়াপ্তির আদেশ প্রদান করা যাইবেনা, যদি অনুরূপ ব্যক্তি প্রমান করিতে সক্ষম হন যে, উক্ত সম্পদ সন্ত্রাসী কর্মকাণ্ডে-লব্ধ সম্পদ ছিল তাহা তিনি অবগত ছিলেন না এবং উপযুক্ত মূল্যের বিনিময়ে তিনি তাহা খরিদ করিয়াছেন।

৩৭। আপীল।-- (১) ধারা ৩৫ এর অধীন প্রদত্ত বাজেয়াপ্তকরণ আদেশ দ্বারা সংক্ষুব্ধ কোন ব্যক্তি উক্ত আদেশ প্রাপ্তির তারিখ হইতে এক মাসের মধ্যে হাইকোর্ট বিভাগে আপীল করিতে পারিবেন।

(২) হাইকোর্ট বিভাগ কর্তৃক ধারা ৩৫ এর অধীন প্রদত্ত কোন আদেশ সংশোধিত বা বাতিল করা হইলে অথবা এই আইনের কোন বিধান লংঘনপূর্বক কোন মামলা দায়ের করা হইলে, যে ব্যক্তির বিরুদ্ধে ধারা ৩৫ এর অধীন বাজেয়াপ্তির আদেশ প্রদান করা হইয়াছে, উক্ত ব্যক্তি খালাসপ্রাপ্ত হইলে উক্ত বাজেয়াপ্তকৃত সম্পত্তি ফেরত প্রদান করা হইবে এবং যদি উক্ত ব্যক্তির নিকট বাজেয়াপ্তকৃত সম্পত্তি ফেরত প্রদান সম্ভব না হয়, তাহা হইলে উক্ত ব্যক্তিকে উক্ত সম্পত্তি সরকারের নিকট বিক্রয় হইয়াছেন গণ্যে, সম্পত্তি জব্দের দিন হইতে যুক্তিসঙ্গত সুদ গণনাপূর্বক এবং যুক্তিসঙ্গতভাবে মূল্য নির্ধারণপূর্বক উহার মূল্য পরিশোধ করিতে হইবে।

নবম অধ্যায়

পারস্পরিক আইনগত সহায়তা

৩৮। পারস্পরিক আইনগত সহায়তা।-- (১) যখন কোন সন্ত্রাসীকার্য এইরূপে সংঘটিত হয় বা উহার সংঘটনে এইরূপে সহায়তা, চেষ্টা, ষড়যন্ত্র বা অর্থায়ন করা হয় যাহাতে কোন বিদেশী রাষ্ট্রের ভূখণ্ড সংশ্লিষ্ট থাকে, অথবা কোন সন্ত্রাসীকার্য বা উহার সংঘটনে সহায়তা, চেষ্টা, ষড়যন্ত্র বা অর্থায়ন কোন বিদেশী সার্বভৌম রাষ্ট্রের ভূখণ্ড হইতে বাংলাদেশের অভ্যন্তরে অথবা বাংলাদেশের অভ্যন্তর হইতে অন্য কোন সার্বভৌম রাষ্ট্রের ভূখণ্ডে সংঘটিত হইয়া থাকে, তাহা হইলে উক্ত বিদেশী রাষ্ট্র অনুরোধ করিলে বাংলাদেশ সরকার, সম্মত হইলে, এই ধারার পরবর্তী বিধানাবলী সাপেক্ষে, ফৌজদারী তদন্ত, বিচারকার্য বা বহিঃসমর্পন সম্পর্কিত সকল প্রয়োজনীয় বিষয়ে উক্ত বিদেশী রাষ্ট্রকে আইনগত সহায়তা প্রদান করিবে।

(২) অনুরোধকারী রাষ্ট্র এবং অনুরোধপ্রাপ্ত রাষ্ট্রের মধ্যে পারস্পরিক মত বিনিময়ের মাধ্যমে সম্পাদিত আনুষ্ঠানিক চুক্তি কিংবা পত্র বিনিময়ের ভিত্তিতে আইনগত সহযোগিতার শর্তাদি নির্ধারণ করা হইবে।

(৩) এই আইনের অধীন কোন অপরাধের অভিযোগে বিচারের জন্য বাংলাদেশের কোন নাগরিককে এই ধারার অধীনে কোন বিদেশী রাষ্ট্রের নিকট সমর্পন করা যাইবে না।

(৪) এই ধারার অধীন পারস্পরিক আইনগত সহায়তার উদ্দেশ্যে বাংলাদেশের কোন নাগরিককে, তাহার সম্মতি সাপেক্ষে, সংশ্লিষ্ট ফৌজদারী মামলা বা তদন্ত কার্যে সাক্ষী হিসেবে সহায়তা প্রদান করিবার জন্য কোন বিদেশী রাষ্ট্রের নিকট সমর্পন করা যাইবে।

(৫) যদি সরকারের নিকট বিশ্বাস করিবার মত যথেষ্ট কারণ থাকে যে, কোন ব্যক্তিকে কোন মামলায় শুধুমাত্র তাহার গোত্র, ধর্ম, জাতীয়তা বা রাজনৈতিক মতাদর্শের কারণে বিচার করিবার বা শাস্তি প্রদানের লক্ষ্যে এই ধারার অধীন আইনগত সহায়তার জন্য অনুরোধ করা হইয়াছে, তাহা হইলে অনুরোধপ্রাপ্ত রাষ্ট্র হিসেবে বাংলাদেশ অনুরূপ কোন নির্দিষ্ট মামলার ক্ষেত্রে বহিঃ সমর্পন বা পারস্পরিক আইনগত সহায়তার অনুরোধ প্রত্যাখান করিতে পারিবে।

দশম অধ্যায়

সাধারণ বিধানবলী

৩৯। অপরাধের আমলযোগ্যতা ও জামিন অযোগ্যতা। -- (১) এই আইনের অধীন সকল অপরাধ আমলযোগ্য (cognizable) হইবে।

(২) এই আইনের অধীন সকল অপরাধ জামিন অযোগ্য (Non-bailable) হইবে।

৪০। তদন্ত ও বিচার বিষয়ে পূর্বানুমোদনের অপরিহার্যতা।-- (১) জেলা ম্যাজিস্ট্রেটের পূর্বানুমোদন ব্যতিরেকে কোন পুলিশ কর্মকর্তা এই আইনের অধীন কোন অপরাধের তদন্ত করিতে পারিবেন না।

(২) সরকারের পূর্বানুমোদন (sanction) ব্যতিরেকে কোন আদালত এই আইনের অধীন কোন অপরাধ বিচারার্থ আমলে গ্রহণ (cognizance) করিবে না।

৪১। বিশেষ ট্রাইব্যুনাল এবং বিশেষ ট্রাইব্যুনাল হইতে মামলা স্থানান্তর।-- সরকার, সাক্ষ্য সমাপ্তির পূর্বে বিচারের যে কোন পর্যায়ে, যুক্তিসঙ্গত কারণে, এই আইনের অধীন কোন অপরাধ সংক্রান্ত মামলা বা মামলাসমূহ কোন দায়রা আদালত হইতে কোন বিশেষ ট্রাইব্যুনালে বা কোন বিশেষ ট্রাইব্যুনাল হইতে কোন দায়রা আদালতে স্থানান্তর করিতে পারিবে।

৪২। তফসিল সংশোধনের ক্ষমতা।-- সরকার, সরকারী গেজেটে প্রজ্ঞাপিত আদেশ দ্বারা, এই আইনের তফসিল সংশোধন করিতে পারিবে।

৪৩। বিধি প্রণয়নের ক্ষমতা।-- সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের উদ্দেশ্যে পূরণকল্পে, বিধি প্রণয়ন করিতে পারিবে।

৪৪। মূল পাঠ এবং ইংরেজী পাঠ।-- এই আইনের মূল পাঠ বাংলাতে হইবে এবং ইংরেজীতে অনূদিত উহার একটি নির্ভরযোগ্য পাঠ থাকিবে :

তবে শর্ত থাকে যে, বাংলা ও ইংরেজী পাঠের মধ্যে বিরোধের ক্ষেত্রে বাংলা পাঠ প্রাধান্য পাইবে।

৪৫। রহিতকরণ ও হেফাজত।-- (১) সন্ত্রাস বিরোধী অধ্যাদেশ, ২০০৮ (২০০৮ সনের ২৮ নং অধ্যাদেশ) এতদ্বারা রহিত করা হইল।

(২) উক্তরূপ রহিতকরণ সত্ত্বেও, রহিত অধ্যাদেশের অধীন কৃত কাজকর্ম বা গৃহীত ব্যবস্থা এই আইনের অধীন কৃত বা গৃহীত হইয়াছে বলিয়া গণ্য হইবে।

তফসিল

(ধারা-১৮ দ্রষ্টব্য)

১	২	৩	৪	৫
ক্রমিক নং	সংগঠনের নাম	সংগঠনের ঠিকানা	নিষিদ্ধকরণের তারিখ	মন্তব্য

আশফাক হামিদ
সচিব।

রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ



গেজেট

অতিরিক্ত সংখ্যা
কর্তৃপক্ষ কর্তৃক প্রকাশিত

বৃহস্পতিবার, জুন ৭, ২০১২

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
আইন, বিচার ও সংসদ বিষয়ক মন্ত্রণালয়
লেজিসলেটিভ ও সংসদ বিষয়ক বিভাগ
প্রজ্ঞাপন

তারিখ, ৩০ মে, ২০১২ ইং

নং ০৮ (আঃম)(লেঃস)(মুঃপ্রঃ)-আইন-অনুবাদ-২০১২—সরকারি কার্যবিধিমালা, ১৯৯৬ এর প্রথম তফসিল (বিভিন্ন মন্ত্রণালয় এবং বিভাগের মধ্যে কার্যবন্টন) এর আইটেম ৩০ এ ক্রমিক ৭ ও ১০ এবং মন্ত্রিপরিষদ বিভাগের বিগত ৩-৭-২০০০ইং তারিখের সভায় গৃহীত সিদ্ধান্ত বাস্তবায়নের নিমিত্ত মানিলিভারিং আইন, ২০১২ (২০১২ সনের ০৫ নং আইন) এর ইংরেজী অনুবাদ সর্বসাধারণের জ্ঞাতার্থে প্রকাশ করিল।

মোঃ দেলোয়ার হোসেন
সহকারী সচিব (চঃ দাঃ)।

(৮৬২৬৭)
মূল্য : টাকা ২৪.০০

Money Laundering Prevention Act, 2012**Bangladesh Parliament**

Dhaka, 20 February, 2012/08 Falgun, 1418

The following Act of Parliament received the assent of the President on 20 February, 2012 (08 Falgun, 1418) and is hereby published for general information :—

Act No. 5 of 2012**An Act to repeal the existing Act and Ordinance regarding the prevention of money laundering and to reenact a law relating thereto**

Whereas it is expedient and necessary to reenact a law regarding the prevention of money laundering and other offences connected therewith including punishment thereof and the matters ancillary thereto by repealing the existing Act and Ordinance relating thereto;

Therefore, it is hereby enacted as follows :—

1. Short title and commencement.—(1) This Act may be called the Money Laundering Prevention Act, 2012.

(2) It shall be deemed to have come into force on 3 Magh, 1418 BE/16 January, 2012 AD.

2. Definitions.—Unless there is anything repugnant in the subject or context, in this Act—

(a) “smuggling of money or property” means—

- (i) transfer or holding money or property outside the country in breach of the existing laws in the country; or
- (ii) refrain from repatriating money or property from abroad in which Bangladesh has an interest and was due to be repatriated; or
- (iii) not bringing into the country the actual dues from a foreign country, or paying to a foreign country in excess of the actual dues;

(b) “money value transferor” means a financial service in which the service provider receives currency, cheques, other financial instruments (electronic or otherwise) in one location, and provides the beneficiary with the equal value in currency or financial instruments or any other means in a different location;

- (c) “proceeds of crime” means any property obtained or derived, directly or indirectly, from a predicate offence or any such property retained or controlled by anybody;
- (d) “freeze” means any action taken by the competent authorities pursuant to this Act by which any property is brought within the control of the relevant authorities or the court on a temporary basis and the property shall be disposed of by taking a final decision by the court regarding confiscation of the property;
- (e) “non-profit organization/institution” means any institution registered under section 28 of the Company Act, 1994 (Act XVIII of 1994);
- (f) “financial instrument” means all papers or electronic documents which have a financial value;
- (g) “financial institution” means a financial institution defined under section 2(b) of the Financial Institutions Act, 1993 (Act No. XXVII of 1993),
- (h) “court” means the court of a special judge;
- (i) “attachment” means any action taken by the court pursuant to this Act by which any property is restrained or held by the relevant authorities or the court on a temporary basis and the property shall be disposed of by taking a final decision by the court;
- (j) “customer” means any person or persons or entity or entities that may be defined by Bangladesh Bank from time to time;
- (k) “trust and company service providers” means any person or business institution that is not defined in any other laws and provides with any of the following services to any third party:—
- (1) to act as an agent of establishing any legal entity,
 - (2) to act as or appoint someone to act as a director, secretary of any legal entity or act as a partner in a partnership business, or perform other responsibilities in an equivalent position.
 - (3) to act as a registered agent for any legal entity,
 - (4) to act as or appoint someone to act as a trustee of an express trust,
 - (5) to act as or appoint someone to act as a director instead of a nominee shareholder or any other person;

- (l) “investigation agency” means the Anti Corruption Commission established under the Anti Corruption Commission Act, 2004 (Act No. V of 2004); and any officer of the Commission authorized in this behalf by it to investigate or notwithstanding anything contained in any other law, it shall also include any officer of any other investigation agency;
- (m) “cash” means any currency recognized by a country as being the authorized currency for that country, including coins, paper currency, travelers’ cheques, postal notes, money orders, cheques, bank drafts, bearer bonds, letters of credit, bills of exchange, credit card, debit card or promissory notes;
- (n) “disposal” means the sale of property which is degradable, perishable or unsuitable for use after a certain time, or the destruction of property which falls within properties suitable for destruction under any other law or it shall also include any legal transfer of property by means of an open auction;
- (o) “confiscation” means the permanent transfer of the title of any property in favour of the State pursuant to a court order made under section 17;
- (p) “Bangladesh Bank” means Bangladesh Bank established under the Bangladesh Bank Order, 1972 (P.O. No. 127 of 1972);
- (q) “insurer” means an insurer defined under section 2(25) of the Insurance Act, 2010 (Act No. XIII of 2010);
- (r) “non government organization” means the institutions authorized or registered under the Societies Registration Act, 1860 (Act No. XXI of 1860), the Voluntary Social Welfare Agencies (Registration and Control) Ordinance, 1961 (Ordinance No. XLVI of 1961), the Foreign Donations (Voluntary Activities) Regulation Ordinance, 1978 (Ordinance No. XLVI of 1978), the Foreign Contributions Regulation Ordinance, 1982 [(Ordinance No. XXXI of 1982), and the Microcredit Regulatory Authority Act, 2006 (Act No. XXXII of 2006) which—
- (i) receive fund (loan, grant, deposit) from local sources or provides with fund to others; and/or
- (ii) receive any kind of foreign donation or loan or grant;
- (s) “foreign currency” means any foreign exchange defined under section 2(d) of the Foreign Exchange regulation Act, 1947 (Act No. VII of 1947);

- (t) "bank" means a bank company defined under section 5(o) of the Bank Companies Act, 1991 (Act No. XIV of 1991) and it shall also include any other institution designated as a bank under any other law;
- (u) "money changer" means any person or institution approved by Bangladesh Bank under section 3 of the Foreign Exchange Regulation Act, 1947 (Act No. VII of 1947) for dealing in foreign exchange transactions;
- (v) "money laundering" means—
- (i) knowingly moving, converting, or transferring property involved in an offence for the following purposes:—
 - (1) concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
 - (2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
 - (ii) smuggling money or property earned through legal or illegal means to a foreign country;
 - (iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
 - (iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
 - (v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
 - (vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
 - (vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
 - (viii) participating in, associating with conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

- (w) "reporting organization" means—
- (i) bank;
 - (ii) financial institution;
 - (iii) insurer;
 - (iv) money changer;
 - (v) any company or institution which remits or transfers money or money value;
 - (vi) any other institution carrying out its business with the approval of Bangladesh Bank;
 - (vii) (1) stock dealer and stock broker,
(2) portfolio manager and merchant banker,
(3) securities custodian,
(4) asset manager;
 - (viii) (1) non-profit organization,
(2) non-government organization,
(3) cooperative society;
 - (ix) real estate developer;
 - (x) dealer in precious metals or stones;
 - (xi) trust and company service provider;
 - (xii) lawyer, notary, other legal professional and accountant;
 - (xiii) any other institution which Bangladesh Bank may, from time to time, notify with the approval of the Government;
- (x) "real estate developer" means any real estate developer or its officers or employees or agents defined under section 2(15) or Real Estate Development and Management Act, 2010 (Act No. 48 of 2010) who are engaged in constructing and buying and selling of land, house, commercial building and flat etc.;
- (y) "entity" means any kind of legal entity, statutory body, commercial or non commercial organization, partnership firm, cooperative society or any organization comprising one or more than one person;

- (z) “suspicious transaction” means such transaction—
- (i) which deviates from usual transactions;
 - (ii) of which there is ground to suspect that,
 - (1) the property is the proceeds of an offence,
 - (2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;
 - (iii) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Bank from time to time;
- (aa) “cooperative society” means an institution established under section 2(20) of the Cooperative Societies Act, 2001 (Act No. XLVII of 2001) which is involved in receiving deposits and providing loans;
- (bb) “property” means—
- (i) any type of tangible, intangible, moveable, immoveable property; or
 - (ii) cash, any deed or legal instrument of any form including electronic or digital form giving evidence of title or evidence of interest related to title in the property which is located within or outside the country;
- (cc) “predicate offence” means the offences mentioned below, by committing which within or outside the country, the money or property derived from is laundered or attempt to be laundered, namely :—
- (1) corruption and bribery;
 - (2) counterfeiting currency;
 - (3) counterfeiting deeds and documents;
 - (4) extortion;
 - (5) fraud;
 - (6) forgery;
 - (7) illegal trade of firearms;
 - (8) illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;

-
- (9) illegal trade in stolen and other goods;
 - (10) kidnapping, illegal restrain and hostage taking;
 - (11) murder, grievous physical injury;
 - (12) trafficking of women and children;
 - (13) black marketing;
 - (14) smuggling of domestic and foreign currency;
 - (15) theft or robbery or dacoity or piracy or hijacking of aircraft;
 - (16) human trafficking;
 - (17) dowry;
 - (18) smuggling and offences related to customs and excise duties;
 - (19) tax related offences;
 - (20) infringement of intellectual property rights;
 - (21) terrorism or financing in terrorist activities;
 - (22) adulteration or the manufacture of goods through infringement of title;
 - (23) offences relating to the environment;
 - (24) sexual exploitation;
 - (25) insider trading and market manipulation using price sensitive information relating to the capital market in share transactions before it is published for general information to take advantage of the market and attempting to manipulate the market for personal or institutional gain;
 - (26) organized crime, and participation in organized criminal groups;
 - (27) racketeering; and
 - (28) any other offence declared as predicate offence by Bangladesh Bank, with the approval of the Government, by notification in the official Gazette, for the purpose of this Act.
- (dd) “special judge” means a special judge appointed under section 3 of the Criminal Law Amendment Act, 1958 (Act No. XL of 1958);

- (ee) (1) “stock dealer and stock broker” means an institution defined under rule 2(i) and (j) of the Securities and Exchange Commission (Stock Dealer, Stock Broker and Authorized Representative) Rules, 2000;
- (2) “portfolio manager and merchant banker” means an institution defined under rule 2(f) and 2(j) of the Securities and Exchange Commission (Merchant Banker and Portfolio Manager) Rules, 1996;
- (3) “securities custodian” means an institution defined under rule 2(j) of the Securities and Exchange Commission (Security Custodial Service) Rules, 2003;
- (4) “asset managers” means an institution defined under rule 2(s) of the Securities and Exchange Commission (Mutual Fund) Rules, 2001;
- (ff) “High Court Division” means the High Court Division of the Bangladesh Supreme Court.

3. **Act to override other laws.**—Notwithstanding anything contained in any other law for the time being in force, the provisions of this Act shall, subject to the provisions of section 9, have effect.

4. **Offence of money laundering and punishment.**—(1) For the purposes of this Act, money laundering shall be deemed to be an offence.

(2) Any person who commits or abets or conspires to commit the offence of money laundering shall be punished with imprisonment for a term of at least 4 (four) years but not exceeding 12 (twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lacks, whichever is greater.

(3) In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favour of the State which directly or indirectly involved in or related with money laundering or any predicate offence.

(4) Any entity which commits an offence under this section shall be punished with a fine of not less than twice of the value of the property or taka 20 (twenty) lacks, whichever is greater and in addition to this the registration of the said entity shall be liable to be cancelled.

(5) It shall not be a prerequisite to charge or punish for money laundering to be convicted or sentenced for any predicate offence.

5. Punishment for violation of an order for freezing or attachment.—Any person who violates a freezing or attachment order issued under this Act shall be punished with imprisonment for a term not exceeding 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or with both.

6. Punishment for divulging information.—(1) No person shall, with an ill motive divulge any information relating to the investigation or any other related information to any person, organization or news media.

(2) Any person, institution or agent empowered under this Act shall refrain from using or divulging any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act.

(3) Any person who contravenes the provisions of sub-sections (1) and (2) shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

7. Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information.—(1) Any person who, under this Act—

- (a) obstructs or declines to cooperate with any investigation officer for carrying out the investigation; or
- (b) declines to supply information or submit a report being requested without any reasonable ground;

shall be deemed to have committed an offence under this Act.

(2) Any person who is convicted under sub-section (1) shall be punished with imprisonment for a term not exceeding 1 (one) year or with a fine not exceeding taka 25 (twenty five) thousand or with both.

8. Punishment for providing false information.—(1) No person shall knowingly provide false information in any manner regarding the source of fund or self identity or the identity of an account holder or the beneficiary or nominee of an account.

(2) Any person who violates the provision of sub-section (1) shall be punished with imprisonment for a term not exceeding 3 (three) years or a fine not exceeding taka 50 (fifty) thousand or with both.

9. Investigation and trial of an offence.—(1) Notwithstanding anything contained in any other law, the offences under this Act shall be considered as the scheduled offences under the Anti Corruption Commission Act, 2004 (Act No. V of 2004) and shall be investigated by the Anti Corruption Commission or any officer of the Commission empowered by it in this behalf or any officer of any other investigating agency authorized by the Anti Corruption Commission.

(2) The offences under this Act shall be tried by a special judge appointed under section 3 of the Criminal Law Amendment Act, 1958 (Act No. XL of 1958).

(3) For the purpose of the investigation and identification of property of an accused person, the Anti Corruption Commission may, besides this Act, also exercise the powers vested in it under the Anti Corruption Commission Act, 2004 (Act No. V of 2004) and an officer of any other investigating agency authorized by the Anti Corruption Commission may, besides this Act, also exercise the powers vested in it under any other law.

10. Extraordinary jurisdiction of the special judge.—(1) The special judge may impose such punishments as are specified for the offences under this Act, and where appropriate, may pass any other necessary order including orders for further investigation, freezing, attachment and confiscation of property.

(2) If the special judge passes an order for further investigation of any case filed under this Act, he shall, in the said order, specify a time-limit which shall not exceed 6 (six) months directing the investigation officer to submit his investigation report.

11. Cognizancy, non-compoundability and non-bailability of offences.—Offences under this Act shall be cognizable, non-compoundable and non-bailable.

12. Inevitability of the approval of the Anti Corruption Commission.—(1) Notwithstanding anything contained in the Code of Criminal Procedure or any other law for the time being in force, no court shall take cognizance of any offence under this Act, except with the approval of the Anti Corruption Commission.

(2) After concluding the investigation under this Act, the investigation officer shall take prior approval of the Anti Corruption Commission before submitting his report and shall submit a copy of the approval before the court along with the report.

13. Provisions relating to bail.—Any person accused under this Act shall be released on bail, if—

- (a) the complainant is given an opportunity of being heard on the application for bail; and
- (b) the court is not satisfied that there are reasonable grounds to believe that the accused shall be found guilty of the charges brought against him; or
- (c) the accused is a woman, child or physically disabled person and the court is satisfied that justice may not be hindered by reason of releasing him on bail.

14. Orders to freeze or attach property.—(1) The court may, on the basis of a written application by the Anti Corruption Commission or any person or organization authorized by it, issue an order to freeze or attach the property, within or outside the country, involved in money laundering or any other offence.

(2) At the time of making a written application before the court under subsection (1) for an order to freeze or attach any property, the Anti Corruption Commission or any person or organization authorized by it shall mention the following information in the application, namely :—

- (a) full description of the property for which an order for freezing or attachment is sought;
- (b) grounds and primary evidence in support of the property for being attachable due to its involvement in money laundering or any other offence;
- (c) the apprehension that the property may be transferred or taken beyond possession before the disposal of the complaint, if an order is not passed by the court according to the application.

(3) If an order for freezing or attachment is passed under sub-section (1), the court shall, by notification in the official Gazette, publish the matter with details of the property for general information and at least in 2 (two) widely circulated national dailies [1 (one) Bengali and 1 (one) English] in the form of a notice.

(4) In an order passed under this section to freeze or attach any property, the name of the accused, the names of his parents, the name of spouse, nationality, designation (if any), occupation, tax identification number (TIN), present and permanent addresses and any other identification of the accused shall, in so far as possible, be mentioned, but the enforcement of the provisions of this Act shall not be impeded by any trifling errors and omissions of these information.

(5) Subject to the provisions of sub-section (6), if the court passes an order for freezing or attachment of any property of a person under this section, the property may, unless the court directs otherwise, not be in any way transferred elsewhere and no transactions may be carried out with respect to the property not may any encumbrances be attached to the property while the order is in force.

(6) While an order for freezing with respect to any person's bank account is in force, all money receivable by that person may be deposited into the frozen bank account, unless otherwise mentioned in the order.

15. Return of frozen or attached property.—(1) If any court makes an order to freeze or attach any property under section 14 and any person or entity other than the accused person or entity has an interest in that property, the person or the entity may make an application before the court for the return of the property within 30 (thirty) days of the publication of the notice on the order to freeze or attach the property.

(2) If any person or entity makes an application before the court under sub-section (1), the following information shall be mentioned in the application:—

- (a) the property is not involved directly or indirectly in money laundering or any predicate offence;
- (b) the applicant is not involved directly or indirectly in the alleged money laundering or any other predicate offence;

- (c) the applicant is not acting as a nominee of, or on behalf of, the accused person;
- (d) the accused person or entity has no proprietary right, interest or ownership with regard to the frozen or attached property; and
- (e) the applicant has a proprietary right, interest and ownership in the frozen or attached property.

(3) Notwithstanding anything contained in sub-section (5) of section 14, if the court receives any application for return of any property under this section, it shall give the applicant, the investigation agency and the accused person or entity an opportunity of being heard and at the end of the hearing, after reviewing the necessary documents, if the court is satisfied with the application of the applicant brought under sub-section (1) and finds that the Government has not persented a reasonable suspicion that the property is involved directly or indirectly in money laundering or a predicate offence, it shall set aside the order to freeze or attach the property, and pass an order for transfer of the property in favour of the applicant within the time specified in the order.

16. Appeal against the order to freeze or attach property.—(1) Any person or entity aggrieved by an order for freezing or attachment of any property, passed by a court under this Act, may prefer an appeal against such order before the High Court Division within 30 (thirty) days.

(2) If an appeal is preferred under sub-section (1) the appellate court shall give the parties reasonable time for being heard, and at the end of hearing, may pass such order as it deems fit.

(3) If any person or entity aggrieved by an order to freeze or attach any property passed by any court under section 14 prefers an appeal against such order, the said order shall have effect pending the appeal to be disposal of, unless the appellate court directs otherwise.

17. Confiscation of property.—(1) If any person or entity is convicted of the offence of money laundering under this Act, the court may pass an order for confiscation of any property, within or outside the country, involved directly or indirectly in money laundering or predicate offence in favour of the State.

(2) Notwithstanding anything contained in sub-section (1) during an inquiry and investigation or prosecution under this Act relating to an offence of money laundering, the respective court may, where necessary, pass an order for the confiscation of any property situated within or outside the country in favour of the State.

(3) If any person convicted of the offence of money laundering under this Act absconds or dies after submitting the charge sheet, the court may pass order for confiscation of that person's property which was involved in the money laundering or predicate offence in favour of the State.

Explanation.—A person shall be deemed to have absconded for the purposes of this section where the person, despite adequate measures being taken, fails to surrender before the court within 6 (six) months of issuance of the warrant of arrest, or it is not possible to arrest the person within the period.

(4) If any person or entity purchases any property applied for confiscation in good faith and for proper value before an order for confiscation of the property is passed by the court under the provisions of this section or before a case is filed or a complaint is lodged, and the person or the entity is able to satisfy the court that he or it was not aware of the matter that the said property was involved in money laundering, and purchased the property in good faith, then the court may, instead of ordering for confiscation of the property, order the convicted person or entity to deposit the proceeds of the sale of the property to the treasury of the State within the time specified by it.

(5) If the court finds that the property involved directly or indirectly in money laundering or any predicate offence cannot be located or confiscated or has been dissipated for being used otherwise, the court may—

- (a) pass an order for confiscation of such property of an equivalent value of the accused as is not related with the offence;
- (b) impose a fine on the accused equivalent to the value of the unrecovered property.

(6) If any property is confiscated under this section, the notice of the order of confiscation shall be sent by registered post to the last known address of the person or entity having control of the confiscated property and such notice, along with the schedule and full details of the property, shall be published in the official Gazette and at least 2 (two) widely circulated national dailies [1(one) Bengali and 1(one) English].

(7) If any court pass an order for confiscation of any property under this section, the ownership of the property shall be vested in the State and the person or entity who is the owner or custodian of the property shall hand over the possession of the property to the State as early as possible.

(8) If the proceeds of crime have been mingled with property acquired from legitimate sources, such property shall be liable to confiscation up to the assessed value of the mingled proceeds by the court or where the value of the proceeds of crime cannot be determined, the court may pass a confiscation order on the full value of the mingled money or property in favour of the State.

18. Return of confiscated property.—(1) If a court pass an order of confiscation of any property under section 17 and any person or entity other than the convicted person has any title, interest or right in the property, the person or the entity may make an application before the court for the return of the property within 30 (thirty) days of the publication of the notice of confiscation of the property in newspaper.

(2) If any application is received under sub-section (1), the court shall give a reasonable time to the person who filed the case, the convicted person or entity and the applicant to be heard and after hearing, the court may pass necessary order considering the following matters, namely :—

- (a) whether the applicant or the confiscated property or any part thereof had any involvement in the commission of the offence;
- (b) whether the applicant has a valid right to acquire the confiscated property;
- (c) the duration of the commission of the offence and the duration of alleged ownership of the confiscated property by the applicant; and
- (d) any other information deemed to be relevant by the court.

19. Appeal against any order for confiscation.—(1) If any court pass an order for confiscation of any property under this Act, the party aggrieved by such an order may prefer an appeal against the order before the High Court Division within 30 (thirty) days.

(2) If an appeal is preferred under sub-section (1), the appellate court shall give both the parties reasonable opportunity of being heard and may, on conclusion of such hearing, pass such orders as it deems fit.

20. Procedure for disposal of confiscated property.—(1) If any property is confiscated under this Act, the Government may, subject to the permission of the court, sell or, in any other way, dispose of such property other than the property which is required to be destroyed under any other law, by means of an open auction or by any other commercially profitable and lawful means.

(2) The proceeds of the sale or disposal of the property in any other legal manner under sub-section (1) shall be deposited into the treasury of the State.

21. Appointment of a manager or caretaker for taking care of the frozen, attached or confiscated property.—If any property is frozen, attached or confiscated under this Act, the court may, upon an application of the investigation agency or any person authorized by it in this behalf, appoint any law enforcement agency as a manager or caretaker of the property to take control, manage, look after or, in any other manner, deal with the total property or any part thereof under such terms and conditions as the court may deem fit.

22. Appeal.—Notwithstanding anything contained in any other law for the time being in force, any party aggrieved by an order, judgment, decree or sentence passed by a court under this Act may prefer an appeal before the High Court Division within 30 (thirty) days from the date of such order, judgment, decree or sentence.

23. Powers and responsibilities of Bangladesh Bank in restraining and preventing the offence of money laundering.—(1) For the purposes of this Act, Bangladesh Bank shall have the following powers and responsibilities, namely:—

- (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 involves 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 onto 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 directions 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.

(2) If any investigation agency makes a request to provide it with any information in any investigation relating to money laundering or suspicious transaction, then Bangladesh Bank shall provide with such information where there is no obligation for it under any existing law or for any other reason.

(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 licence 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 subsection (1), 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-section (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.

24. Establishment of the Bangladesh Financial Intelligence Unit (BFIU).—(1) In order to exercise the power and perform the duties vested in Bangladesh Bank under section 23 of this Act, there shall be a separate unit to be called the Bangladesh Financial Intelligence Unit (BFIU) within Bangladesh Bank.

(2) For the purposes of this Act, the governmental, semi-governmental, autonomous organizations or any other relevant institutions or organizations shall, upon any request or spontaneously, provide the Bangladesh Financial Intelligence Unit with the information preserved or gathered by them.

(3) The Bangladesh Financial Intelligence Unit may, if necessary, spontaneously provide other law enforcement agencies with the information relating to money laundering and terrorist financing.

(4) The Bangladesh Financial Intelligence Unit shall provide with information relating to money laundering or terrorist financing or any suspicious transactions to the Financial Intelligence Unit of another country on the basis of any contract or agreement entered into with that country under the provisions of this Act and may ask for any such information from any other country.

(5) The Bangladesh Financial Intelligence Unit may also provide with such information to the Financial Intelligence Units of other countries spontaneously where there is no such contract or agreement under sub-section (4).

25. Responsibilities of the reporting organizations in prevention of money laundering.—(1) The reporting organizations shall have the following responsibilities in the prevention of money laundering, namely :—

- (a) to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
- (b) if any account of a customer is closed, to preserve previous records of transactions of such account for at least 5(five) years from the date of such 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 doubtful transaction or attempt of such transaction as defined under clause (n) of section 2 is observed, to report the matter as 'suspicious transaction report' to the Bangladesh Bank immediately on its own accord.

(2) If any reporting organization violates the provisions of sub-section (1), 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 be relevant authority may take appropriate measures against the organization.
- (3) Bangladesh Bank shall collect the sum of fine imposed under sub-section (2) in such manner as it may determine and the sum collected shall be deposited into treasury of the State.

26. Contract with foreign countries.—(1) For the purposes of this Act, the Government may enter into a contract with any foreign State under bilateral or multilateral agreements, conventions or any other means recognized by international law.

(2) If the Government enters into any contract with any foreign State under this section, the Government may, for the purpose of prevention of money laundering :—

- (a) ask for necessary information from the foreign State or organization; and
- (b) provide with information asked for by the foreign State or organization if it is not a threat to national security.

(3) For the purposes of this Act, the Bangladesh Financial Intelligence Unit (BFIU) may sign any memorandum of understanding with any foreign financial intelligence unit or other organization and under the memorandum of understanding BFIU may—

- (a) ask for necessary information from the foreign financial Intelligence unit or organization; and
- (b) provide information sought by the foreign financial Intelligence unit or organization if it is not a threat to national security.

(4) Any court may, upon the application of Attorney General's Office, pass such orders as it deems fit where, for the purpose of this Act, it is necessary to confiscate or return any property situated in Bangladesh in order to comply with an order made by a court of a foreign State under a contract; similarly the Attorney General's Office may make a request to a foreign State for the purpose of complying with an order passed by a court in Bangladesh for confiscation or return of property under a contract or memorandum of understanding.

(5) Notwithstanding anything contained in any other law, any documents received from the appropriate authorities of any foreign State under the scope of mutual legal assistance, shall, for the purposes of this Act, be admissible as evidence before the relevant court.

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

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

28. Protection of actions taken in good faith.—No suit or prosecution or administrative measures or any other legal proceedings shall lie against the Government or any officer or staff of the Government or Bangladesh Bank or any officer or staff of Bangladesh Bank or the Anti-Corruption Commission or any officer or staff of the Commission or any reporting organization or its Board of Directors or any of its officers or staff for anything which is done in good faith under this Act or rules made thereunder for which any person is or likely to be affected.

29. **Power to make rules.**—For the purposes of this Act, the Government may, by notification in the official Gazette, make rules.

30. **Publication of an English Text of the Act.**—(1) After the commencement of this Act, the Government shall, as soon as possible, by notification in the official Gazette, publish an Authentic English Text of this Act.

(2) In case of any conflict between the Bangla Text and the English Text, the Bangla Text shall prevail.

31. **Repeal and savings.**—(1) The Money Laundering Prevention Act, 2009 (Act No. VIII of 2009) and the Money Laundering Prevention Ordinance, 2012 (Ordinance No. II of 2012), hereinafter referred to as the Act and Ordinance, are hereby repealed.

(2) Notwithstanding such repeal, any action taken or any case filed or any proceeding taken under the Act and Ordinance which are pending shall be disposed of in such a manner as if it had been filed and taken under this Act.

(3) Notwithstanding such repeal, if any offence committed or remains under investigation or trial under the Foreign Exchange Regulation Act, 1947 (Act No. VII of 1947) and the Act and Ordinance, such offences shall be disposed of in such a manner as if it had been filed and taken under this Act.

Md. Mahfuzur Rahman
Acting Secretary.

বাংলাদেশ



গেজেট

অতিরিক্ত সংখ্যা

কর্তৃপক্ষ কর্তৃক প্রকাশিত

বুধবার, জুন ১২, ২০১৩

বাংলাদেশ জাতীয় সংসদ

ঢাকা, ১২ জুন, ২০১৩/২৯ জ্যৈষ্ঠ, ১৪২০

সংসদ কর্তৃক গৃহীত নিম্নলিখিত আইনটি ১২ জুন, ২০১৩ (২৯ জ্যৈষ্ঠ, ১৪২০) তারিখে রাষ্ট্রপতির সম্মতি লাভ করিয়াছে এবং এতদ্বারা এই আইনটি সর্বসাধারণের অবগতির জন্য প্রকাশ করা যাইতেছে :—

২০১৩ সনের ২২ নং আইন

সন্ত্রাস বিরোধী আইন, ২০০৯ (২০০৯ সনের ১৬ নং আইন) এর অধিকতর সংশোধনকল্পে প্রণীত আইন

যেহেতু নিম্নবর্ণিত উদ্দেশ্যসমূহ পূরণকল্পে সন্ত্রাস বিরোধী আইন, ২০০৯ (২০০৯ সনের ১৬ নং আইন) এর অধিকতর সংশোধন করা সমীচীন ও প্রয়োজনীয়;

সেহেতু এতদ্বারা নিম্নরূপ আইন করা হইল:—

১। সর্বাঙ্গিক শিরোনাম।—এই আইন সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১৩ নামে অভিহিত হইবে।

২। ২০০৯ সনের ১৬ নং আইনের ধারা ১ এর সংশোধন।—সন্ত্রাস বিরোধী আইন, ২০০৯ (২০০৯ সনের ১৬ নং আইন), অতঃপর উক্ত আইন বলিয়া উল্লিখিত, এর ধারা ১ এর উপ-ধারা (২) এর পরিবর্তে নিম্নরূপ উপ-ধারা (২) প্রতিস্থাপিত হইবে, যথা:—

“(২) সমগ্র বাংলাদেশে ইহার প্রয়োগ হইবে, এবং যেখানেই অবস্থান করুক না কেন, বাংলাদেশে নিবন্ধিত জাহাজ বা বিমানে অবস্থানকারীর ক্ষেত্রেও, ইহা প্রযোজ্য হইবে।”।

(৪৩৩৫)

মূল্য : টাকা ২৪.০০

৩। ২০০৯ সনের ১৬ নং আইনের ধারা ২ এর সংশোধন।—উক্ত আইনের ধারা ২ এর—

(ক) দফা (৩) এর পর নিম্নরূপ একটি নূতন দফা (৩ক) সন্নিবেশিত হইবে, যথা:—

“(৩ক) ‘কনভেনশন’ অর্থ বাংলাদেশ সরকার কর্তৃক যথাযথভাবে অনুসমর্থিত জাতিসংঘ কনভেনশন, ট্রিটি ও প্রটোকলসমূহ, যাহা এই আইনের তফসিল ১ এ অন্তর্ভুক্ত করা হইয়াছে, এবং বাংলাদেশ সরকার কর্তৃক, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, সময় সময় তফসিল ১ এ অন্তর্ভুক্ত হইতে পারে এইরূপ জাতিসংঘ কনভেনশন, ট্রিটি ও প্রটোকল;”;

(খ) দফা (১১) এর পর নিম্নরূপ একটি নূতন দফা (১১ক) সন্নিবেশিত হইবে, যথা:—

“(১১ক) ‘বিদেশী নাগরিক’ অর্থ Foreigners Act, 1946 (Act No. XXXI of 1946) এর section 2 (a) তে সংজ্ঞায়িত ‘foreigner’;”;

(গ) দফা (১৪) এর পরিবর্তে নিম্নরূপ দফা (১৪) প্রতিস্থাপিত হইবে, যথা:—

“(১৪) ‘সম্পত্তি’ অর্থ দেশের অভ্যন্তরে বা বাহিরে অবস্থিত—

(অ) কোন বস্ত্রগত বা অবস্ত্রগত, স্থাবর বা অস্থাবর, দৃশ্যমান বা অদৃশ্যমান যে কোন প্রকৃতির তহবিল বা সম্পদ, উহা যেভাবেই অর্জিত হউক না কেন, এবং ইলেকট্রনিক বা ডিজিটালসহ যে কোন ধরনের আইনি দলিল বা ইনস্ট্রুমেন্ট যাহা উক্ত তহবিল বা সম্পদের মালিকানা স্বত্ব বা মালিকানা স্বত্বের স্বার্থ নির্দেশ করে, এবং উক্ত তহবিল বা সম্পদ হইতে প্রাপ্ত বা উদ্ধৃত কোন মুনাফা, ডিভিডেন্ড বা অন্য কোন আয় বা মূল্যও ইহার অন্তর্ভুক্ত হইবে;

(আ) নগদ অর্থ বা স্থাবর বা অস্থাবর, দৃশ্যমান বা অদৃশ্যমান যে কোন প্রকৃতির আর্থিক পরিসম্পদ বা আর্থিক উৎস, উহা যেভাবেই অর্জিত হউক না কেন, এবং ইলেকট্রনিক বা ডিজিটালসহ যে কোন ধরনের আইনি দলিল বা ইনস্ট্রুমেন্ট যাহা উক্ত তহবিল বা অন্যান্য সম্পদের মালিকানা স্বত্ব বা মালিকানা স্বত্বের স্বার্থ নির্দেশ করে এবং ব্যাংক ক্রেডিট, ট্রাভেলারস্ চেক, ব্যাংক চেক, মানি অর্ডার, শেয়ার, সিকিউরিটি, বন্ড, ড্রাফট বা স্বপত্র এবং উক্ত তহবিল বা সম্পদ হইতে উদ্ধৃত বা সৃষ্ট কোন মুনাফা, ডিভিডেন্ড বা অন্য কোন আয় বা মূল্য ইহার অন্তর্ভুক্ত হইবে, তবে উহাতে সীমাবদ্ধ করিবে না;”;

(ঘ) দফা (১৪) এর পর নিম্নরূপ ছয়টি নূতন দফা যথাক্রমে (১৪ক), (১৪খ), (১৪গ) ও (১৪ঘ) সন্নিবেশিত হইবে, যথা:—

“(১৪ক) ‘সম্ভাসী ব্যক্তি’ অর্থ কোন ‘স্বাভাবিক ব্যক্তি (natural person) যিনি ধারা ৬(১), ১০, ১১, ১২ বা ১৩ এর অধীন কোন অপরাধ সংঘটন করেন;

(১৪খ) ‘সম্ভাসী সত্তা’ অর্থ তফসিল-২ এ উল্লিখিত কোন সত্তা বা এই আইনের ধারা ৬(১), ১০, ১১, ১২ বা ১৩ এর অধীন কোন অপরাধ সংঘটন করে এইরূপ কোন সত্তা;

(১৪গ) 'সন্ত্রাসী সম্পত্তি' অর্থ এইরূপ কোন সম্পত্তি যাহা—

(অ) এই আইনের অধীন কোন সন্ত্রাসী কার্য সংঘটন বা কোন বিদেশী রাষ্ট্রের আইনের অধীন অনুরূপ সমশ্রেণীর অপরাধ সংঘটনে ব্যবহৃত হইয়াছে বা হইতেছে, বা হইবার অভিপ্রায় রহিয়াছে;

(আ) কোন সন্ত্রাসী কার্যের সহিত সম্পৃক্ত;

(ই) কোন সন্ত্রাসী কার্য সংঘটনের মাধ্যমে প্রত্যক্ষ বা পরোক্ষভাবে উদ্ধৃত বা অর্জিত;

(ঈ) সন্ত্রাসী কার্যের উদ্দেশ্যে অথবা কোন সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তাকে সমর্থনের উদ্দেশ্যে ব্যবহার করিবার অভিপ্রায়ে, প্রত্যক্ষ বা পরোক্ষ যে কোন উপায়ে সংগৃহীত হইয়াছে;

(উ) প্রত্যক্ষ বা পরোক্ষভাবে কোন সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তার মালিকানাধীন বা নিয়ন্ত্রণাধীন এবং কোন সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তার পক্ষে বা নির্দেশনা অনুসারে কাজ করে এইরূপ ব্যক্তি বা সত্তার সম্পত্তিসহ অনুরূপ ব্যক্তি ও সহযোগী ব্যক্তি বা সত্তার মালিকানাধীন বা প্রত্যক্ষ বা পরোক্ষভাবে নিয়ন্ত্রণাধীন সম্পত্তি হইতে উদ্ধৃত বা সৃষ্ট তহবিল;

(১৪ঘ) 'সমবায় সমিতি' অর্থ সমবায় সমিতি আইন, ২০০১ (২০০১ সনের ৪৭ নং আইন) এর অধীন অনুমোদিত ও নিবন্ধিত কোন প্রতিষ্ঠান;"

(৩) দফা (১৬) এর উপ-দফা (২) এর পরিবর্তে নিম্নরূপ উপ-দফা (২) প্রতিস্থাপিত হইবে, যথা:—

" (২) যেই লেনদেন সম্পর্কে এইরূপ ধারণা হয় যে,—

(ক) উহা এই আইনের অধীন কোন অপরাধ হইতে উদ্ধৃত;

(খ) উহা কোন সন্ত্রাসী কার্যে অর্থায়ন বা কোন সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তাকে অর্থায়নের সহিত সম্পর্কযুক্ত;"

(৩) দফা (২৪) এ উল্লিখিত 'সমবায় সমিতি আইন, ২০০১ (২০০১ সনের ৪৭ নং আইন)' শব্দগুলি, কমাগুলি, সংখ্যাগুলি এবং বন্ধনি বিলুপ্ত হইবে;

(৪) দফা (২৫) এ উল্লিখিত '২০০৯' সংখ্যাটির পরিবর্তে '২০১২' সংখ্যাটি প্রতিস্থাপিত হইবে;

(৫) দফা ৩০ এ উল্লিখিত "গোষ্ঠীর" শব্দটির পরিবর্তে "জনগোষ্ঠীর" শব্দটি প্রতিস্থাপিত হইবে।

৪। ২০০৯ সনের ১৬ নং আইনের ধারা ৫ এর সংশোধন।—উক্ত আইনের ধারা ৫ এর উপ-ধারা (২) এর পর নিম্নরূপ একটি নূতন উপ-ধারা (৩) সংযোজিত হইবে, যথা:—

“(৩) যদি কোন ব্যক্তি কোন বিদেশী রাষ্ট্রে অপরাধ সংঘটন করিয়া বাংলাদেশে আশ্রয় গ্রহণ করে, যাহা বাংলাদেশে সংঘটিত হইলে এই আইনের অধীন শাস্তিযোগ্য হইত, তাহা হইলে উক্ত অপরাধ বাংলাদেশে সংঘটিত হইয়াছে বলিয়া গণ্য হইবে এবং যদি তাহাকে উক্ত অপরাধ বিচারের এখতিয়ার সম্পন্ন কোন বিদেশী রাষ্ট্রে বহিসমর্পণ করা না যায়, তাহা হইলে উক্ত ব্যক্তি ও অপরাধের ক্ষেত্রে এই আইনের বিধানাবলী প্রযোজ্য হইবে।”।

৫। ২০০৯ সনের ১৬ নং আইনের ধারা ৬ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ৬ এর পরিবর্তে নিম্নরূপ ধারা ৬ প্রতিস্থাপিত হইবে, যথা:—

“৬। সন্ত্রাসী কার্য।—(১) যদি কোন ব্যক্তি, সত্তা বা বিদেশী নাগরিক—

(ক) বাংলাদেশের অখণ্ডতা, সংহতি, জননিরাপত্তা বা সার্বভৌমত্ব বিপন্ন করিবার জন্য জনসাধারণ বা জনসাধারণের কোন অংশের মধ্যে আতঙ্ক সৃষ্টির মাধ্যমে সরকার বা কোন সত্তা বা কোন ব্যক্তিকে কোন কার্য করিতে বা করা হইতে বিরত রাখিতে বাধ্য করিবার উদ্দেশ্যে—

(অ) অন্য কোন ব্যক্তিকে হত্যা, গুরুতর আঘাত, আটক বা অপহরণ করে বা করিবার প্রচেষ্টা গ্রহণ করে; অথবা

(আ) অন্য কোন ব্যক্তিকে হত্যা, গুরুতর জখম, আটক বা অপহরণ করার জন্য অপর কোন ব্যক্তিকে ষড়যন্ত্র বা সহায়তা বা প্ররোচিত করে; অথবা

(ই) অন্য কোন ব্যক্তি, সত্তা বা প্রজাতন্ত্রের কোন সম্পত্তির ক্ষতি সাধন করে বা করিবার প্রচেষ্টা গ্রহণ করে; অথবা

(ঈ) অন্য কোন ব্যক্তি, সত্তা বা প্রজাতন্ত্রের কোন সম্পত্তির ক্ষতি সাধন করিবার উদ্দেশ্যে ষড়যন্ত্র বা সহায়তা বা প্ররোচিত করে; অথবা

(উ) উপ-দফা (অ), (আ), (ই) বা (ঈ) এর উদ্দেশ্য সাধনকল্পে কোন বিস্ফোরক দ্রব্য, দাহ্য পদার্থ ও আগ্নেয়াস্ত্র ব্যবহার করে বা নিজ দখলে রাখে;

(খ) অন্য কোন রাষ্ট্রের নিরাপত্তা বিঘ্নিত বা উহার সম্পত্তি বিনষ্ট করিবার অভিপ্রায়ে দফা (ক) এর উপ-দফা (অ), (আ), (ই), (ঈ) বা (উ) এর অনুরূপ কোন অপরাধ সংঘটন করে বা সংঘটনের প্রচেষ্টা করে বা উক্তরূপ অপরাধ সংঘটনের জন্য প্ররোচিত, ষড়যন্ত্র বা সহায়তা করে;

(গ) কোন আন্তর্জাতিক সংস্থাকে কোন কার্য করিতে বা করা হইতে বিরত রাখিবার জন্য দফা (ক) এর উপ-দফা (অ), (আ), (ই), (ঈ) বা (উ) এর অনুরূপ কোন অপরাধ সংঘটন করে বা সংঘটনের উদ্যোগ গ্রহণ করে বা উক্তরূপ অপরাধ সংঘটনের জন্য প্ররোচিত, ষড়যন্ত্র বা সহায়তা করে;

(ঘ) জ্ঞাতসারে কোন সন্ত্রাসী সম্পত্তি ব্যবহার করে বা অধিকারে রাখে;

(ঙ) এই আইনের তফসিল-১ এ অন্তর্ভুক্ত জাতিসংঘ কনভেনশনে বর্ণিত কোন অপরাধ করিতে সহায়তা, প্ররোচিত বা ষড়যন্ত্র করে বা সংঘটন করে বা সংঘটন করিবার প্রচেষ্টা করে;

(চ) কোন সশস্ত্র সংঘাতময় স্বন্দুর বৈরি পরিস্থিতিতে (hostilities in a situation of armed conflict) সক্রিয় অংশগ্রহণ করেন নাই এইরূপ কোন বেসামরিক, কিংবা অন্য কোন ব্যক্তির মৃত্যু ঘটাইবার বা মারাত্মক শারীরিক জখম ঘটাইবার অভিপ্রায়ে এইরূপ কোন কার্য করে, যাহার উদ্দেশ্য, উহার প্রকৃতিগত বা ব্যক্তির কারণে, কোন জনগোষ্ঠীকে ভীতি প্রদর্শন বা অন্য কোন সরকার বা রাষ্ট্রে বা কোন আন্তর্জাতিক সংস্থাকে কোন কার্য করিতে বা কোন কার্য করা হইতে বিরত থাকিতে বাধ্য করে;

তাহা হইলে উক্ত ব্যক্তি, সত্তা বা বিদেশী নাগরিক "সন্ত্রাসী কার্য" সংঘটনের অপরাধ করিয়াছে বলিয়া গণ্য হইবে।

(২) যদি কোন ব্যক্তি বা বিদেশী নাগরিক উপ-ধারা (১) এর দফা (ক) এর—

(অ) উপ-দফা (অ) এর অধীন কোন অপরাধ সংঘটন করেন তাহা হইলে তিনি মৃত্যুদণ্ড বা যাবজ্জীবন কারাদণ্ডে দণ্ডিত হইবেন এবং উহার অতিরিক্ত অর্ধদণ্ড আরোপ করা যাইবে;

(আ) উপ-দফা (আ) এর অধীন কোন অপরাধ সংঘটন করেন তাহা হইলে উক্ত অপরাধের নির্ধারিত শাস্তি যদি মৃত্যুদণ্ড হয় সেইক্ষেত্রে তিনি যাবজ্জীবন কারাদণ্ড বা অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অন্যান ৪ (চার) বৎসরের সশ্রম কারাদণ্ড এবং অর্ধদণ্ডে দণ্ডিত হইবেন;

(ই) উপ-দফা (ই) এর অধীন কোন অপরাধ সংঘটন করেন তাহা হইলে তিনি যাবজ্জীবন কারাদণ্ড বা অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অন্যান ৪ (চার) বৎসরের সশ্রম কারাদণ্ড এবং অর্ধদণ্ডে দণ্ডিত হইবেন;

(ঈ) উপ-দফা (ঈ) এর অধীন কোন অপরাধ সংঘটন করেন তাহা হইলে তিনি অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অন্যান ৪ (চার) বৎসরের সশ্রম কারাদণ্ড এবং অর্ধদণ্ডে দণ্ডিত হইবেন;

(উ) উপ-দফা (উ) এর অধীন কোন অপরাধ সংঘটন করেন তাহা হইলে তিনি যাবজ্জীবন কারাদণ্ড বা অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অন্যান ৪ (চার) বৎসরের সশ্রম কারাদণ্ড এবং অর্ধদণ্ডে দণ্ডিত হইবেন।

(৩) যদি কোন ব্যক্তি বা বিদেশী নাগরিক উপ-ধারা (১) এর দফা (খ), (গ), (ঘ), (ঙ) বা (চ) এর অধীন কোন অপরাধ সংঘটন করেন তাহা হইলে তিনি যাবজ্জীবন কারাদণ্ড বা অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অন্যান ৪ (চার) বৎসরের সশ্রম কারাদণ্ড এবং অর্ধদণ্ডে দণ্ডিত হইবেন।

(৪) যদি কোন সত্তা সন্ত্রাসী কার্য সংঘটন করে, তাহা হইলে—

(ক) উক্ত সত্তার বিরুদ্ধে ধারা ১৮ অনুসারে পদক্ষেপ গ্রহণ করা যাইবে এবং উহার অতিরিক্ত উক্ত অপরাধের সহিত সংশ্লিষ্ট সম্পত্তির মূল্যের তিনগুণ পরিমাণ অর্থ বা ৫০ (পঞ্চাশ) লক্ষ টাকা, যাহা অধিক, অর্ধদণ্ড আরোপ করা যাইবে; এবং

(খ) উক্ত সত্তার প্রধান, তিনি চেয়ারম্যান, ব্যবস্থাপনা পরিচালক, প্রধান নির্বাহী বা অন্য যে কোন নামে অভিহিত হউক না কেন, অনুর্ধ্ব ২০ (বিশ) বৎসর ও অনূন্য ৪ (চার) বৎসরের সশ্রম কারাদণ্ডে দণ্ডিত হইবেন এবং উহার অতিরিক্ত উক্ত অপরাধের সহিত সম্পৃক্ত সম্পত্তির মূল্যের দ্বিগুণ পরিমাণ অর্থ বা ২০ (বিশ) লক্ষ টাকা, যাহা অধিক, অর্থদণ্ড আরোপ করা যাইবে, যদি না তিনি প্রমাণ করিতে সমর্থ হন যে, উক্তরূপ অপরাধ তাহার অজ্ঞাতসারে সংঘটিত হইয়াছিল বা উহার সংঘটন নিবৃত্ত করিবার জন্য তিনি সর্বাঙ্গিক প্রচেষ্টা গ্রহণ করিয়াছিলেন।”।

৬। ২০০৯ সনের ১৬ নং আইনের ধারা ৭ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ৭ এর পরিবর্তে নিম্নরূপ ধারা ৭ প্রতিস্থাপিত হইবে, যথা:—

“৭। সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত অপরাধ।—(১) যদি কোন ব্যক্তি বা সত্তা স্বেচ্ছায়, বৈধ বা অবৈধ উৎস হইতে, প্রত্যক্ষ বা পরোক্ষ যে কোনভাবে এই অভিপ্রায়ে অর্থ, সেবা বা অন্য যে কোন সম্পত্তি সরবরাহ, গ্রহণ, সংগ্রহ বা উহার এইরূপ ব্যবস্থা করে যে, উহার সম্পূর্ণ বা অংশবিশেষ—

(ক) সন্ত্রাসী কার্য পরিচালনায় ব্যবহৃত হইবে; বা

(খ) সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তা কর্তৃক যে কোন উদ্দেশ্যে ব্যবহৃত হইবে, অথবা ব্যবহৃত হইতে পারে মর্মে জ্ঞাত থাকে;

তাহা হইলে উক্ত ব্যক্তি বা সত্তা সন্ত্রাসী কার্যে অর্থায়নের অপরাধ সংঘটন করিয়াছে বলিয়া গণ্য হইবে।

(২) সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত অপরাধে দোষী সাব্যস্তকরণের ক্ষেত্রে উপ-ধারা (১) এ উল্লিখিত অর্থ, সেবা বা অন্য যে কোন সম্পত্তি প্রকৃতই কোন সন্ত্রাসী কার্য সম্পাদনের বা পরিচালনার ক্ষেত্রে বা সন্ত্রাসী কার্য সম্পাদনের প্রচেষ্টার ক্ষেত্রে ব্যবহৃত হইয়াছে কিনা বা কোন সুনির্দিষ্ট সন্ত্রাসী কার্যের সহিত সম্পর্কযুক্ত ছিল কিনা, উহার উপর নির্ভর করিবে না।

(৩) যদি কোন ব্যক্তি উপ-ধারা (১) এ উল্লিখিত কোন অপরাধে দোষী সাব্যস্ত হন, তাহা হইলে তিনি অনুর্ধ্ব ২০ (বিশ) বৎসর ও অনূন্য ৪ (চার) বৎসরের সশ্রম কারাদণ্ডে দণ্ডিত হইবেন, এবং উহার অতিরিক্ত উক্ত অপরাধের সহিত সংশ্লিষ্ট সম্পত্তির মূল্যের দ্বিগুণ পরিমাণ অর্থ বা ১০ (দশ) লক্ষ টাকা, যাহা অধিক, অর্থদণ্ড আরোপ করা যাইবে।

(৪) যদি কোন সত্তা উপ-ধারা (১) এ উল্লিখিত কোন অপরাধে দোষী সাব্যস্ত হয়, তাহা হইলে—

(ক) উক্ত সত্তার বিরুদ্ধে ধারা ১৮ অনুসারে পদক্ষেপ গ্রহণ করা যাইবে এবং উহার অতিরিক্ত উক্ত অপরাধের সহিত সংশ্লিষ্ট সম্পত্তির মূল্যের তিনগুণ পরিমাণ অর্থ বা ৫০ (পঞ্চাশ) লক্ষ টাকা, যাহা অধিক, অর্থদণ্ড আরোপ করা যাইবে; এবং

(খ) উক্ত সত্তার প্রধান, তিনি চেয়ারম্যান, ব্যবস্থাপনা পরিচালক, প্রধান নির্বাহী বা অন্য যে কোন নামে অভিহিত হউক না কেন, অনুর্ধ্ব ২০ (বিশ) বৎসর ও অনূন্য ৪ (চার) বৎসরের সশ্রম কারাদণ্ডে দণ্ডিত হইবেন এবং উহার অতিরিক্ত উক্ত অপরাধের সহিত সম্পৃক্ত সম্পত্তির মূল্যের দ্বিগুণ পরিমাণ অর্থ বা ২০ (বিশ) লক্ষ টাকা, যাহা অধিক, অর্থদণ্ড আরোপ করা যাইবে, যদি না তিনি প্রমাণ করিতে সমর্থ হন যে, উক্তরূপ অপরাধ তাহার অজ্ঞাতসারে সংঘটিত হইয়াছিল বা উহার সংঘটন নিবৃত্ত করিবার জন্য তিনি সর্বাঙ্গিক প্রচেষ্টা গ্রহণ করিয়াছিলেন।”।

৭। ২০০৯ সনের ১৬ নং আইনের ধারা ৮ এর সংশোধন।—উক্ত আইনের ধারা ৮ এর—

- (ক) উপাত্ত টীকায় উল্লিখিত 'সংগঠনের' শব্দটির পরিবর্তে 'সত্তার' শব্দটি প্রতিস্থাপিত হইবে; এবং
- (খ) মূল অংশে উল্লিখিত 'সংগঠনের' শব্দটির পরিবর্তে 'সত্তার' শব্দটি প্রতিস্থাপিত হইবে।

৮। ২০০৯ সনের ১৬ নং আইনের ধারা ৯ এর সংশোধন।—উক্ত আইনের ধারা ৯ এর—

- (ক) উপাত্ত টীকায় উল্লিখিত 'সংগঠন' শব্দটির পরিবর্তে 'সত্তা' শব্দটি প্রতিস্থাপিত হইবে;
- (খ) উপ-ধারা (১) এ দুইবার উল্লিখিত 'সংগঠনকে' শব্দটির পরিবর্তে উভয় স্থানে 'সত্তাকে' শব্দটি প্রতিস্থাপিত হইবে; এবং
- (গ) উপ-ধারা (২) এ উল্লিখিত 'সংগঠনের' শব্দটির পরিবর্তে 'সত্তার' শব্দটি প্রতিস্থাপিত হইবে।

৯। ২০০৯ সনের ১৬ নং আইনের ধারা ১০ এর সংশোধন।—উক্ত আইনের ধারা ১০ এ উল্লিখিত 'এই আইনের অধীন অপরাধ সংঘটনের যড়যন্ত্র করেন, তাহা হইলে' শব্দগুলি ও কমার পর 'তিনি অপরাধ করিয়াছেন বলিয়া গণ্য হইবেন এবং' শব্দগুলি সন্নিবেশিত হইবে এবং 'পাঁচ' শব্দটির পরিবর্তে "৪ (চার)" শব্দ, সংখ্যা ও বন্ধনী প্রতিস্থাপিত হইবে।

১০। ২০০৯ সনের ১৬ নং আইনের ধারা ১১ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ১১ এর পরিবর্তে নিম্নরূপ ধারা ১১ প্রতিস্থাপিত হইবে, যথা:—

"১১। অপরাধ সংঘটনের প্রচেষ্টার (attempt) শাস্তি।—যদি কোন ব্যক্তি বা সত্তা এই আইনের অধীন কোন অপরাধ সংঘটনের প্রচেষ্টা করে, তাহা হইলে উক্ত ব্যক্তি বা সত্তা অপরাধ সংঘটন করিয়াছেন বলিয়া গণ্য হইবে এবং উক্ত ব্যক্তি বা উক্ত সত্তার প্রধান, তিনি চেয়ারম্যান, ব্যবস্থাপনা পরিচালক, প্রধান নির্বাহী বা অন্য যে কোন নামে অভিহিত হউক না কেন, উক্ত অপরাধের জন্য নির্ধারিত সর্বোচ্চ শাস্তির দুই-তৃতীয়াংশ মেয়াদের যে কোন কারাদণ্ডে অথবা অর্থদণ্ডে, অথবা উভয় দণ্ডে দণ্ডিত হইবেন, এবং যদি উক্ত অপরাধের জন্য নির্ধারিত শাস্তি মৃত্যুদণ্ড হয়, তাহা হইলে উক্ত অপরাধের শাস্তি হইবে যাবজ্জীবন কারাদণ্ড অথবা অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অন্যান্য ৪ (চার) বৎসরের সশ্রম কারাদণ্ড, এবং উহার অতিরিক্ত সংশ্লিষ্ট সত্তার বিরুদ্ধে ধারা ১৮ অনুসারে ব্যবস্থা গ্রহণ করা যাইবে।"

১১। ২০০৯ সনের ১৬ নং আইনের ধারা ১২ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ১২ এর পরিবর্তে নিম্নরূপ ধারা ১২ প্রতিস্থাপিত হইবে, যথা:—

"১২। অপরাধ সংঘটনে সাহায্য ও সহায়তার (aid and abetment) শাস্তি।—যদি কোন ব্যক্তি বা সত্তা এই আইনের অধীন কোন অপরাধ সংঘটনে—

- (ক) সাহায্য বা সহায়তা করে; বা
- (খ) সহায়তাকারী হিসাবে (as an accomplice) অংশগ্রহণ করে; বা
- (গ) অন্যদেরকে সংগঠিত বা পরিচালনা করে; বা
- (ঘ) অবদান রাখে;

তাহা হইলে উক্ত ব্যক্তি বা সত্তা অপরাধ সংঘটন করিয়াছেন বলিয়া গণ্য হইবে এবং উক্ত ব্যক্তি বা উক্ত সত্তার প্রধান, তিনি চেয়ারম্যান, ব্যবস্থাপনা পরিচালক, প্রধান নির্বাহী বা অন্য যে কোন নামে অভিহিত হউক না কেন, উক্ত অপরাধের জন্য নির্ধারিত সর্বোচ্চ শাস্তির দুই-তৃতীয়াংশ মেয়াদের যে কোন কারাদণ্ডে, অথবা অর্ধদণ্ডে, অথবা উভয় দণ্ডে দণ্ডিত হইবেন; এবং যদি উক্ত অপরাধের জন্য নির্ধারিত শাস্তি মৃত্যুদণ্ড হয়, তাহা হইলে উক্ত অপরাধের শাস্তি হইবে যাবজ্জীবন কারাদণ্ড অথবা অনূর্ধ্ব ১৪ (চৌদ্দ) বৎসর ও অনূন ৪ (চার) বৎসরের সশ্রম কারাদণ্ড, এবং উহার অতিরিক্ত সংশ্লিষ্ট সত্তার বিরুদ্ধে ধারা ১৮ অনুসারে ব্যবস্থা গ্রহণ করা যাইবে।”।

১২। ২০০৯ সনের ১৬ নং আইনের ধারা ১৩ এর সংশোধন।—উক্ত আইনের ধারা ১৩ এ উল্লিখিত ‘সংগঠনকে’ শব্দটির পরিবর্তে ‘সত্তাকে’ শব্দটি, ‘সংগঠন’ শব্দটির পরিবর্তে ‘সত্তা’ শব্দটি এবং ‘পাঁচ’ শব্দটির পরিবর্তে ‘৪ (চার)’ শব্দ, সংখ্যা ও বন্ধনী প্রতিস্থাপিত হইবে।

১৩। ২০০৯ সনের ১৬ নং আইনের ধারা ১৪ এর সংশোধন।—উক্ত আইনের ধারা ১৪ এর—

(ক) উপাত্ত টীকায় উল্লিখিত “অপরাধীকে আশ্রয় প্রদান” শব্দগুলির পরিবর্তে “অপরাধীকে আশ্রয় প্রদানের শাস্তি” শব্দগুলি প্রতিস্থাপিত হইবে; এবং

(খ) উপ-ধারা (২) এর পর নিম্নরূপ একটি নূতন উপ-ধারা (৩) সংযোজিত হইবে, যথা:—

“(৩) যেক্ষেত্রে কোন সত্তা কর্তৃক আশ্রয় প্রদানের অপরাধ সংঘটিত হয়, সেইক্ষেত্রে উহার প্রধান হিসাবে দায়িত্ব পালনকারী চেয়ারম্যান, ব্যবস্থাপনা পরিচালক, প্রধান নির্বাহী বা অন্য কোন নামের পদধারীর প্রতি উপ-ধারা (১) এর বিধানাবলী প্রযোজ্য হইবে, যদি না তিনি প্রমাণ করিতে সমর্থ হন যে, উক্তরূপ অপরাধ তাহার অজ্ঞাতসারে সংঘটিত হইয়াছিল বা উহার সংঘটন নিবৃত্ত করিবার জন্য তিনি সর্বাঙ্গিক প্রচেষ্টা গ্রহণ করিয়াছিলেন।”।

১৪। ২০০৯ সনের ১৬ নং আইনের ধারা ১৫ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ১৫ এর পরিবর্তে নিম্নরূপ ধারা ১৫ প্রতিস্থাপিত হইবে, যথা:—

“১৫। বাংলাদেশ ব্যাংকের ক্ষমতা।—(১) এই আইনের অধীন কোন অপরাধ সংঘটনের উদ্দেশ্যে কোন রিপোর্ট প্রদানকারী সংস্থার মাধ্যমে লেনদেন প্রতিরোধ ও সনাক্ত করিতে বাংলাদেশ ব্যাংক প্রয়োজনীয় পদক্ষেপ গ্রহণ করিতে পারিবে এবং এতদুদ্দেশ্যে উহার নিম্নবর্ণিত ক্ষমতা ও কর্তৃত্ব থাকিবে, যথা:—

(ক) কোন রিপোর্ট প্রদানকারী সংস্থা হইতে সন্দেহজনক লেনদেন সম্পর্কিত প্রতিবেদন তলব করা, উহা বিশ্লেষণ বা পুনরীক্ষণ করা এবং বিশ্লেষণ বা পুনরীক্ষণের উদ্দেশ্যে উহার সহিত সম্পর্কিত অতিরিক্ত তথ্য সংগ্রহ করা এবং উহার রেকর্ড বা ড্যাটাভেজ সংরক্ষণ করা এবং ক্ষেত্রমত, প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য পুলিশ বা সংশ্লিষ্ট অন্যান্য আইন প্রয়োগকারী সংস্থাকে উক্ত তথ্য সরবরাহ বা রিপোর্ট প্রদান করা;

(খ) কোন লেনদেন সন্ত্রাসী কার্যের সহিত সম্পৃক্ত মর্মে সন্দেহ করিবার যুক্তিসঙ্গত কারণ থাকিলে, সংশ্লিষ্ট রিপোর্ট প্রদানকারী সংস্থাকে উক্ত লেনদেনের হিসাব অনধিক ৩০ (ত্রিশ) দিনের জন্য স্থগিত বা অবরুদ্ধ রাখিবার উদ্দেশ্যে লিখিত আদেশ জারি করা এবং এইরূপে উক্ত হিসাবের লেনদেন সম্পর্কিত সঠিক তথ্য উদ্ঘাটনের প্রয়োজন দেখা দিলে লেনদেন স্থগিত বা অবরুদ্ধ রাখিবার মেয়াদ অতিরিক্ত ৩০ (ত্রিশ) দিন করিয়া সর্বোচ্চ ৬ (ছয়) মাস বর্ধিত করা;

- (গ) রিপোর্ট প্রদানকারী সংস্থার কার্যক্রম পরিবীক্ষণ ও তদারক করা;
- (ঘ) সন্ত্রাসী কার্যে এবং ব্যাপক ধ্বংসাত্মক অস্ত্রের (weapons of mass destruction, WMD) বিস্তারে অর্থ যোগান প্রতিহত করিবার উদ্দেশ্যে প্রতিরোধমূলক পদক্ষেপ গ্রহণে রিপোর্ট প্রদানকারী সংস্থাসমূহকে নির্দেশ প্রদান করা;
- (ঙ) রিপোর্ট প্রদানকারী সংস্থা কর্তৃক নির্দেশ প্রতিপালন পর্যবেক্ষণ করা এবং এই আইনের যে কোন উদ্দেশ্য পূরণকল্পে রিপোর্ট প্রদানকারী সংস্থাসমূহকে সরেজমিনে পরিদর্শন করা; এবং
- (চ) সন্দেহজনক লেনদেন সনাক্ত ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের উদ্দেশ্যে রিপোর্ট প্রদানকারী সংস্থাসমূহের কর্মকর্তা ও কর্মচারীগণকে প্রশিক্ষণের ব্যবস্থা করা।

(২) বাংলাদেশ ব্যাংক, সন্ত্রাসী কার্যে অর্থায়নের সহিত সম্পৃক্ত সন্দেহজনক কোন লেনদেনের বিষয়ে কোন রিপোর্ট প্রদানকারী সংস্থা বা উহার গ্রাহককে সনাক্ত করিবার সঙ্গে সঙ্গে উহা পুলিশ বা যথাযথ আইন প্রয়োগকারী সংস্থাকে অবহিত করিবে, এবং অনুসন্ধান ও তদন্ত কার্যে পুলিশ বা সংশ্লিষ্ট আইন প্রয়োগকারী সংস্থাকে প্রয়োজনীয় সকল প্রকার সহযোগিতা প্রদান করিবে।

(৩) অপরাধটি যদি অন্য কোন রাষ্ট্রে সংঘটিত হয় বা অন্য কোন রাষ্ট্রে বিচারাধীন থাকে, তাহা হইলে বাংলাদেশ ব্যাংক উক্ত বিদেশী রাষ্ট্রের অনুরোধের প্রেক্ষিতে বা কোন আন্তর্জাতিক, আঞ্চলিক বা ঐপাক্ষিক চুক্তি, বাংলাদেশ সরকার কর্তৃক অনুসমর্থিত জাতিসংঘের কনভেনশন বা জাতিসংঘের নিরাপত্তা পরিষদ কর্তৃক গৃহীত সংশ্লিষ্ট রেজুলেশনের আওতায় কোন ব্যক্তি বা সত্তার হিসাব জব্দ করিবার উদ্যোগ গ্রহণ করিবে।

(৪) উপ-ধারা (৩) এর অধীন জন্মকৃত অর্থ সংশ্লিষ্ট আদালত কর্তৃক বা সংশ্লিষ্ট চুক্তি, কনভেনশন বা জাতিসংঘের নিরাপত্তা পরিষদ কর্তৃক গৃহীত রেজুলেশনের আওতায় সম্পত্তিযোগ্য হইবে।

(৫) এই আইনের অধীন বাংলাদেশ ব্যাংকের ক্ষমতা ও দায়-দায়িত্ব বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট (বি,এফ,আই,ইউ) কর্তৃক প্রয়োগ ও সম্পাদিত হইবে এবং বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট এই আইনের অধীন কোন তথ্য সরবরাহের অনুরোধ করিলে, সকল সরকারি, আধা-সরকারি, স্বায়ত্তশাসিত সংস্থা বা সংশ্লিষ্ট অন্য কোন প্রতিষ্ঠান বা সংস্থা উহাকে তাহা সরবরাহ করিবে অথবা, ক্ষেত্রমত, স্বপ্রণোদিত হইয়া তথ্য সরবরাহ করিবে।

(৬) বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট, অনুরোধের প্রেক্ষিতে বা, ক্ষেত্রমত, স্বপ্রণোদিত হইয়া সন্ত্রাসী কার্য বা সন্ত্রাসী কার্যে অর্থায়ন সম্পৃক্ত তথ্যাদি অন্য দেশের ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট বা অন্য কোন রাষ্ট্রের অনুরূপ কর্তৃপক্ষকে (counter part) সরবরাহ করিবে।

(৭) সন্ত্রাসী কার্যে অর্থায়নের বিষয়ে তদন্তের স্বার্থে কোন আইন প্রয়োগকারী সংস্থা কর্তৃক কোন ব্যাংকের দলিল বা কোন নথিতে নিম্নবর্ণিত শর্তে প্রবেশাধিকার থাকিবে, যথা:—

- (ক) উপযুক্ত আদালত বা বিশেষ ট্রাইব্যুনালের আদেশক্রমে; অথবা
- (খ) বাংলাদেশ ব্যাংকের অনুমোদনক্রমে।

(৮) যদি কোন রিপোর্ট প্রদানকারী সংস্থা এই ধারার অধীন বাংলাদেশ ব্যাংক কর্তৃক জ্ঞানকৃত নির্দেশনা প্রতিপালনে ব্যর্থ হয় অথবা জ্ঞাতসারে কোন ভুল বা মিথ্যা তথ্য বা বিবরণী সরবরাহ করে, তাহা হইলে উক্ত রিপোর্ট প্রদানকারী সংস্থা বাংলাদেশ ব্যাংক কর্তৃক নির্ধারিত ও নির্দেশিত অনূর্ধ্ব ২৫ (পঁচিশ) লক্ষ টাকা জরিমানা পরিশোধ করিতে বাধ্য থাকিবে এবং বাংলাদেশ ব্যাংক উক্ত সংস্থা বা সংস্থার কোন শাখা, সেবাকেন্দ্র, বুথ বা এজেন্টের বাংলাদেশে কার্যক্রম পরিচালনা বন্ধ করিবার উদ্দেশ্যে উহার নিবন্ধন বা লাইসেন্স স্থগিত করিতে পারিবে অথবা, ক্ষেত্রমত, উক্ত সংস্থার বিরুদ্ধে যথাযথ কার্যকরী ব্যবস্থা গ্রহণের জন্য নিবন্ধনকারী বা লাইসেন্স প্রদানকারী কর্তৃপক্ষকে বিষয়টি সম্পর্কে অবহিত করিবে।

(৯) যদি কোন রিপোর্ট প্রদানকারী সংস্থা বাংলাদেশ ব্যাংক কর্তৃক উপ-ধারা (৮) অনুসারে আরোপিত জরিমানা পরিশোধে ব্যর্থ হয় বা পরিশোধ না করে, তাহা হইলে বাংলাদেশ ব্যাংক উক্ত রিপোর্ট প্রদানকারী সংস্থার নিকট হইতে উক্ত জরিমানার অর্থ উক্ত সংস্থা কর্তৃক অন্য কোন ব্যাংক বা আর্থিক প্রতিষ্ঠান বা বাংলাদেশ ব্যাংকে পরিচালিত হিসাব বিকলনপূর্বক আদায় করিতে পারিবে এবং জরিমানার কোন অংশ অনাদায়ী বা অপরিশোধিত থাকিলে, বাংলাদেশ ব্যাংক, প্রয়োজনে, উহা আদায়ের জন্য সংশ্লিষ্ট আদালতে আবেদন করিতে পারিবে।”

১৫। ২০০৯ সনের ১৬ নং আইনের ধারা ১৬ এর সংশোধন।—উক্ত আইনের ধারা ১৬ এর উপ-ধারা (৩) ও (৪) এর পরিবর্তে নিম্নরূপ উপ-ধারা (৩), (৪) ও (৫) প্রতিস্থাপিত হইবে, যথা:—

“(৩) কোন রিপোর্ট প্রদানকারী সংস্থা উপ-ধারা (১) এর বিধান প্রতিপালনে ব্যর্থ হইলে, উক্ত রিপোর্ট প্রদানকারী সংস্থা বাংলাদেশ ব্যাংক কর্তৃক নির্ধারিত ও নির্দেশিত অনধিক ২৫ (পঁচিশ) লক্ষ টাকা জরিমানা পরিশোধ করিতে বাধ্য থাকিবে এবং বাংলাদেশ ব্যাংক উক্ত সংস্থা বা সংস্থার কোন শাখা, সেবাকেন্দ্র, বুথ বা এজেন্টের বাংলাদেশে কার্যক্রম পরিচালনা বন্ধ করিবার উদ্দেশ্যে নিবন্ধন বা লাইসেন্স স্থগিত করিতে পারিবে অথবা ক্ষেত্রমত, নিবন্ধনকারী বা লাইসেন্স প্রদানকারী কর্তৃপক্ষকে উক্ত সংস্থা বা সংস্থার কোন শাখা, সেবাকেন্দ্র, বুথ বা এজেন্টের বিরুদ্ধে যথাযথ কার্যকরী ব্যবস্থা গ্রহণের নিমিত্ত বিষয়টি সম্পর্কে অবহিত করিবে।

(৪) যদি কোন রিপোর্ট প্রদানকারী সংস্থার পরিচালনা পরিষদ বা, পরিচালনা পরিষদ না থাকিলে, উহার প্রধান নির্বাহী কর্মকর্তা, যে নামেই অভিহিত হউক, উপ-ধারা (২) এর বিধান প্রতিপালনে ব্যর্থ হন, তাহা হইলে পরিচালনা পরিষদের চেয়ারম্যান বা, ক্ষেত্রমত, প্রধান নির্বাহী কর্মকর্তা বাংলাদেশ ব্যাংক কর্তৃক নির্ধারিত ও নির্দেশিত অনধিক ২৫ (পঁচিশ) লক্ষ টাকা জরিমানা পরিশোধ করিতে বাধ্য থাকিবেন এবং বাংলাদেশ ব্যাংক উক্ত ব্যক্তিকে তাহার পদ হইতে অপসারণ করিতে পারিবে বা, ক্ষেত্রমত, উক্ত ব্যক্তির বিরুদ্ধে যথাযথ কার্যকরী ব্যবস্থা গ্রহণের জন্য উপযুক্ত কর্তৃপক্ষকে বিষয়টি সম্পর্কে অবহিত করিবে।

(৫) যদি কোন রিপোর্ট প্রদানকারী সংস্থা উপ-ধারা (৩) এর অধীন বাংলাদেশ ব্যাংক কর্তৃক আরোপিত জরিমানা পরিশোধ করিতে ব্যর্থ হয় বা পরিশোধ না করে, অথবা যদি পরিচালনা পরিষদের চেয়ারম্যান, বা প্রধান নির্বাহী কর্মকর্তা, যে নামেই অভিহিত হউক, উপ-ধারা (৪) এর অধীন বাংলাদেশ ব্যাংক কর্তৃক আরোপিত জরিমানা পরিশোধে ব্যর্থ হন বা পরিশোধ না করেন, তাহা হইলে বাংলাদেশ ব্যাংক উক্ত রিপোর্ট প্রদানকারী সংস্থার নিকট হইতে জরিমানার অর্থ আদায় করিতে পারিবে বা উক্ত ব্যক্তি কর্তৃক কোন ব্যাংক, আর্থিক প্রতিষ্ঠান বা বাংলাদেশ ব্যাংকে পরিচালিত তাহার হিসাব বিকলনপূর্বক আদায় করিতে পারিবে এবং উক্ত জরিমানার কোন অংশ অনাদায়ী থাকিলে বা অপরিশোধিত থাকিলে, উহা আদায়ের জন্য বাংলাদেশ ব্যাংক, প্রয়োজনে, সংশ্লিষ্ট আদালতে আবেদন করিতে পারিবে।”

১৬। ২০০৯ সনের ১৬ নং আইনের চতুর্থ অধ্যায় এর শিরোনাম সংশোধন।—উক্ত আইনের চতুর্থ অধ্যায় এর শিরোনামে উল্লিখিত “সন্ত্রাসী সংগঠন” শব্দগুলির পরিবর্তে “নিষিদ্ধ ঘোষণা ও তালিকাভুক্তকরণ এবং জাতিসংঘ নিরাপত্তা পরিষদের রেজুলেশন বাস্তবায়ন” শব্দগুলি প্রতিস্থাপিত হইবে।

১৭। ২০০৯ সনের ১৬ নং আইনের ধারা ১৭ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ১৭ এর পরিবর্তে নিম্নরূপ ধারা ১৭ প্রতিস্থাপিত হইবে, যথা:—

“১৭। সন্ত্রাসী কার্যের সহিত জড়িত ব্যক্তি বা সত্তা।—এই আইনের উদ্দেশ্য পূরণকল্পে, কোন ব্যক্তি বা সত্তা সন্ত্রাসী কার্যের সহিত জড়িত বলিয়া গণ্য হইবে, যদি সেই ব্যক্তি বা উহা—

- (ক) সন্ত্রাসী কার্য সংঘটিত করে বা উক্ত কার্যে অংশগ্রহণ করে;
- (খ) সন্ত্রাসী কার্যের জন্য প্ররোচনা গ্রহণ করে;
- (গ) সন্ত্রাসী কার্য সংঘটনে সাহায্য বা উৎসাহ প্রদান করে;
- (ঘ) সন্ত্রাসী কার্যের সহিত জড়িত কোন সত্তাকে সমর্থন ও সহায়তা প্রদান করে;
- (ঙ) জাতিসংঘের নিরাপত্তা পরিষদের রেজুলেশন নং ১৩৭৩ (UNSCR 1373) এ উল্লিখিত নিম্নবর্ণিত তালিকাভুক্তি বা নিষিদ্ধের মানদণ্ডের (listing criteria) আওতাভুক্ত হয়, যথা:—
 - (১) যদি কোন ব্যক্তি বা সত্তা কোন সন্ত্রাসী কার্য করে বা প্রচেষ্টা গ্রহণ করে বা অংশগ্রহণ করে বা সন্ত্রাসী কার্য সংঘটনে সহযোগিতা করে;
 - (২) তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত যে কোন ব্যক্তি বা সত্তার প্রত্যক্ষ বা পরোক্ষ মালিকানাধীন বা নিয়ন্ত্রানাধীন কোন সত্তা;
 - (৩) তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত যে কোন ব্যক্তি বা সত্তার পক্ষে বা নির্দেশে কাজ করে এইরূপ অন্য কোন ব্যক্তি বা সত্তা।
- (চ) কোন সন্ত্রাসী ব্যক্তিকে আশ্রয় প্রদান করে; অথবা
- (ছ) অন্য কোনভাবে সন্ত্রাসী কার্যের সহিত জড়িত হয়।”।

১৮। ২০০৯ সনের ১৬ নং আইনের ধারা ১৮ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ১৮ এর পরিবর্তে নিম্নরূপ ধারা ১৮ প্রতিস্থাপিত হইবে, যথা:—

“১৮। নিষিদ্ধ ঘোষণা ও তালিকাভুক্তকরণ।—(১) এই আইনের উদ্দেশ্য পূরণকল্পে, সরকার, কোন ব্যক্তি বা সত্তা সন্ত্রাসী কার্যের সহিত জড়িত রহিয়াছে মর্মে যুক্তিসঙ্গত কারণের ভিত্তিতে, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, উক্ত ব্যক্তিকে তফসিলে তালিকাভুক্ত করিতে পারিবে বা সত্তাকে নিষিদ্ধ ঘোষণা ও তফসিলে তালিকাভুক্ত করিতে পারিবে।

(২) সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, যে কোন ব্যক্তি বা সত্তাকে তফসিলে তালিকাভুক্ত করিতে বা তফসিল হইতে বাদ দিতে পারিবে অথবা অন্য কোনভাবে তফসিল সংশোধন করিতে পারিবে।”।

১৯। ২০০৯ সনের ১৬ নং আইনের ধারা ১৯ এর সংশোধন।—উক্ত আইনের ধারা ১৯ এর উপ-ধারা (১) ও উপ-ধারা (২) এ দুইবার উল্লিখিত "সংগঠন" শব্দের পরিবর্তে উভয়স্থানে "ব্যক্তি বা সত্তা" শব্দগুলি প্রতিস্থাপিত হইবে।

২০। ২০০৯ সনের ১৬ নং আইনের ধারা ২০ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ২০ এর পরিবর্তে নিম্নরূপ ধারা ২০ প্রতিস্থাপিত হইবে, যথা:—

"২০। তালিকাভুক্ত ব্যক্তি বা নিষিদ্ধ সত্তার বিরুদ্ধে ব্যবস্থা গ্রহণ।—(১) যদি কোন ব্যক্তিকে ধারা ১৮ এর বিধান অনুসারে তালিকাভুক্ত করা হয় বা কোন সত্তাকে নিষিদ্ধ করা হয়, তাহা হইলে, এই আইনে বর্ণিত অন্যান্য ব্যবস্থা গ্রহণ ছাড়াও সরকার, প্রযোজ্য ক্ষেত্রে, নিম্নবর্ণিত যে কোন পদক্ষেপ গ্রহণ করিবে, যথা:—

- (ক) উক্ত সত্তার কার্যালয়, যদি থাকে, বন্ধ করিয়া দিবে;
- (খ) ব্যাংক এবং অন্যান্য হিসাব, যদি থাকে, অবরুদ্ধ করিবে, এবং উহার সকল সম্পত্তি জব্দ বা আটক করিবে;
- (গ) নিষিদ্ধ সত্তার সদস্যদের দেশ ত্যাগে বাধা নিষেধ আরোপ করিবে;
- (ঘ) সকল প্রকার প্রচারপত্র, পোস্টার, ব্যানার অথবা মুদ্রিত, ইলেক্ট্রনিক, ডিজিটাল বা অন্যান্য উপকরণ বাজেয়াপ্ত করিবে; এবং
- (ঙ) নিষিদ্ধ সত্তা কর্তৃক বা উহার পক্ষে বা সমর্থনে যে কোন প্রেস বিবৃতির প্রকাশনা, মুদ্রণ বা প্রচারণা, সংবাদ সম্মেলন বা জনসম্মুখে বক্তৃতা প্রদান নিষিদ্ধ করিবে।

(২) নিষিদ্ধ সত্তা উহার আয় ও ব্যয়ের হিসাব এতদুদ্দেশ্যে সরকার কর্তৃক মনোনীত উপযুক্ত কর্তৃপক্ষের নিকট দাখিল করিবে এবং আয়ের সকল উৎস প্রকাশ করিবে।

(৩) যদি প্রতীয়মান হয় যে, তালিকাভুক্ত ব্যক্তি বা নিষিদ্ধ সংঘটনের সম্পত্তি অবৈধভাবে অর্জিত হইয়াছে অথবা এই আইনের অধীন কোন অপরাধ সংঘটনে ব্যবহৃত হইয়াছে, তাহা হইলে উক্ত সম্পত্তি আদালত কর্তৃক রাষ্ট্রের অনুকূলে বাজেয়াপ্ত হইবে।"

২১। ২০০৯ সনের ১৬ নং আইনে ধারা ২০ক এর সন্নিবেশ।—উক্ত আইনের ধারা ২০ এর পর নিম্নরূপ একটি নূতন ধারা ২০ক সন্নিবেশিত হইবে, যথা:—

"২০ক। জাতিসংঘ নিরাপত্তা পরিষদের রেজুলেশন বাস্তবায়নে পদক্ষেপ।—(১) এই আইনের উদ্দেশ্য পূরণকল্পে, জাতিসংঘ নিরাপত্তা পরিষদের রেজুলেশন নং ১২৬৭ এবং উহার অনুবর্তী রেজুলেশনসমূহ ও জাতিসংঘ নিরাপত্তা পরিষদের রেজুলেশন নং ১৩৭৩ এবং ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তার ও উহাতে অর্থ সংস্থান প্রতিরোধ, দমন এবং ব্যাহতকরণ সম্পর্কিত জাতিসংঘ নিরাপত্তা পরিষদের রেজুলেশনসমূহ বাস্তবায়নের উদ্দেশ্যে, বাংলাদেশ সরকারের এই আইনের অন্যান্য ধারা অথবা আপাতত বলবৎ অন্যান্য আইনে উল্লিখিত ক্ষমতার অতিরিক্ত হিসাবে নিম্নবর্ণিত ব্যবস্থাসমূহ গ্রহণ করিবার ক্ষমতা থাকিবে:

- (ক) তালিকাভুক্ত ব্যক্তি বা সত্তা কর্তৃক অথবা তালিকাভুক্ত ব্যক্তি বা সত্তার মালিকানাধীন বা উক্ত ব্যক্তি বা সত্তা কর্তৃক প্রত্যক্ষ বা পরোক্ষভাবে নিয়ন্ত্রিত কোন সংস্থা কর্তৃক অথবা, যদি জাতিসংঘ নিরাপত্তা পরিষদের ১২৬৭ নং রেজুলেশনের অধীন সংকলিত তালিকায় কোন স্বাভাবিক ব্যক্তি (natural person) বা সত্তার নাম অন্তর্ভুক্ত থাকে, তাহা হইলে উক্ত স্বাভাবিক ব্যক্তি বা সত্তার পক্ষে, ধারণকৃত সম্পত্তি, তহবিল বা অন্যান্য আর্থিক পরিসম্পদ বা আর্থিক উৎসসহ উহা হইতে উদ্ধৃত বা সৃষ্ট তহবিল, পূর্ব নোটিশ ব্যতীত, অনতিবিলম্বে অবরুদ্ধ, জব্দ বা ফ্রোক করিবে;
- (খ) সন্ত্রাসী কার্য সংঘটন বা সংঘটনের প্রচেষ্টাকারী বা সন্ত্রাসী কার্য সংঘটনে অংশগ্রহণ বা সুযোগ সৃষ্টিকারী কোন ব্যক্তি অথবা উক্তরূপ ব্যক্তির মালিকানাধীন বা তৎকর্তৃক প্রত্যক্ষ বা পরোক্ষভাবে নিয়ন্ত্রিত সত্তার অথবা উক্তরূপ ব্যক্তি বা সত্তার পক্ষে বা নির্দেশনা অনুসারে কার্য সম্পাদনকারী ব্যক্তি বা সত্তার অথবা জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত বা ১৩৭৩ নং রেজুলেশনের অধীন নিষিদ্ধ বা তালিকাভুক্ত ব্যক্তির এবং সহযোগী ব্যক্তি ও সত্তার তহবিল বা অন্যান্য আর্থিক পরিসম্পদ বা আর্থিক উৎসসহ উহা হইতে উদ্ধৃত বা সৃষ্ট তহবিল, পূর্ব নোটিশ ব্যতীত, অনতিবিলম্বে অবরুদ্ধ, জব্দ বা ফ্রোক করিবে;
- (গ) বাংলাদেশের অভ্যন্তরে বা বাহিরে কোন ব্যক্তি বা সত্তা কর্তৃক কোন তহবিল সন্ত্রাসী কার্যে ব্যবহারের অভিপ্রায়ে বা উহা সন্ত্রাসী কার্যে ব্যবহৃত হইবে এইরূপ জ্ঞাত থাকিয়া, বৈচ্ছায় প্রত্যক্ষ বা পরোক্ষভাবে, তহবিল গঠন বা সংগ্রহ করা হইলে, উহা নিষিদ্ধ করিবে;
- (ঘ) জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত বা ১৩৭৩ নং রেজুলেশনের অধীন নিষিদ্ধ বা তালিকাভুক্ত ব্যক্তি বা সত্তার অথবা উক্তরূপ ব্যক্তির মালিকানাধীন বা তৎকর্তৃক প্রত্যক্ষ বা পরোক্ষভাবে নিয়ন্ত্রিত সত্তার অথবা উক্তরূপ ব্যক্তির পক্ষে বা নির্দেশনা অনুসারে কার্য সম্পাদনকারী ব্যক্তি বা সত্তার প্রত্যক্ষ বা পরোক্ষ কল্যাণে কোন ব্যক্তি বা সত্তা কর্তৃক কোন তহবিল গঠন, আর্থিক পরিসম্পদ বা আর্থিক উৎস বা সম্পূর্ণ অন্যান্য সেবা সৃষ্টি করা হইলে, উহা নিষিদ্ধ করিবে;
- (ঙ) কার্যকর সীমানা নিয়ন্ত্রণ এবং অভিবাসন ব্যবস্থার মাধ্যমে জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত ব্যক্তিগণের বাংলাদেশে প্রবেশ বা বাংলাদেশের ভিতর দিয়া অন্য দেশে গমনাগমন প্রতিরোধ করিবে;
- (চ) জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা সত্তার নিকট, প্রত্যক্ষ বা পরোক্ষভাবে, বাংলাদেশের অভ্যন্তরে বা বাহিরে কোন অস্ত্র এবং গোলাবারুদ এবং অন্যান্য সহশ্রিষ্ট উপকরণ, বস্তু, হাতিয়ার (equipment), পণ্য এবং প্রযুক্তি সরবরাহ, বিক্রয় এবং হস্তান্তর প্রতিরোধ করিবে;
- (ছ) জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত ব্যক্তি বা সত্তার মালিকানাধীন, ইজারাধীন বা তৎকর্তৃক বা উহার পক্ষে পরিচালিত যে কোন বিমান (any aircraft) তাহাদের রাষ্ট্রীয় সীমানায় উড্ডয়ন বা অবতরণের অনুমতি প্রদানে অস্বীকৃতি প্রদান করিবে;

- (জ) জাতিসংঘের নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত ব্যক্তি বা সত্তার নিকটে বা নিকট হইতে প্রেরিত কার্গো পরিদর্শনের মাধ্যমে পারমাণবিক, রাসায়নিক বা জৈব (Biological) অস্ত্রসমূহ, উহা সরবরাহের সরঞ্জাম এবং সংশ্লিষ্ট অন্যান্য বস্তুর অবৈধ পাচার প্রতিরোধ করিবে;
- (ঝ) জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক তালিকাভুক্ত ব্যক্তি এবং সত্তার সহিত সম্পর্কিত উক্ত রেজুলেশনে উল্লিখিত যে কোন কার্য নিষিদ্ধ এবং প্রতিরোধ করিবে;
- (ঞ) এই ধারার যথাযথ বাস্তবায়নের উদ্দেশ্যে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক রিপোর্ট প্রদানকারী সংস্থাকে সময় সময় অনুশাসন প্রদান করিবে;
- (ট) দফা (ক) হইতে (ঝ) তে বর্ণিত ক্ষমতা মোতাবেক প্রয়োজনীয় কার্যক্রম গ্রহণের জন্যে সরকার সময়ে সময়ে প্রজ্ঞাপন বা আদেশ জারির মাধ্যমে উপযুক্ত কর্তৃপক্ষ নির্ধারণ করিবে।

(২) যদি কোন ব্যক্তি বা সত্তা এই ধারার অধীন প্রদত্ত অবরুদ্ধ বা ফ্রোক আদেশ লংঘন করে, তাহা হইলে উক্ত ব্যক্তি বা উক্ত সত্তার সংশ্লিষ্ট ব্যক্তি অনধিক ৪ (চার) বৎসরের কারাদণ্ডে দণ্ডিত হইবেন অথবা অবরুদ্ধ বা ফ্রোকযোগ্য সম্পত্তির মূল্যের দ্বিগুণ অর্থের সমপরিমাণ অর্থদণ্ড অথবা উভয় দণ্ডে দণ্ডিত হইবেন।

(৩) যদি কোন ব্যক্তি বা সত্তা উপ-ধারা (১) এর দফা (গ) এবং (ঘ) লংঘন করিয়া কোন কার্য করে বা কোন কার্য করিতে ব্যর্থ হয়, তাহা হইলে উক্ত ব্যক্তি বা সত্তা সন্ত্রাসী কার্যে অর্থায়নের অপরাধ সংঘটন করিয়াছে বলিয়া গণ্য হইবে এবং ধারা ৭ এর উপ-ধারা (৩), (৪)(ক) বা, ক্ষেত্রমত, (৪)(খ) এর বিধান অনুসারে দণ্ডিত হইবে।

(৪) যদি কোন ব্যক্তি বা সত্তা উপ-ধারা (১) এর দফা (ঙ) হইতে (জ) লংঘন করিয়া কোন কার্য করে বা কোন কার্য করিতে ব্যর্থ হয়, তাহা হইলে উক্ত ব্যক্তি বা সত্তা সন্ত্রাসী কার্যের অপরাধ সংঘটন করিয়াছে বলিয়া গণ্য হইবে এবং ধারা ৬ এর উপ-ধারা (২), (৩)(ক) বা, ক্ষেত্রমত, (৩)(খ) এর বিধান অনুসারে দণ্ডিত হইবে।

(৫) যদি কোন রিপোর্ট প্রদানকারী সংস্থা এই ধারার অধীন বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক প্রদত্ত অনুশাসনাবলী প্রতিপালনে ব্যর্থ হয়, অথবা এই ধারার অধীন অবিলম্বে অবরুদ্ধ কার্যক্রম গ্রহণে ব্যর্থ হয়, তাহা হইলে উক্ত রিপোর্ট প্রদানকারী সংস্থা বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক নির্ধারিত এবং নির্দেশিত অনধিক ২৫ (পঁচিশ) লক্ষ টাকা তবে অন্য় ৫ (পাঁচ) লক্ষ টাকা জরিমানা অথবা সন্দেহযুক্ত তহবিলের দ্বিগুণ পরিমাণ অর্থ, উহাদের মধ্যে যাহা অধিক হয়, জরিমানা পরিশোধ করিতে বাধ্য থাকিবে এবং বাংলাদেশ ব্যাংক উক্ত সংস্থা বা সংস্থার কোন শাখা, সেবাকেন্দ্র, বুথ বা এজেন্টের বাংলাদেশে কার্যক্রম পরিচালনা বন্ধ করিবার উদ্দেশ্যে নিবন্ধন বা লাইসেন্স স্থগিত করিতে পারিবে বা, ক্ষেত্রমত, নিবন্ধনকারী বা লাইসেন্স প্রদানকারী কর্তৃপক্ষকে উক্ত সংস্থার বিরুদ্ধে যথাযথ ব্যবস্থা গ্রহণের নিমিত্ত বিষয়টি সম্পর্কে অবহিত করিবে।

(৬) কোন জনসেবকের (public servant) বিরুদ্ধে, এই ধারার বিধান কার্যকর করিবার ক্ষেত্রে, কোনরূপ অবহেলা করিবার অভিযোগ প্রমাণিত হইলে, তাহার নিজস্ব চাকুরি বিধিমালা অনুসারে তাহার বিরুদ্ধে প্রশাসনিক কার্যক্রম গ্রহণ করা হইবে।”।

২২। ২০০৯ সনের ১৬ নং আইনের ধারা ২১ এর সংশোধন।—উক্ত আইনের ধারা ২১ এর উপ-ধারা (২) এর পর নিম্নরূপ নূতন উপ-ধারা (৩) সংযোজিত হইবে, যথা:—

“(৩) কোন সন্ত্রাসী ব্যক্তি বা সত্তা কর্তৃক ব্যবহৃত ফেসবুক, স্কাইপি, টুইটার বা যে কোন ইন্টারনেট এর মাধ্যমে আলাপ আলোচনা ও কথাবার্তা অথবা তাহাদের অপরাধ সংশ্লিষ্ট স্থির বা ভিডিও চিত্র পুলিশ বা আইন প্রয়োগকারী সংস্থা কর্তৃক কোন মামলার তদন্তের স্বার্থে যদি আদালতে উপস্থাপন করা হয়, তাহা হইলে, সাক্ষ্য আইনে যাহা কিছুই থাকুক না কেন, পুলিশ বা আইন প্রয়োগকারী সংস্থা কর্তৃক উপস্থাপিত উক্ত তথ্যাদি আদালতে সাক্ষ্য হিসাবে গ্রহণযোগ্য হইবে।”।

২৩। ২০০৯ সনের ১৬ নং আইনের ধারা ২৩ এর প্রতিস্থাপন।—উক্ত আইনের ধারা ২৩ এর পরিবর্তে নিম্নরূপ ধারা ২৩ ও ২৩ক প্রতিস্থাপিত হইবে, যথা:—

“২৩। অভিযুক্ত ব্যক্তির স্বীকারোক্তি রেকর্ড সম্পর্কিত বিশেষ বিধান।—যে কোন মেট্রোপলিটন ম্যাজিস্ট্রেট, চীফ জুডিসিয়াল ম্যাজিস্ট্রেট বা জুডিসিয়াল ম্যাজিস্ট্রেট অথবা এতদুদ্দেশ্যে বিশেষভাবে ক্ষমতাপ্রাপ্ত যে কোন ম্যাজিস্ট্রেট অভিযুক্ত ব্যক্তি কর্তৃক প্রদত্ত স্বীকারোক্তিমূলক কোন বক্তব্য রেকর্ডকালে, যদি উক্ত ব্যক্তি ঘটনা সম্পর্কে লিখিতভাবে বিবৃতি প্রদান করিতে সক্ষম ও আগ্রহী হন, তাহা হইলে উক্ত ব্যক্তিকে তাহার স্বীকারোক্তিমূলক বক্তব্য স্বহস্তে লিপিবদ্ধ করিবার অনুমতি প্রদান করিবেন।

২৩ক। তদন্তকারী সন্ত্রাসী সম্পত্তি জব্দ বা ক্রোকের বিশেষ বিধান।—(১) যদি এই আইনের অধীন সংঘটিত অপরাধের বিষয়ে তদন্তকারী কোন কর্মকর্তার নিকট বিশ্বাস করিবার কারণ থাকে যে, তদন্তকারী সম্পত্তি সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ধৃত সম্পদ (proceeds of terrorism), তাহা হইলে তিনি উক্ত সম্পত্তি যে জেলায় অবস্থিত উক্ত জেলার জেলা ম্যাজিস্ট্রেটের নিকট উক্ত সম্পত্তি জব্দ করিবার পূর্বানুমতির জন্য লিখিত আবেদন করিবেন এবং জেলা ম্যাজিস্ট্রেট তদন্তকারী কর্মকর্তার আবেদন যাচাই করিবার পর সন্তুষ্ট হইলে, অনুরূপ সম্পত্তি জব্দ করিবার অনুমতি প্রদান করিতে পারিবেন এবং যেক্ষেত্রে অনুরূপ সম্পত্তি জব্দ করা বাস্তবসম্মত নহে, সেইক্ষেত্রে ক্রোক আদেশের (order of attachment) মাধ্যমে নির্দেশ প্রদান করিবেন যে, অনুরূপ আদেশ প্রদানকারী কর্মকর্তার পূর্বানুমতি ব্যতীত, অনুরূপ সম্পত্তি হস্তান্তর বা অন্য কোন ব্যবস্থা করা যাইবে না।

(২) যদি বৈধ উৎস হইতে অর্জিত সম্পত্তির সহিত সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ধৃত সম্পত্তির মিশ্রণ (mingle) ঘটে, তাহা হইলে উক্ত মিশ্রিত (mingled) সম্পত্তিতে স্থিত সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ধৃত সম্পত্তি, অথবা যেক্ষেত্রে সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ধৃত সম্পত্তির মূল্য নিরূপণ করা না যায়, সেইক্ষেত্রে মিশ্রিত সম্পত্তির সম্পূর্ণ মূল্য এই ধারায় বর্ণিত বিধান অনুসারে তদন্তকারী কর্মকর্তা কর্তৃক জব্দ বা ক্রোকযোগ্য হইবে।

(৩) তদন্তকারী কর্মকর্তা অনুরূপ সম্পত্তি জব্দ বা ক্রোকের ৪৮ (আটচল্লিশ) ঘন্টার মধ্যে সরকারকে যথাযথভাবে অবহিত করিবেন এবং সরকার অনুরূপ জব্দ বা ক্রোক আদেশ জারির ৬০ (ষাট) কর্ম দিবসের মধ্যে উক্ত জব্দ বা ক্রোক আদেশ অনুমোদন করিবেন অথবা বাতিল করিবেন:

তবে শর্ত থাকে যে, যাহার সম্পত্তি জব্দ বা ক্রোক হইয়াছে তাহাকে বক্তব্য উপস্থাপনের যথাযথ সুযোগ প্রদান করিতে হইবে।

(৪) উপ-ধারা (৩) এর অধীন কোন ক্রোক বা জব্দের মেয়াদকাল আদালতে তদন্ত প্রতিবেদন দাখিল করিবার পূর্ব পর্যন্ত বহাল থাকিবে।”।

২৪। ২০০৯ সনের ১৬ নং আইনের ধারা ৩৪ এর সংশোধন।—উক্ত আইনের ধারা ৩৪ এর—

(ক) উপাত্ত-টীকার পরিবর্তে নিম্নরূপ উপাত্ত-টীকা প্রতিস্থাপিত হইবে, যথা:—

“সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদের দখল (Possession of property obtained from terrorist activities)”;

(খ) উপ-ধারা (১) ও (২) এবং ব্যাখ্যার পরিবর্তে নিম্নরূপ উপ-ধারা (১) ও (২) প্রতিস্থাপিত হইবে, যথা:—

“(১) কোন সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তা বা অন্য কোন ব্যক্তি সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ভূত বা কোন সন্ত্রাসী ব্যক্তি বা সন্ত্রাসী সত্তা কর্তৃক প্রদত্ত অর্থ বা সম্পদ বা অন্য যে কোন সন্ত্রাসী সম্পত্তি ভোগ করিতে বা দখলে রাখিতে পারিবে না।

(২) এই আইনের অধীন দণ্ডপ্রাপ্ত হউক বা না হউক, এরূপ কোন সন্ত্রাসী ব্যক্তি বা কোন সন্ত্রাসী সত্তা বা অন্য কোন ব্যক্তির দখলে থাকা কোন সন্ত্রাসী সম্পত্তি রাষ্ট্রের অনুকূলে বাজেয়াপ্তযোগ্য হইবে।”।

২৫। ২০০৯ সনের ১৬ নং আইনের ধারা ৩৫ এর সংশোধন।—উক্ত আইনের ধারা ৩৫ এর—

(ক) উপাত্ত-টীকার পরিবর্তে নিম্নরূপ উপাত্ত-টীকা প্রতিস্থাপিত হইবে, যথা:—

‘সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ এবং সন্ত্রাসী কর্মকাণ্ড হইতে উদ্ভূত সম্পদ বাজেয়াপ্ত (Confiscation of assets obtained from terrorist activities and proceeds of terrorism)’;

(খ) উপ-ধারা (১) এ উল্লিখিত ‘সন্ত্রাসী কার্য হইতে উদ্ভূত’ শব্দগুলির পরিবর্তে ‘সন্ত্রাসী কার্য হইতে সৃষ্ট (deriving from terrorist activities) বা সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ হইতে উদ্ভূত (or it constitutes from proceeds of terrorism)’ শব্দগুলি, বন্ধনীগুলি ও হাইফেন প্রতিস্থাপিত হইবে;

(গ) উপ-ধারা (২) এ উল্লিখিত ‘কোন সন্ত্রাসী কার্য হইতে উদ্ভূত কোন সম্পত্তি’ শব্দগুলির পরিবর্তে ‘সন্ত্রাসী কর্মকাণ্ড-লব্ধ সম্পদ (proceeds of terrorism) বা কোন সন্ত্রাসী কার্য হইতে সৃষ্ট কোন সম্পত্তি’ শব্দগুলি, বন্ধনী ও হাইফেন প্রতিস্থাপিত হইবে।

২৬। ২০০৯ সনের ১৬ নং আইনের ধারা ৪০ এর সংশোধন।—উক্ত আইনের ধারা ৪০ এর উপ-ধারা (১) এর পরিবর্তে নিম্নরূপ উপ-ধারা (১) প্রতিস্থাপিত হইবে, যথা:—

“(১) এই আইনের অধীন কোন অপরাধ সংঘটিত হইলে, সংশ্লিষ্ট পুলিশ কর্মকর্তা, তাৎক্ষণিকভাবে সংশ্লিষ্ট জেলা ম্যাজিস্ট্রেটকে অবহিতক্রমে মামলা রুজু করিবে এবং তদন্ত কার্যক্রম শুরু করিবে।”।

২৭। ২০০৯ সনের ১৬ নং আইনের তফসিলের প্রতিস্থাপন।—উক্ত আইনের তফসিলের পরিবর্তে নিম্নরূপ তফসিল ১, ২ ও ৩ প্রতিস্থাপিত হইবে, যথা:—

“তফসিল-১

[ধারা ২ এর দফা (৩ক) দ্রষ্টব্য]

- (ক) ১৬ই ডিসেম্বর, ১৯৭০ খ্রিস্টাব্দ তারিখে হেগে সম্পাদিত অবৈধভাবে বিমান আটক প্রতিরোধ সংক্রান্ত কনভেনশন (Convention for the suppression of unlawful seizure of Aircraft, done at the Hague on 16th December, 1970);
- (খ) ২৩শে সেপ্টেম্বর, ১৯৭১ খ্রিস্টাব্দ তারিখে মন্ট্রিলে সম্পাদিত বেসামরিক বিমান চলাচলের বিরুদ্ধে অবৈধ কার্যক্রম দমন সংক্রান্ত কনভেনশন (Convention for the suppression of unlawful Acts against the safety of Civil Aviation, done at Montreal on 23rd September, 1971);
- (গ) ১৪ই ডিসেম্বর, ১৯৭৩ খ্রিস্টাব্দ তারিখে জাতিসংঘের সাধারণ পরিষদ কর্তৃক গৃহীত কূটনৈতিক প্রতিনিধিসহ আন্তর্জাতিকভাবে সুরক্ষিত ব্যক্তির বিরুদ্ধে অপরাধ প্রতিরোধ ও শাস্তি সংক্রান্ত কনভেনশন (Convention on the prevention and punishment of Crimes against internationally protected person, including diplomatic agents, adopted by the General Assembly of the United Nations on 14th December, 1973);
- (ঘ) ১৭ই ডিসেম্বর, ১৯৭৯ খ্রিস্টাব্দ তারিখে জাতিসংঘের সাধারণ পরিষদ কর্তৃক গৃহীত জিম্মি গ্রহণের বিরুদ্ধে কনভেনশন (International convention against the taking of hostages adopted by the General Assembly of the United Nations on 17th December, 1979);
- (ঙ) ৩রা মার্চ, ১৯৮০ খ্রিস্টাব্দ তারিখে ভিয়েনায় গৃহীত পারমাণবিক বস্তুর ভৌত সুরক্ষা সংক্রান্ত কনভেনশন (Convention on the physical protection of nuclear material, adopted at Vienna on 3rd March, 1980);

(চ) ২৪শে ফেব্রুয়ারি, ১৯৮৮ খ্রিস্টাব্দ তারিখে মন্ট্রিালে সম্পাদিত বেসামরিক বিমান চলাচলের নিরাপত্তার বিরুদ্ধে হিংস্র অবৈধ কার্যক্রম দমন সংক্রান্ত কনভেনশনের সম্পূর্ণ আন্তর্জাতিক বিমান বন্দরে কর্মরত কর্মীদের অবৈধ কার্যক্রম দমন সংক্রান্ত প্রটোকল (Protocol for the suppression of unlawful Acts of violence at Airports serving International Civil Aviation, supplementary to the convention for the suppression of unlawful Acts against the safety of Civil Aviation, done at Montreal on 24th February, 1988);

(ছ) ১০ই মার্চ, ১৯৮৮ খ্রিস্টাব্দ তারিখে রোমে সম্পাদিত সামুদ্রিক নৌচালনার নিরাপত্তার বিরুদ্ধে অবৈধ কার্যক্রম দমন সংক্রান্ত কনভেনশন (Convention for the suppression of unlawful Acts against the safety of maritime navigation, done at Rome on 10th March, 1988);

(জ) ১০ই মার্চ, ১৯৮৮ খ্রিস্টাব্দ তারিখে রোমে সম্পাদিত মহিসোপানে অবস্থিত স্থায়ী প্রটফর্মের নিরাপত্তার বিরুদ্ধে অবৈধ কার্যক্রম দমন সংক্রান্ত প্রটোকল (Protocol for the suppression of unlawful Acts against the safety of fixed platforms located on the continental shelf, done at Rome on 10th March, 1988);

(ঝ) ১৫ই ডিসেম্বর, ১৯৯৭ খ্রিস্টাব্দ তারিখে জাতিসংঘের সাধারণ পরিষদ কর্তৃক গৃহীত সন্ত্রাসী বোমা হামলা দমন সংক্রান্ত আন্তর্জাতিক কনভেনশন (International convention for the suppression of terrorist Bombings, adopted by the General Assembly of the United Nations on 15th December, 1997)।

তফসিল-২
(ধারা ১৮ প্রক্ৰিয়া)

১	২	৩	৪	৫
ক্রমিক নং	সত্তার নাম	সত্তার ঠিকানা	নিষিদ্ধকরণের তারিখ	মন্তব্য
০১	শাহাদাত-ই-আল হিকমা পার্টি বাংলাদেশ	জনৈক মিজানুর রহমানের বাড়ী, হুড়ঘাম নতুন পাড়া বাইপাস সড়ক, ধানা-রাজপাড়া, রাজশাহী মহানগর	০৯/০২/২০০৩ খ্রিঃ	
০২	জায়াত মুসলিম জনতা বাংলাদেশ (জেএমজেবি)	সুনির্দিষ্ট ঠিকানাবিহীন	২৩/০২/২০০৫ খ্রিঃ	
০৩	জামাতুল মুজাহেদীন	সুনির্দিষ্ট ঠিকানাবিহীন	২৩/০২/২০০৫ খ্রিঃ	
০৪	হরকাতুল জিহাদ আল ইসলামী	সুনির্দিষ্ট ঠিকানাবিহীন	১৭/১০/২০০৫ খ্রিঃ	
০৫	হিজবুত তাহরীর বাংলাদেশ	এইচ. এম সিদ্দিক ম্যানসন, ৫৫/এ পুরানা পল্টন, ঢাকা এবং ২০১/সি পল্টন টাওয়ার (৩য় তলা), ২৭ পুরানা পল্টন লেন, ঢাকা	২২/১০/২০০৯ খ্রিঃ	

রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ



গেজেট

অতিরিক্ত সংখ্যা
কর্তৃপক্ষ কর্তৃক প্রকাশিত

বৃহস্পতিবার, নভেম্বর ২৬, ২০১৫

বাংলাদেশ জাতীয় সংসদ

ঢাকা, ১২ অগ্রহায়ণ, ১৪২২/২৬ নভেম্বর, ২০১৫

সংসদ কর্তৃক গৃহীত নিম্নলিখিত আইনটি ১২ অগ্রহায়ণ, ১৪২২ মোতাবেক ২৬ নভেম্বর, ২০১৫ তারিখে রাষ্ট্রপতির সম্মতিলাভ করিয়াছে এবং এতদ্বারা এই আইনটি সর্বসাধারণের অবগতির জন্য প্রকাশ করা যাইতেছে :—

২০১৫ সনের ২৫ নং আইন

মানিলভারিং প্রতিরোধ আইন, ২০১২ এর সংশোধনকল্পে প্রণীত আইন

যেহেতু নিম্নবর্ণিত উদ্দেশ্যসমূহ পূরণকল্পে মানিলভারিং প্রতিরোধ আইন, ২০১২ (২০১২ সনের ৫নং আইন) এর সংশোধন সমীচীন ও প্রয়োজনীয়; এবং

সেহেতু এতদ্বারা নিম্নরূপ আইন করা হইল :—

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন।—(১) এই আইন মানিলভারিং প্রতিরোধ (সংশোধন) আইন, ২০১৫ নামে অভিহিত হইবে।

(২) ইহা অবিলম্বে কার্যকর হইবে।

২। ২০১২ সনের ৫নং আইনের ধারা ২ এর সংশোধন।—মানিলভারিং প্রতিরোধ আইন, ২০১২ (২০১২ সনের ৫নং আইন), অতঃপর উক্ত আইন বলিয়া উল্লিখিত, এর ধারা ২ এর—

(ক) দফা (এ৪) এর “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশনস ইউনিট” শব্দগুলি প্রতিস্থাপিত হইবে;

(৯২৫১)

মূল্য : টাকা ১২.০০

(খ) দফা (ঠ) এর পরিবর্তে নিম্নরূপ দফা (ঠ) প্রতিস্থাপিত হইবে, যথা :—

“(ঠ) “তদন্তকারী সংস্থা” অর্থ এই আইনের অন্য কোন বিধানে ভিন্নরূপ কোন কিছু না থাকিলে,—

(অ) দফা (শ) এ বর্ণিত ‘সম্পূর্ণ অপরাধ’ তদন্তের জন্য সংশ্লিষ্ট আইনে ক্ষমতাপ্রাপ্ত তদন্তকারী সংস্থা:

তবে শর্ত থাকে যে, যে সকল সম্পূর্ণ অপরাধ বাংলাদেশ পুলিশ কর্তৃক তদন্তযোগ্য তাহা বাংলাদেশ পুলিশের অপরাধ তদন্ত বিভাগ (Criminal investigation department) কর্তৃক তদন্ত করিতে হইবে;

(আ) সরকারের সহিত পরামর্শক্রমে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক ক্ষমতাপ্রাপ্ত উপ-দফা (অ) এ উল্লিখিত এক বা একাধিক তদন্তকারী সংস্থা;”;

(গ) দফা (ভ) এর পরিবর্তে নিম্নরূপ দফা (ভ) প্রতিস্থাপিত হইবে, যথা :—

“(ভ) “রিয়েল এস্টেট ডেভেলপার” অর্থ—

(অ) রিয়েল এস্টেট উন্নয়ন ও ব্যবস্থাপনা আইন, ২০১০ (২০১০ সনের ৪৮ নং আইন) এর ধারা ২(১৫) এ সংজ্ঞায়িত যে কোন রিয়েল এস্টেট ডেভেলপার বা উহার কর্মকর্তা বা কর্মচারী; অথবা

(আ) রিয়েল এস্টেট এজেন্ট যাহারা জমি, আবাসিক বা বাণিজ্যিক ভবন এবং ফ্ল্যাট ইত্যাদি নির্মাণ ও ক্রয়-বিক্রয়ের সহিত জড়িত;”;

(ঘ) দফা (শ) এর—

(অ) উপ-দফা (১৬) এর পরিবর্তে নিম্নরূপ উপ-দফা (১৬) প্রতিস্থাপিত হইবে, যথা :—

“(১৬) মানব পাচার বা কোন ব্যক্তিকে বৈদেশিক কর্মসংস্থানের মিথ্যা আশ্বাস প্রদান করিয়া কোন অর্থ বা মূল্যবান দ্রব্য গ্রহণ করা বা করিবার চেষ্টা;”;

(আ) উপ-দফা (২৮) এর “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট” শব্দগুলি প্রতিস্থাপিত হইবে।

৩। ২০১২ সনের ৫নং আইনের ধারা ৩ এর সংশোধন।—উক্ত আইনের ধারা ৩ এর “এই আইনের ধারা ৯ এর বিধান সাপেক্ষে” শব্দগুলি ও সংখ্যা বিলুপ্ত হইবে।

৪। ২০১২ সনের ৫নং আইনের ধারা ৪ এর সংশোধন।—উক্ত আইনের ধারা ৪ এর—

(ক) উপ-ধারা (২) এর প্রাপ্তস্থিত “।” দাঁড়ি চিহ্নটির পরিবর্তে “:” কোলন চিহ্নটি প্রতিস্থাপিত হইবে এবং অতঃপর নিম্নরূপ শর্তাংশ সংযোজিত হইবে, যথা :—

“তবে শর্ত থাকে যে, আদালত কর্তৃক ধার্যকৃত সময়সীমার মধ্যে অর্থদণ্ড পরিশোধে ব্যর্থ হইলে আদালত অপরিশোধিত অর্থদণ্ডের পরিমাণ বিবেচনায় অতিরিক্ত কারাদণ্ডে দণ্ডিত করিবার আদেশ প্রদান করিতে পারিবে।”;

(খ) উপ-ধারা (৪) এর পরিবর্তে নিম্নরূপ উপ-ধারা (৪) প্রতিস্থাপিত হইবে, যথা:—

“(৪) কোন সত্তা এই আইনের অধীন কোন অপরাধ সংঘটন করিলে বা অপরাধ সংঘটনের চেষ্টা, সহায়তা বা ষড়যন্ত্র করিলে ধারা ২৭ এর বিধান সাপেক্ষে, উপ-ধারা (২) এর বিধান অনুসারে ব্যবস্থা গ্রহণ করা যাইবে এবং অপরাধের সহিত সংশ্লিষ্ট সম্পত্তির মূল্যের অন্যান্য দ্বিগুণ অথবা ২০ (বিশ) লক্ষ টাকা, যাহা অধিক হয়, অর্থদণ্ড প্রদান করা যাইবে এবং উক্ত প্রতিষ্ঠানের নিবন্ধন বাতিলযোগ্য হইবে :

তবে শর্ত থাকে যে, উক্ত সত্তা আদালত কর্তৃক ধার্যকৃত সময়সীমার মধ্যে অর্থদণ্ড পরিশোধে ব্যর্থ হইলে আদালত অপরিশোধিত অর্থদণ্ডের পরিমাণ বিবেচনায় সত্তার মালিক, চেয়ারম্যান বা পরিচালক যে নামেই অভিহিত করা হউক না কেন, তাহার বিরুদ্ধে কারাদণ্ডে দণ্ডিত করিবার আদেশ প্রদান করিতে পারিবে।”।

৫। ২০১২ সনের ৫নং আইনের ধারা ৯ এর সংশোধন।—উক্ত আইনের ধারা ৯ এর পরিবর্তে নিম্নরূপ ধারা ৯ প্রতিস্থাপিত হইবে, যথা :—

“৯। অপরাধের তদন্ত ও বিচার।—(১) আপাতত বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এই আইনের অধীন অপরাধসমূহ ধারা ২(ঠ) তে উল্লিখিত তদন্তকারী সংস্থার কর্মকর্তা বা এতদুদ্দেশ্যে সরকারের সহিত পরামর্শক্রমে, বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক একাধিক তদন্তকারী সংস্থার কর্মকর্তাদের সমন্বয়ে গঠিত যৌথ তদন্তকারী দল, তদন্ত করিবে।

(২) আপাতত বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এই আইনের অধীন অপরাধসমূহ Criminal Law (Amendment) Act, 1958 (Act XL of 1958) এর section 3 এর অধীন নিযুক্ত স্পেশাল জজ কর্তৃক বিচার্য হইবে।

(৩) অভিযুক্ত ব্যক্তি বা সত্তার সম্পত্তি অনুসন্ধান ও সনাক্তকরণের লক্ষ্যে তদন্ত কর্মকর্তা কর্তৃক এই আইনের পাশাপাশি অন্যান্য আইনে এতদুদ্দেশ্যে প্রদত্ত ক্ষমতাও প্রয়োগ করিতে পারিবে।

(৪) তদন্তকারী সংস্থা এই আইনের অধীন সংঘটিত অপরাধ অনুসন্ধান বা তদন্ত কার্যক্রম পরিচালনার বিষয়টি বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবহিত করিবে।”।

৬। ২০১২ সনের ৫নং আইনের ধারা ১২ এর সংশোধন।—উক্ত আইনের ধারা ১২ এর—

- (ক) উপাস্তটিকায় উল্লিখিত “দুর্নীতি দমন কমিশনের” শব্দগুলির পরিবর্তে “কর্তৃপক্ষের” শব্দটি প্রতিস্থাপিত হইবে;
- (খ) উপ-ধারা (১) এর দ্বিতীয় লাইনে উল্লিখিত “দুর্নীতি দমন কমিশনের” শব্দগুলির পরিবর্তে “সরকার কর্তৃক বিধি দ্বারা নির্ধারিত কর্তৃপক্ষের” শব্দগুলি প্রতিস্থাপিত হইবে;
- (গ) উপ-ধারা (২) এর দ্বিতীয় লাইনে উল্লিখিত “কমিশনের” শব্দটির পরিবর্তে “উপ-ধারা (১) এর অধীন নির্ধারিত কর্তৃপক্ষের” শব্দগুলি এবং অতঃপর উল্লিখিত “কমিশন” শব্দটির পরিবর্তে “কর্তৃপক্ষ” শব্দটি প্রতিস্থাপিত হইবে।

৭। ২০১২ সনের ৫নং আইনের ধারা ১৪ এর সংশোধন।—উক্ত আইনের ধারা ১৪ এর—

- (ক) উপ-ধারা (১) এর পরিবর্তে নিম্নরূপ উপ-ধারা (১) প্রতিস্থাপিত হইবে, যথা:—

“(১) তদন্তকারী সংস্থার লিখিত আবেদনের ভিত্তিতে আদালত বাংলাদেশে বা বাংলাদেশের বাহিরে অবস্থিত মানিলভারিং অপরাধের সহিত সম্পৃক্ত সম্পত্তি বা অপরাধলব্ধ আয় বা সম্পত্তি অবরুদ্ধকরণ বা ফ্রোক আদেশ প্রদান করিতে পারিবে:

তবে শর্ত থাকে যে, মানিলভারিং অপরাধের সহিত সম্পৃক্ত সম্পত্তি, অপরাধলব্ধ আয়, অর্থ বা সম্পত্তি চিহ্নিত করা সম্ভব না হইলে অভিযুক্ত ব্যক্তি বা সত্তার অন্য অর্থ বা সম্পত্তি হইতে সমমূল্যের অর্থ বা সম্পত্তি অবরুদ্ধ বা ফ্রোক করা যাইবে।”;

- (খ) উপ-ধারা (২) এর “দুর্নীতি দমন কমিশন বা তৎকর্তৃক ক্ষমতাপ্রাপ্ত কোন ব্যক্তি বা সংস্থা” শব্দগুলির পরিবর্তে “তদন্তকারী কোন সংস্থা কর্তৃক” শব্দগুলি প্রতিস্থাপিত হইবে।

৮। ২০১২ সনের ৫নং আইনের ধারা ২৩ এর সংশোধন।—উক্ত আইনের ধারা ২৩ এর—

- (ক) উপাস্তটিকায় উল্লিখিত “বাংলাদেশ ব্যাংকের” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইন্সটিটিউটের” শব্দগুলি প্রতিস্থাপিত হইবে;

- (খ) উপ-ধারা (১) এর—

(অ) “বাংলাদেশ ব্যাংকের” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইন্সটিটিউটের” শব্দগুলি প্রতিস্থাপিত হইবে;

(আ) দফা (ক) এর “লেনদেন সম্পর্কিত তথ্যাদি” শব্দগুলির পর “ও অন্য কোন মাধ্যমে প্রাপ্ত তথ্যাদি” শব্দগুলি, “পর্যালোচনার উদ্দেশ্যে” শব্দগুলির পর “প্রয়োজনীয়” শব্দটি, “ডাটা” শব্দটির পরিবর্তে “তথ্য-উপাত্ত” শব্দটি প্রতিস্থাপিত হইবে এবং “ক্ষেত্রমত, সংশ্লিষ্ট” শব্দগুলি ও কুমার পর “তদন্তকারী সংস্থা বা” শব্দগুলি সন্নিবেশিত হইবে;

- (ই) দফা (খ) এর পরিবর্তে নিম্নরূপ দফা (খ) প্রতিস্থাপিত হইবে, যথা:—
- “(খ) অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, রিপোর্ট প্রদানকারী সংস্থা হইতে প্রয়োজনীয় তথ্য বা প্রতিবেদন সংগ্রহ করা;”;
- (ঈ) দফা (গ) এর “হিসাবে জমা হইয়াছে” শব্দগুলির পর “বা কোন হিসাবের অর্থ কোন অপরাধ সংঘটনে ব্যবহৃত হইয়াছে বা হইতে পারে” শব্দগুলি সন্নিবেশিত হইবে এবং
- শর্তাংশে উল্লিখিত “স্থগিত বা অবরুদ্ধ রাখিবার মেয়াদ অতিরিক্ত ৩০ (ত্রিশ) দিন করিয়া সর্বোচ্চ ৬ (ছয়) মাস বর্ধিত করা যাইবে” শব্দগুলি, সংখ্যাগুলি ও বন্ধনীগুলির পরিবর্তে “স্থগিত বা অবরুদ্ধ রাখিবার জন্য উক্ত রিপোর্ট প্রদানকারী সংস্থাকে ৩০ (ত্রিশ) দিন করিয়া সর্বোচ্চ ৭ (সাত) বার নির্দেশ প্রদান করা যাইবে” শব্দগুলি, সংখ্যাগুলি ও বন্ধনীগুলি প্রতিস্থাপিত হইবে;
- (উ) দফা (ঙ) এর পরিবর্তে নিম্নরূপ দফা (ঙ) প্রতিস্থাপিত হইবে, যথা:—
- “(ঙ) প্রয়োজনে রিপোর্ট প্রদানকারী সংস্থা সরেজমিন পরিদর্শন করা;”;
- (ঊ) দফা (চ) এর “বাংলাদেশ ব্যাংকের” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটের” শব্দগুলি প্রতিস্থাপিত হইবে;
- (এ) দফা (ছ) এর “উদ্দেশ্য পূরণকল্পে” শব্দগুলির পর “রিপোর্ট প্রদানকারী সংস্থার কার্যক্রম তদারকিসহ” শব্দগুলি সন্নিবেশিত হইবে;
- (গ) উপ-ধারা (২), (৩), (৪), (৫), (৬) ও (৮) এর “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট” শব্দগুলি প্রতিস্থাপিত হইবে;
- (ঘ) উপ-ধারা (৭) এ প্রথমবার উল্লিখিত “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট” শব্দগুলি এবং দ্বিতীয়বার উল্লিখিত “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট বাংলাদেশ ব্যাংক-কে অবহিত করিবে এবং বাংলাদেশ ব্যাংক” শব্দগুলি প্রতিস্থাপিত হইবে এবং তৃতীয়বার উল্লিখিত “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট” শব্দগুলি প্রতিস্থাপিত হইবে;
- (ঙ) উপ-ধারা (৭) এর পর নিম্নরূপ নতুন উপ-ধারা (৭ক) সন্নিবেশিত হইবে, যথা:—
- “(৭ক) এই আইনে বর্ণিত অপরাধের অনুসন্ধান ও তদন্তে কোন তদন্তকারী সংস্থা কোন ব্যাংক বা আর্থিক প্রতিষ্ঠানের গ্রাহকের হিসাব সংক্রান্ত দলিল ও তথ্যাদি উপযুক্ত আদালতের আদেশক্রমে অথবা বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটের মাধ্যমে সংগ্রহ করিতে পারিবে।”।

৯। ২০১২ সনের ৫নং আইনের ধারা ২৪ এর সংশোধন।—উক্ত আইনের ধারা ২৪ এর—

(ক) উপ-ধারা (১) এর পরিবর্তে নিম্নরূপ উপ-ধারা (১) প্রতিস্থাপিত হইবে, যথা:—

“(১) এই আইনে প্রদত্ত ক্ষমতা ও কার্যাবলী সুষ্ঠুভাবে সম্পাদনের লক্ষ্যে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট (Bangladesh Financial Intelligence Unit) নামে একটি পৃথক কেন্দ্রীয় সংস্থা থাকিবে, যাহার—

- (ক) একটি পৃথক সীল মোহর ও লেটার হেড প্যাড থাকিবে;
- (খ) একটি স্বতন্ত্র কার্যালয় বাংলাদেশ ব্যাংকে অবস্থিত হইবে;
- (গ) কার্যাবলী সম্পাদনের জন্য বাংলাদেশ ব্যাংক প্রয়োজনীয় অফিসস্থান, লোকবল, তহবিল, প্রশাসনিক সুবিধাসহ অন্যান্য আনুষঙ্গিক বিষয়াদি সরবরাহ করিবে;
- (ঘ) বাংলাদেশ ব্যাংকের ডেপুটি গভর্নর পদমর্যাদার একজন সার্বক্ষণিক প্রধান কর্মকর্তা থাকিবে, যিনি বাংলাদেশ ব্যাংকের গভর্নর এর নেতৃত্বে গঠিত বাছাই কমিটির সুপারিশ অনুযায়ী নির্ধারিত শর্তে সরকার কর্তৃক চুক্তিভিত্তিক বা অন্যবিধভাবে নিয়োগপ্রাপ্ত হইবেন;
- (ঙ) প্রধান কর্মকর্তা যাবতীয় প্রশাসনিক বিষয়ে গভর্নর, বাংলাদেশ ব্যাংক-এর পূর্বানুমোদন গ্রহণ করিবেন;
- (চ) প্রধান কর্মকর্তা মানিলভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধের লক্ষ্যে প্রয়োজনীয় দিক-নির্দেশনা, নীতি প্রণয়ন এবং বাস্তবায়নের লক্ষ্যে সরকারের সহিত পরামর্শক্রমে প্রয়োজনীয় ব্যবস্থা গ্রহণ করিবেন;
- (ছ) প্রধান কর্মকর্তার চাহিদার প্রেক্ষিতে বাংলাদেশ ব্যাংক উহাতে প্রয়োজনীয় সংখ্যক কর্মকর্তা ও কর্মচারী পদায়ন করিতে পারিবে এবং প্রয়োজন অনুযায়ী তিনি সরকার বা আইন প্রয়োগকারী সংস্থা হইতে প্রেষণে বা অন্যবিধভাবে কর্মকর্তা ও কর্মচারী নিয়োগের জন্য সরকারকে অনুরোধ করিতে পারিবে; এবং
- (জ) প্রধান কর্মকর্তার চাহিদার প্রেক্ষিতে উহাতে চুক্তিভিত্তিক পরামর্শক নিয়োগ করা যাইবে।”;

(খ) উপ-ধারা (৩) এর পরিবর্তে নিম্নরূপ উপ-ধারা (৩) প্রতিস্থাপিত হইবে, যথা :—

“(৩) এই আইনের উদ্দেশ্য পূরণকল্পে, বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন সংক্রান্ত তথ্যাদি অনুরোধের প্রেক্ষিতে বা প্রয়োজন মোতাবেক স্ব-উদ্যোগে সরকারি অন্য কোন সংস্থাকে সরবরাহ করিতে পারিবে।”।

১০। ২০১২ সনের ৫নং আইনের ধারা ২৫ এর সংশোধন।—উক্ত আইনের ধারা ২৫ এর—

(ক) উপ-ধারা (১) এর—

(অ) “দায়-দায়িত্ব” শব্দগুলির পরিবর্তে “দায়-দায়িত্বসহ বিধি দ্বারা নির্ধারিত অন্যান্য দায়-দায়িত্ব” শব্দগুলি প্রতিস্থাপিত হইবে;

(আ) দফা (খ) এর “হিসাবের” শব্দটির পূর্বে “হিসাব ও” শব্দগুলি সন্নিবেশিত হইবে;

(ই) দফা (গ) এর “বাংলাদেশ ব্যাংকের” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটের” শব্দগুলি প্রতিস্থাপিত হইবে;

(ঈ) দফা (ঘ) এর “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটে” শব্দগুলি প্রতিস্থাপিত হইবে;

(খ) উপ-ধারা (২) এর প্রথম লাইনে উল্লিখিত “বাংলাদেশ ব্যাংক” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট বা রিপোর্ট প্রদানকারী সংস্থার নিয়ন্ত্রণকারী কর্তৃপক্ষ” শব্দগুলি প্রতিস্থাপিত হইবে;

(গ) উপ-ধারা (৩) এ উল্লিখিত “বাংলাদেশ ব্যাংক তৎকর্তৃক নির্ধারিত পদ্ধতিতে আদায় করিবে এবং আদায়কৃত অর্থ” শব্দগুলি বিলুপ্ত হইবে;

(ঘ) উপ-ধারা (৩) এর পর নিম্নরূপ নতুন উপ-ধারা (৪), (৫) ও (৬) সংযোজিত হইবে, যথা :—

“(৪) রিপোর্ট প্রদানকারী সংস্থার নিয়ন্ত্রণকারী কর্তৃপক্ষ তাহাদের বিদ্যমান তদারকি কার্যক্রমের অংশ হিসেবে উপ-ধারা (১) ও বিধি দ্বারা নির্ধারিত দায়-দায়িত্ব পরিপালন নিশ্চিত করিবে এবং উপ-ধারা (১) ও বিধি দ্বারা নির্ধারিত দায়-দায়িত্ব পরিপালনে রিপোর্ট প্রদানকারী সংস্থার ব্যর্থতার দায় নিয়ন্ত্রণকারী কর্তৃপক্ষের উপরও বর্তাইবে।

(৫) কোন রিপোর্ট প্রদানকারী সংস্থা উপ-ধারা (১) এর বিধানসহ বিধি দ্বারা নির্ধারিত কোন বিধান লংঘন করিলে নিয়ন্ত্রণকারী কর্তৃপক্ষ উপ-ধারা (২) মোতাবেক ব্যবস্থা গ্রহণ করিতে পারিবে এবং এইরূপে গৃহীত ব্যবস্থা বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবিলম্বে অবহিত করিতে হইবে।

(৬) রিপোর্ট প্রদানকারী সংস্থার নিয়ন্ত্রণকারী কর্তৃপক্ষ তাহাদের তদারকি কার্যক্রম বা অন্য কোনভাবে এই আইনের অধীন সংঘটিত কোন অপরাধ সম্পর্কে অবহিত হইলে বা চিহ্নিত করিলে অবিলম্বে তাহা বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিটকে অবহিত করিবে।”।

১১। ২০১২ সনের ফেনং আইনের ধারা ২৮ এর সংশোধন।—উক্ত আইনের ধারা ২৮ এর “বাংলাদেশ ব্যাংক বা বাংলাদেশ ব্যাংকের” শব্দগুলির পরিবর্তে “বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট বা ইহার” শব্দগুলি এবং “দুর্নীতি দমন কমিশন বা কমিশনের” শব্দগুলির পরিবর্তে “তদন্তকারী সংস্থা বা ইহার” শব্দগুলি প্রতিস্থাপিত হইবে।

১২। রহিতকরণ ও হেফাজত।—(১) মানিলভারিং প্রতিরোধ (সংশোধন) অধ্যাদেশ, ২০১৫ (অধ্যাদেশ নং ২, ২০১৫) এতদ্বারা রহিত করা হইল।

(২) উপ-ধারা (১) এর অধীন রহিতকরণ সত্ত্বেও, উক্ত অধ্যাদেশের অধীন কৃত কাজকর্ম বা গৃহীত ব্যবস্থা এই আইনের অধীন কৃত বা গৃহীত হইয়াছে বলিয়া গণ্য হইবে।

মোঃ আশরাফুল মকবুল
সিনিয়র সচিব।

মানি লন্ডারিং প্রতিরোধ বিভাগ
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা।

ওয়েবসাইট: www.bangladeshbank.org.bd

এ.এম.এল. সার্কুলার নং-২২/২০০৯

তারিখ : ০৮ বৈশাখ, ১৪১৬
২১ এপ্রিল, ২০০৯

সকল তফসিলী ব্যাংক, আর্থিক প্রতিষ্ঠান, মানিচেঞ্জার
এবং অন্যান্য প্রতিষ্ঠান (সন্ত্রাস বিরোধী আইন, ২০০৯ এর ২(১০) ধারা মোতাবেক)

প্রিয় মহোদয়গণ,

সন্ত্রাস বিরোধী আইন, ২০০৯

বাংলাদেশ জাতীয় সংসদ কর্তৃক গৃহীত সন্ত্রাস বিরোধী আইন, ২০০৯ ২৪ ফেব্রুয়ারী, ২০০৯ তারিখে মহামান্য রাষ্ট্রপতির সম্মতি লাভের মাধ্যমে বিগত ১১ জুন, ২০০৮ হতে কার্যকর হয়েছে। এই আইন কার্যকর হবার সঙ্গে সঙ্গে সন্ত্রাস বিরোধী অধ্যাদেশ, ২০০৮ রহিত করা হয়েছে। বাংলাদেশ গেজেটের (অতিরিক্ত সংখ্যা) মাধ্যমে জারীকৃত এই আইনের গেজেট কপি সংযুক্ত করা হ'ল।

২. এই আইনের নির্দেশনা পরিপালন নিশ্চিত করার এবং বিষয়টি সংশ্লিষ্ট সকলের অবগতিতে আনার জন্য আপনাদেরকে অনুরোধ করা যাচ্ছে।

৩. ২৯ জুন, ২০০৮ তারিখে ইস্যুকৃত এ.এম.এল. সার্কুলার নম্বর ১৭ উল্লিখিত আইনের কার্যকারিতার তারিখ হতে বাতিল বলে গণ্য হবে।

৪. অনুগ্রহপূর্বক প্রাপ্তি স্বীকার করবেন।

আপনাদের বিশ্বস্ত,

সংযোজনী : ৫ (পাঁচ) পাতা।

(ম. মাহফুজুর রহমান)
মহাব্যবস্থাপক
ফোন : ৭১২০৬৫৯

বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউট

বাংলাদেশ ব্যাংক

প্রধান কার্যালয়, ঢাকা।

ওয়েবসাইট : www.bangladeshbank.org.bd

বিএফআইইউ সার্কুলার নম্বর : ২

০১ চৈত্র, ১৪১৮

তারিখ : ১৫ মার্চ, ২০১২

ব্যবস্থাপনা পরিচালক/ প্রধান নির্বাহী কর্মকর্তা/প্রতিষ্ঠান প্রধান

সকল ব্যাংক, আর্থিক প্রতিষ্ঠান, বীমাকারী, মানি চেঞ্জার, অর্থ অথবা অর্থমূল্য প্রেরণকারী বা স্থানান্তরকারী কোম্পানী বা প্রতিষ্ঠান, বাংলাদেশ ব্যাংকের অনুমতিক্রমে ব্যবসা পরিচালনাকারী প্রতিষ্ঠান, স্টক ডিলার ও স্টক ব্রোকার, পোর্টফোলিও ম্যানেজার ও মার্চেন্ট ব্যাংকার, সিকিউরিটি কাস্টডিয়ান, সম্পদ ব্যবস্থাপক, অ-লাভজনক সংস্থা/প্রতিষ্ঠান (NPO), বেসরকারী উন্নয়ন সংস্থা (NGO), সমবায় সমিতি, রিয়েল এস্টেট ডেভেলপার, মূল্যবান ধাতু বা পাথরের ব্যবসা প্রতিষ্ঠান, ট্রাস্ট ও কোম্পানী সেবা প্রদানকারী, আইনজীবী, নোটারী, অন্যান্য আইন পেশাজীবী এবং একাউন্টেন্ট।

প্রিয় মহোদয়,

মানিলভারিং প্রতিরোধ আইন, ২০১২ ও সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১২ প্রসঙ্গে।

মানিলভারিং ও সংশ্লিষ্ট অন্যান্য অপরাধ প্রতিরোধ এবং এর শাস্তির বিধানসহ আনুষঙ্গিক বিষয়াদি সম্পর্কে বিধান প্রণয়নের উদ্দেশ্যে মানিলভারিং প্রতিরোধ সংক্রান্ত বিদ্যমান আইন ও অধ্যাদেশ রহিতক্রমে প্রণীত মানিলভারিং প্রতিরোধ আইন, ২০১২ (২০১২ সনের ৫ নং আইন, তারিখ ২০ ফেব্রুয়ারি, ২০১২/৮ ফাল্গুন, ১৪১৮) এবং সন্ত্রাস বিরোধী আইন, ২০০৯ সংশোধনের নিমিত্তে প্রণীত সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১২ (২০১২ সনের ৬ নং আইন, তারিখ ২০ ফেব্রুয়ারি, ২০১২/৮ ফাল্গুন, ১৪১৮) এর বিষয়ে গণপ্রজাতন্ত্রী বাংলাদেশের মহামান্য রাষ্ট্রপতির সম্মতির সূত্রে সর্বসাধারণের অবগতির জন্য বাংলাদেশ গেজেটের অতিরিক্ত সংখ্যায় প্রকাশ করা হয়েছে। উক্ত আইন দুটি বাংলাদেশ ব্যাংকের ওয়েবসাইটে আপলোড করা হয়েছে, যা নিম্নবর্ণিত ওয়েবলিংক হতে ডাইনলোড করা যাবেঃ

www.bangladeshbank.org.bd/aboutus/regulationguideline/lawsacts.php

০২। বর্ণিত আইন দুটি সংশ্লিষ্ট সকলের অবগতিতে আনয়ন করা এবং আইন দুটির বিধানসমূহের পরিপালন নিশ্চিত করার জন্য আপনাদেরকে নির্দেশ প্রদান করা যাচ্ছে।

০৩। গত ৩০ জানুয়ারি, ২০১২ তারিখে বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউট হতে জারীকৃত মানিলভারিং প্রতিরোধ অধ্যাদেশ, ২০১২ ও সন্ত্রাস বিরোধী (সংশোধন) অধ্যাদেশ, ২০১২ বিষয়ক বিএফআইইউ সার্কুলার নং-১/২০১২ এতদসঙ্গে বাতিল বলে গণ্য হবে।

০৪। মানিলভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধের নিমিত্তে বাংলাদেশ ব্যাংক হতে ইতোপূর্বে জারীকৃত সার্কুলার ও সার্কুলার লেটারসমূহ (প্রযোজ্য ক্ষেত্রে) মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২৩(১)(ঘ) ধারায় এবং/বা সন্ত্রাস বিরোধী আইন, ২০০৯ ও তদসঙ্গে পঠিতব্য সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১২ এর ১৫(১)(জ) ধারায় প্রদত্ত ক্ষমতা বলে জারীকৃত মর্মে গণ্য হবে।

০৫। অনুগ্রহপূর্বক প্রাপ্তি স্বীকার করবেন।

আপনাদের বিশ্বস্ত,

(দেবপ্রসাদ দেবনাথ)

মহাব্যবস্থাপক

ফোন : ৭১২০৬৫৯

তারিখ : উল্লিখিত

প্রতিলিপি নং- বিএফআইইউ-২/২০১২-৯৯৫

অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য প্রতিলিপি প্রেরণ করা হলো (জ্যেষ্ঠতার ভিত্তিতে নয়) :-

১. ব্যক্তিগত সহকারী, চেয়ারম্যান, বাংলাদেশ বার কাউন্সিল, বার কাউন্সিল ভবন, ঢাকা।
২. ব্যক্তিগত সহকারী, সচিব, সমাজ কল্যাণ মন্ত্রণালয়, বাংলাদেশ সচিবালয়, ঢাকা।
৩. মহাপরিচালক, এনজিও বিষয়ক ব্যুরো, ঢাকা।
৪. মহাপরিচালক, মহিলা বিষয়ক অধিদপ্তর, ঢাকা।
৫. মহাপরিচালক, সমাজ সেবা বিষয়ক অধিদপ্তর, ঢাকা।
৬. মহাপরিচালক, সমবায় অধিদপ্তর, ঢাকা।
৭. এক্সিকিউটিভ ভাইস চেয়ারম্যান, মাইক্রোক্রেডিট রেগুলেটরী অথরিটি, ঢাকা।
৮. রেজিস্ট্রার, রেজিস্ট্রার অব জয়েন্ট স্টক কোম্পানীজ এন্ড ফার্মস, মতিঝিল, ঢাকা।
৯. চেয়ারম্যান, সিকিউরিটিজ এন্ড এক্সচেঞ্জ কমিশন, দিলকুশা, ঢাকা।
১০. চেয়ারম্যান, বীমা উন্নয়ন ও নিয়ন্ত্রণকারী কর্তৃপক্ষ, মতিঝিল বা/এ, ঢাকা।
১১. প্রেসিডেন্ট, দি ইনস্টিটিউট অব চার্টার্ড একাউন্টেন্টস অব বাংলাদেশ, কাওরান বাজার, ঢাকা।
১২. প্রেসিডেন্ট, দি ইনস্টিটিউট অব কস্ট এন্ড ম্যানেজমেন্ট একাউন্টেন্টস অব বাংলাদেশ, নীলক্ষেত, ঢাকা।
১৩. সকল বিভাগীয় প্রধান, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
১৪. মহাব্যবস্থাপক, বাংলাদেশ ব্যাংক, মতিঝিল, ঢাকা/চট্টগ্রাম/রাজশাহী/খুলনা/বগুড়া/সিলেট/সদরঘাট, ঢাকা/বরিশাল/রংপুর।
১৫. গভর্নর মহোদয়ের সচিবালয়, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
১৬. গভর্নর মহোদয়ের ব্যক্তিগত কর্মকর্তা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
১৭. মহাসচিব, দি ইনস্টিটিউট অব ব্যাংকার্স বাংলাদেশ, বিএসআরএস ভবন, ১০ম তলা, ১২ কাওরান বাজার, তেজগাঁও, ঢাকা।
১৮. চেয়ারম্যান, বাংলাদেশ এসোসিয়েশন অব ব্যাংকস, ৪২, কামাল আতা তুর্ক এডিনিউ, বনানী, ঢাকা।
১৯. চেয়ারম্যান, এসোসিয়েশন অব ব্যাংকার্স, বাংলাদেশ লিমিটেড, ইস্টার্ন কমার্শিয়াল কমপ্লেক্স, ৭৩ কাকরাইল, ঢাকা।

(কামাল হোসেন)

উপ-পরিচালক

ফোন : ৭১২৬১০১-১৪/২৪৮২

বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়, ঢাকা।

ওয়েবসাইট : www.bangladeshbank.org.bd

বিএফআইইউ সার্কুলার নম্বর : ০৪

তারিখ : ০১ আশ্বিন, ১৪১৯
১৬ সেপ্টেম্বর, ২০১২

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল আর্থিক প্রতিষ্ঠান

**Guidance Notes on Prevention of Money Laundering
and Terrorist Financing জারীকরণ প্রসঙ্গে।**

প্রিয় মহোদয়,

মানিলভারিং প্রতিরোধ আইন, ২০১২ ও সন্ত্রাস বিরোধী আইন, ২০০৯ (২০১২ সালের সংশোধনীসহ) এর বিধান মোতাবেক অন্যান্য প্রতিষ্ঠানের ন্যায় বাংলাদেশে কার্যক্রম পরিচালনাকারী সকল আর্থিক প্রতিষ্ঠান (মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২(ছ) ধারায় সংজ্ঞায়িত প্রতিষ্ঠান) রিপোর্ট প্রদানকারী সংস্থা হিসেবে অন্তর্ভুক্ত। ইতোপূর্বে জারীকৃত মানিলভারিং প্রতিরোধ আইন, ২০০২ ও ২০০৯ এবং সন্ত্রাস বিরোধী আইন, ২০০৯ এ আর্থিক প্রতিষ্ঠানসমূহ রিপোর্ট প্রদানকারী সংস্থা হিসেবে অন্তর্ভুক্ত ছিল। উক্ত আইনে প্রদত্ত ক্ষমতা বলে মানিলভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধের নিমিত্তে বাংলাদেশ ব্যাংক কর্তৃক আর্থিক প্রতিষ্ঠানসমূহের পরিপালনের জন্য সময় সময় বিভিন্ন সার্কুলার ও সার্কুলার লেটার জারী করা হয়েছে।

০২। আর্থিক প্রতিষ্ঠানসমূহের ব্যবসার ব্যাপ্তি ও প্রকৃতি, কার্যক্রম পরিচালনার আইনী কাঠামো ইত্যাদি বিবেচনায় এ সকল প্রতিষ্ঠানের মাধ্যমে মানিলভারিং ও সন্ত্রাসে অর্থায়ন সংঘটিত হওয়ার ঝুঁকি মোকাবেলায় আর্থিক প্রতিষ্ঠানসমূহের জন্য 'Guidance Notes on Prevention of Money Laundering and Terrorist Financing' শীর্ষক গাইডেন্স নোটস প্রণয়ন করা হয়েছে যা মানিলভারিং প্রতিরোধ আইন, ২০১২ ও সন্ত্রাস বিরোধী আইন, ২০০৯ (২০১২ সালের সংশোধনীসহ) এর যথাক্রমে ২৩ (ঘ) এবং ১৫ (জ) ধারায় প্রদত্ত ক্ষমতা বলে জারী করা হলো। উক্ত গাইডেন্স নোটস বাংলাদেশ ব্যাংকের ওয়েব সাইট (<http://www.bb.org.bd/mediaroom/circulars/circulars.php>) হতে ডাউনলোড করা যাবে।

০৩। আর্থিক প্রতিষ্ঠানসমূহের মাধ্যমে মানিলভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধের নিমিত্তে সকল আর্থিক প্রতিষ্ঠান নিজ নিজ ব্যবসার ক্ষেত্র, ব্যাপ্তি ও প্রকৃতি পর্যালোচনা করতঃ আলোচ্য গাইডেন্স নোটস এর নির্দেশনা ন্যূনতম মানদণ্ড বিবেচনায় নিজস্ব গাইডেন্স নোটস প্রণয়ন করে স্ব-স্ব পরিচালনা পর্যদ কর্তৃক অনুমোদনপূর্বক আগামী ৩১ অক্টোবর, ২০১২ তারিখের মধ্যে অত্র ইউনিটে দাখিল করবে এবং আগামী ৩০ ডিসেম্বর, ২০১২ তারিখের মধ্যে পরিপালনের প্রয়োজনীয় ব্যবস্থা গ্রহণ করবে।

০৪। ইত্যবসরে বিষয়টি সকল পক্ষকে অবহিত করবেন।

(দেবপ্রসাদ দেবনাথ)

মহাব্যবস্থাপক

ফোন : ৯৫৩০১১৮

প্রতিলিপি নং- বিএফআইইউ -১/১/২০১২-

তারিখ : উল্লিখিত

অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য প্রতিলিপি প্রেরণ করা হলো :-

১. নির্বাহী পরিচালক, বাংলাদেশ ব্যাংক, মতিঝিল, ঢাকা/চট্টগ্রাম।
২. নির্বাহী পরিচালক, গভর্নর মহোদয়ের সচিবালয়, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৩. সকল বিভাগীয় প্রধান, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৪. মহাব্যবস্থাপক, বাংলাদেশ ব্যাংক, রাজশাহী/খুলনা/বগুড়া/সিলেট/সদরঘাট, ঢাকা/বরিশাল/রংপুর।
৫. গভর্নর মহোদয়ের ব্যক্তিগত কর্মকর্তা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৬. ডেপুটি গভর্নর মহোদয়গণের সাথে সংযুক্ত উপ-পরিচালক/সহকারী পরিচালক, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৭. অর্থনৈতিক উপদেষ্টা/নির্বাহী পরিচালক মহোদয়গণের ব্যক্তিগত সহকারী, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৮. মহাপরিচালক, বাংলাদেশ ইনস্টিটিউট অব ব্যাংক ম্যানেজমেন্ট, মিরপুর, ঢাকা।
৯. মহাসচিব, দি ইনস্টিটিউট অব ব্যাংকার্স বাংলাদেশ, বিএসআরএস ভবন, ১০ম তলা, ১২, কাওরান বাজার, তেজগাঁও, ঢাকা।
১০. চেয়ারম্যান, বাংলাদেশ এসোসিয়েশন অব ব্যাংকস, ৪২, কামাল আতাতুর্ক এভিনিউ, বনানী, ঢাকা।
১১. চেয়ারম্যান, এসোসিয়েশন অব ব্যাংকার্স, বাংলাদেশ, ইস্টার্ন কমার্শিয়াল কমপ্লেক্স, ৭৩, কাকরাইল, ঢাকা।
১২. চেয়ারম্যান, বাংলাদেশ লীজিং এন্ড ফিন্যান্স কোম্পানীজ এসোসিয়েশন, ৬৩, দিলকুশা বা/এ (৪র্থ তলা), ঢাকা-১০০০।
১৩. ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা, সকল তফসিলী ব্যাংক।
১৪. ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা, সকল আর্থিক প্রতিষ্ঠান।

(কামাল হোসেন)

উপ-পরিচালক

ফোন : ৯৫৩০০১০-৭৫/২৪৮২

ই-মেইল: kamal.hossain@bb.org.bd

বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট

বাংলাদেশ ব্যাংক

প্রধান কার্যালয়, ঢাকা।

ওয়েবসাইট : www.bangladeshbank.org.bd

বিএফআইইউ সার্কুলার নম্বর : ৭

৩০ আষাঢ়, ১৪২০

তারিখ : ১৪ জুলাই, ২০১৩

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা/প্রতিষ্ঠান প্রধান

সকল ব্যাংক, আর্থিক প্রতিষ্ঠান, বীমাকারী, মানি চেঞ্জার, অর্থ অথবা অর্থমূল্য প্রেরণকারী বা স্থানান্তরকারী যে কোন কোম্পানী বা প্রতিষ্ঠান, বাংলাদেশ ব্যাংকের অনুমতিক্রমে ব্যবসা পরিচালনাকারী অন্য কোন প্রতিষ্ঠান, স্টক ডিলার ও স্টক ব্রোকার, পোর্টফোলিও ম্যানেজার ও মার্চেন্ট ব্যাংকার, সিকিউরিটি কাস্টডিয়ান, সম্পদ ব্যবস্থাপক, অ-লাভজনক সংস্থা/প্রতিষ্ঠান (Non Profit Organisation), বেসরকারি উন্নয়ন সংস্থা (Non Government Organisation), সমবায় সমিতি, রিয়েল এস্টেট ডেভেলপার, মূল্যবান ধাতু বা পাথরের ব্যবসায়ী, ট্রাস্ট ও কোম্পানী সেবা প্রদানকারী, আইনজীবী, নোটারী, অন্যান্য আইন পেশাজীবী এবং একাউন্টেন্ট।

সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১৩ প্রসঙ্গে।

সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধিকতর সংশোধনকল্পে গত ১১ জুন, ২০১৩ তারিখে জাতীয় সংসদ কর্তৃক গৃহীত সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১৩ গত ১২ জুন, ২০১৩ তারিখে মহামান্য রাষ্ট্রপতির সম্মতি লাভ করায় সর্বসাধারণের অবগতির জন্য বাংলাদেশ গেজেটের অতিরিক্ত সংখ্যায় প্রকাশিত হয়েছে। আলোচ্য আইনটি জারী হওয়ায় রিপোর্ট প্রদানকারী সংস্থার দায়িত্ব ও কর্তব্য বিস্তৃত হয়েছে। উক্ত আইনের বিধানাবলী পরিপালন ও সংশ্লিষ্ট সকলের অবগতিতে আনয়নের সুবিধার্থে উক্ত আইনটি বাংলাদেশ ব্যাংকের ওয়েবসাইটে আপলোড করা হয়েছে, যা <http://www.bb.org.bd/aboutus/regulationguideline/lawsnaacts.php> ওয়েবলিংক হতে ডাউনলোড করা যাবে।

০২। বর্ণিত আইনটি সংশ্লিষ্ট সকলের অবগতিতে আনয়ন এবং এর বিধানসমূহের পরিপালন নিশ্চিত করার জন্য আপনাদেরকে নির্দেশ প্রদান করা যাচ্ছে।

০৩। অনুগ্রহপূর্বক প্রাপ্তি স্বীকার করবেন।

আপনাদের বিশ্বস্ত,

স্বাক্ষরিত/--

(কাজী আকতারুল ইসলাম)

উপ-মহাব্যবস্থাপক

ফোন : ৯৫৩০১৭০

বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউট

বাংলাদেশ ব্যাংক

প্রধান কার্যালয়

ঢাকা

www.bangladeshbank.org.bd

বিএফআইইউ সার্কুলার লেটার নং-০৩/২০১৫

তারিখ : ২৬ চৈত্র, ১৪২১
০৯ এপ্রিল, ২০১৫

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা

সকল রিপোর্ট প্রদানকারী সংস্থা

(মানিলভারিং প্রতিরোধ আইন, ২০১২ ও সন্ত্রাস বিরোধী আইন, ২০০৯ এর আওতায়) বাংলাদেশ।

মানিলভারিং প্রতিরোধ বিধিমালা, ২০১৩ এবং সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ প্রসঙ্গে।

প্রিয় মহোদয়,

মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২৯ ধারায় প্রদত্ত ক্ষমতাবলে গত ২১ নভেম্বর, ২০১৩ তারিখে গণপ্রজাতন্ত্রী বাংলাদেশ সরকারের পক্ষে ব্যাংক ও আর্থিক প্রতিষ্ঠান বিভাগ, অর্থ মন্ত্রণালয় মানিলভারিং প্রতিরোধ বিধিমালা, ২০১৩ জারী করেছে যা গত ২৯ জানুয়ারি, ২০১৪ তারিখে বাংলাদেশ গেজেটের অতিরিক্ত সংখ্যায় প্রকাশিত হয়েছে।

০২। সন্ত্রাস বিরোধী আইন, ২০০৯ এর ৪৩ ধারায় প্রদত্ত ক্ষমতাবলে গত ১৩ অক্টোবর, ২০১৩ তারিখে গণপ্রজাতন্ত্রী বাংলাদেশ সরকারের পক্ষে স্বরাষ্ট্র মন্ত্রণালয় সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ জারী করেছে যা গত ০৯ নভেম্বর, ২০১৩ তারিখে বাংলাদেশ গেজেটের অতিরিক্ত সংখ্যায় প্রকাশিত হয়েছে।

০৩। আলোচ্য বিধিমালা দু'টি জারী হওয়ায় রিপোর্ট প্রদানকারী সংস্থাসমূহের দায়িত্ব ও কর্তব্য বিস্তৃত হয়েছে। উক্ত বিধিমালা দু'টির বিধানসমূহ পরিপালন ও সংশ্লিষ্ট সকলের অবগতিতে আনয়নের সুবিধার্থে বিধান দু'টি বাংলাদেশ ব্যাংকের ওয়েবসাইটে আপলোড করা হয়েছে, যা http://www.bb.org.bd/aboutus/dept/bfiu/laws_bfiu.php ওয়েবলিংকে পাওয়া যাবে।

০৪। এক্ষণে বর্ণিত বিধিমালা দু'টি সংশ্লিষ্ট সকলের অবগতিতে আনয়ন এবং এর বিধানসমূহের পরিপালন নিশ্চিত করার জন্য আপনাদেরকে পরামর্শ প্রদান করা হলো।

আপনাদের বিশ্বস্ত,



(মোঃ নাসিরুজ্জামান)

মহাব্যবস্থাপক

ফোনঃ ৯৫৩০১১৮

বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা

www.bangladeshbank.org.bd

বিএফআইইউ সার্কুলার নং-১২

তারিখ : ১৫ আষাঢ়, ১৪২২
২৯ জুন, ২০১৫

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল আর্থিক প্রতিষ্ঠান

মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে আর্থিক প্রতিষ্ঠানসমূহের জন্য
অনুসরণীয় নির্দেশনাসমূহ সম্পর্কিত মাস্টার সার্কুলার

প্রিয় মহোদয়,

মানিলভারিং প্রতিরোধ আইন, ২০১২ ও সন্ত্রাস বিরোধী আইন, ২০০৯ (২০১২ ও ২০১৩ সালের সংশোধনীসহ) এর উদ্দেশ্য পূরণকল্পে এবং উক্ত আইন ও আইনের আওতায় জারীকৃত বিধিমালার সংশ্লিষ্ট বিধানাবলী পরিপালনে আর্থিক প্রতিষ্ঠানসমূহের জন্য অনুসরণীয় নিম্নবর্ণিত নির্দেশনাসমূহ মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২৩(১)(ঘ) এবং সন্ত্রাস বিরোধী আইন, ২০০৯ এর ১৫(১)(জ) ধারায় প্রদত্ত ক্ষমতা বলে জারী করা হলোঃ

১। পরিপালন কাঠামো

১.১ মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালা

মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে আন্তর্জাতিক মানদণ্ড, দেশে বিদ্যমান আইন, বিধিমালা ও বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট (বিএফআইইউ)-এর নির্দেশনাবলীর সমন্বয়ে প্রতিটি আর্থিক প্রতিষ্ঠানের নিজস্ব নীতিমালা থাকবে যা তাদের পরিচালনা পর্যদ বা প্রযোজ্য ক্ষেত্রে প্রতিষ্ঠানের সর্বোচ্চ ব্যবস্থাপনা কমিটি কর্তৃক অনুমোদিত হবে এবং তা' সংশ্লিষ্ট সকলের অবগতিতে আনতে হবে। আর্থিক প্রতিষ্ঠান সময় সময় নীতিমালাটি পর্যালোচনা করবে এবং প্রয়োজনীয় ক্ষেত্রে সংশোধন/পরিমার্জন করবে।

১.২ মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে অঙ্গীকার ঘোষণা

আর্থিক প্রতিষ্ঠানের প্রধান নির্বাহী বাৎসরিক ভিত্তিতে প্রতিষ্ঠানের সকল বিভাগ/শাখার কর্মকর্তা/কর্মচারীদের উদ্দেশ্যে মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে সুস্পষ্ট ও কার্যকর অঙ্গীকার ঘোষণা করবেন এবং অঙ্গীকার বাস্তবায়নে যথাযথ নির্দেশনা প্রদান করবেন।

১.৩ কেন্দ্রীয় পরিপালন ইউনিট (Central Compliance Unit)

- (১) আর্থিক প্রতিষ্ঠানগুলোকে মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক ঝুঁকি হতে মুক্ত রাখার জন্য এবং মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা এবং বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনাবলী যথাযথভাবে পরিপালনার্থে প্রতিটি আর্থিক প্রতিষ্ঠানে একজন উর্ধ্বতন কর্মকর্তার নেতৃত্বে প্রধান কার্যালয়ে একটি 'কেন্দ্রীয় পরিপালন ইউনিট' (Central Compliance Unit) প্রতিষ্ঠা করবে যা সরাসরি প্রতিষ্ঠানের ব্যবস্থাপনা পরিচালক বা প্রধান নির্বাহী কর্মকর্তা কর্তৃক তত্ত্বাবধান করতে হবে। উল্লিখিত 'উর্ধ্বতন কর্মকর্তা' প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা (Chief Anti Money Laundering Compliance Officer-CAMLCO) নামে অভিহিত হবেন। এক্ষেত্রে 'উর্ধ্বতন কর্মকর্তা' বলতে আর্থিক প্রতিষ্ঠানের ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তার অব্যবহিত নীচের ৩ (তিন) ধাপ পর্যন্ত পদমর্যাদার কর্মকর্তাগণ বিবেচিত হবেন। কেন্দ্রীয় পরিপালন ইউনিটে উপ-প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা (Deputy Chief Anti Money Laundering Compliance Officer-DCAMLCO) হিসেবে উপযুক্ত কর্মকর্তাকে মনোনয়ন প্রদান করা যাবে।
- (২) প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তার ন্যূনতম ৭ (সাত) বছরের অভিজ্ঞতা (ব্যাংক/আর্থিক প্রতিষ্ঠানে) থাকতে হবে, তন্মধ্যে কমপক্ষে ৩ (তিন) বছর ব্যবস্থাপনা পর্যায়ে কর্মরত হতে হবে। উপ-প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা নিয়োগের ক্ষেত্রে ন্যূনতম ৫ (পাঁচ) বছরের অভিজ্ঞতা (ব্যাংক/আর্থিক প্রতিষ্ঠানে) থাকতে হবে।

- (৩) প্রধান এবং উপ-প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তার মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনাবলী ও এতদ্বিষয়ে আন্তর্জাতিক মানদণ্ডসমূহের উপর সম্যক ধারণা থাকতে হবে। উক্ত কর্মকর্তাদেরকে প্রতিষ্ঠানের অন্য কোন দায়িত্ব অর্পণের পূর্বে ব্যবস্থাপনা কর্তৃপক্ষকে নিশ্চিত হতে হবে যে এর ফলে প্রতিষ্ঠানটির মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কার্যক্রম বিঘ্নিত হবে না। প্রধান এবং উপ-প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা সম্পর্কিত তথ্যাদি (পরিশিষ্ট-ক) প্রতিবছর জানুয়ারি মাসের প্রথমার্ধে লিখিতভাবে বিএফআইইউ-কে অবহিত করতে হবে।
- (৪) প্রতিটি আর্থিক প্রতিষ্ঠান নিজ প্রতিষ্ঠানের আকার, ব্যাপ্তি, কার্যক্রম, গ্রাহকের সংখ্যা ইত্যাদি বিবেচনাপূর্বক কেন্দ্রীয় পরিপালন ইউনিটে উপযুক্ত সংখ্যক কর্মকর্তা/কর্মচারী নিয়োগ করবে। উল্লেখ্য, কেন্দ্রীয় পরিপালন ইউনিট ও অভ্যন্তরীণ নিরীক্ষা বিভাগ সম্পূর্ণ পৃথক দুইটি ইউনিট বা বিভাগ হিসেবে মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কার্যক্রম সম্পাদন করবে।
- (৫) মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে আর্থিক প্রতিষ্ঠানগুলো প্রাতিষ্ঠানিক কৌশল ও কর্মসূচী নির্ধারণ করবে এবং সময় সময় তা পর্যালোচনা করবে। কেন্দ্রীয় পরিপালন ইউনিট মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কর্মসূচীর বাস্তবায়ন নিশ্চিত করবে।
- (৬) কেন্দ্রীয় পরিপালন ইউনিট মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে আর্থিক প্রতিষ্ঠানের গৃহীত পদক্ষেপ, এ বিষয়ে বাস্তবায়ন অগ্রগতি ও সুপারিশ সম্বলিত প্রতিবেদন ষান্মাসিক ভিত্তিতে (জানুয়ারি-জুন, জুলাই-ডিসেম্বর) প্রতিষ্ঠানের প্রধান নির্বাহীর অবগতি ও নির্দেশনার জন্য দাখিল করবে। উক্ত প্রতিবেদনে এ সার্কুলারের ৮.৩(১) এ বর্ণিত বিষয়সমূহসহ মানিলভারিং এবং সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিএফআইইউ কর্তৃক কোন ব্যবস্থা গৃহীত হয়ে থাকলে তা অন্তর্ভুক্ত করতে হবে। প্রধান নির্বাহীর নির্দেশনা ও মতামতসহ প্রতিবেদনটি প্রতিষ্ঠানের পরিচালনা পর্ষদ বা সর্বোচ্চ ব্যবস্থাপনা কমিটির সভায় উপস্থাপন করতে হবে এবং প্রতিবেদনটির একটি কপি সংশ্লিষ্ট ষান্মাসিক শেষ হওয়ার ২ (দুই) মাসের মধ্যে বিএফআইইউ বরাবরে প্রেরণ করতে হবে।
- (৭) কেন্দ্রীয় পরিপালন ইউনিট নিম্নে উল্লিখিত ১.৪ অনুচ্ছেদের নির্দেশনা মোতাবেক শাখা পর্যায়ে পরিপালন কর্মকর্তা মনোনয়নের মাধ্যমে অভ্যন্তরীণ নিরীক্ষণ ও নিয়ন্ত্রণ ব্যবস্থা প্রতিষ্ঠা করবে। এক্ষেত্রে নির্দিষ্ট কর্মকর্তাকে মনোনয়নপূর্বক মনোনীত কর্মকর্তাকে তার দায়িত্বসমূহ লিখিতভাবে অবহিত করবে।
- (৮) কেন্দ্রীয় পরিপালন ইউনিট শাখাসমূহের জন্য অনুসরণীয় নির্দেশনাবলী জারী করবে যেখানে মানিলভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধে লেনদেন নিরীক্ষণ ব্যবস্থা, অভ্যন্তরীণ নিয়ন্ত্রণ ব্যবস্থা, নীতি ও পদ্ধতিসমূহ অন্তর্ভুক্ত থাকবে।
- (৯) মানিলভারিং, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়ন এবং মানিলভারিং প্রতিরোধ আইন, ২০১২ এ উল্লিখিত সম্পৃক্ত অপরাধ সম্পর্কিত কোন সংবাদ গণমাধ্যমে প্রকাশ হবার সাথে সাথে উক্ত কর্মকর্তাদের সাথে জড়িত কোন ব্যক্তি বা সত্তার কোন হিসাব (আমানত/ঋণ) পরিচালিত হয়ে থাকলে এ বিষয়ক বিস্তারিত তথ্য সংশ্লিষ্ট আর্থিক প্রতিষ্ঠানের কেন্দ্রীয় পরিপালন ইউনিট কর্তৃক অবিলম্বে বিএফআইইউ বরাবরে প্রেরণ করতে হবে এবং প্রয়োজনবোধে সন্দেহজনক লেনদেন রিপোর্ট দাখিল করতে হবে।

১.৪ শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা

- (১) মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ এর নির্দেশনাবলী এবং আর্থিক প্রতিষ্ঠানের নিজস্ব নীতিমালা বাস্তবায়নের জন্য প্রতিষ্ঠানের প্রতিটি শাখায় একজন অভিজ্ঞ শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা (Branch Anti Money Laundering Compliance Officer-BAMLCO) মনোনীত করতে হবে।
- (২) শাখার অভিজ্ঞ কোন উর্ধ্বতন কর্মকর্তাকে শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা হিসেবে মনোনীত করতে হবে। উল্লেখ্য, শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তার ন্যূনতম ৩ (তিন) বছরের অভিজ্ঞতা (ব্যাংক/আর্থিক প্রতিষ্ঠানে) থাকতে হবে এবং মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ এর সকল নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালার বিষয়ে সম্যক ধারণা থাকতে হবে। শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তার মনোনয়নপত্রে তার কর্মপরিধি এবং দায় দায়িত্ব সুনির্দিষ্টভাবে উল্লেখ থাকতে হবে। শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তার উপর অর্পিত দায়িত্ব যথাযথভাবে পরিপালনের জন্য সংশ্লিষ্ট আর্থিক প্রতিষ্ঠান কর্তৃক উক্ত কর্মকর্তাকে সর্বপ্রকার সহযোগিতা নিশ্চিত করতে হবে।
- (৩) শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা শাখার অন্যান্য সংশ্লিষ্ট গুরুত্বপূর্ণ কর্মকর্তাদের নিয়ে ত্রৈমাসিক ভিত্তিতে মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক সভা করবেন এবং উক্ত সভায় নিম্নোক্ত বিষয়সমূহসহ মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে বিদ্যমান আইন, বিধিমালা এবং বিএফআইইউ এর অন্যান্য নির্দেশনার পরিপালন পর্যালোচনাপূর্বক যথাযথ ব্যবস্থা গ্রহণ করবেন :
 - গ্রাহক পরিচিতি (KYC)
 - লেনদেন মনিটরিং (Transaction Monitoring)

- সন্দেহজনক লেনদেন বা কার্যক্রম চিহ্নিতকরণ ও রিপোর্টিং (STR/SAR)
- রেকর্ড সংরক্ষণ (Record Keeping)
- প্রশিক্ষণ (Training)

২। গ্রাহক নির্বাচন নীতিমালা

গ্রাহক নির্বাচনের ক্ষেত্রে প্রতিটি আর্থিক প্রতিষ্ঠানের একটি সুনির্দিষ্ট নীতিমালা থাকতে হবে। উক্ত নীতিমালায় অন্যান্য বিষয়ের সাথে আবশ্যিকভাবে নিম্নোক্ত বিষয়সমূহ অন্তর্ভুক্ত থাকবে :

- (১) বেনামে বা ছদ্মনামে বা শুধুমাত্র নম্বরযুক্ত কোন গ্রাহকের হিসাব খোলা যাবে না।
- (২) জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস ও সন্ত্রাসী কার্যে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার কোন হিসাব খোলা যাবে না বা পরিচালনা করা যাবে না। জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তা বলতে সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ এর ২ (ছ) নং বিধিতে সংজ্ঞায়িত রেজুলেশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তাকে বুঝাবে। এই তালিকাসমূহ http://www.un.org/sc/committees/list_compend.shtml ওয়েবলিংক হতে সংগ্রহ করা যাবে। বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তা বলতে সন্ত্রাস বিরোধী আইন, ২০০৯ এর ১৮ নং ধারায় প্রদত্ত ক্ষমতাবলে বাংলাদেশ সরকার কর্তৃক সময়ে সময়ে সরকারি গেজেট প্রজ্ঞাপন দ্বারা তফসিলভুক্ত কোন ব্যক্তি বা সত্তাকে বুঝাবে।
- (৩) অনিবাসী বাংলাদেশীদের হিসাব খোলার ক্ষেত্রে Foreign Exchange Regulation Act, 1947 এর বিধানাবলী ও এর আওতায় বাংলাদেশ ব্যাংক কর্তৃক জারীকৃত নির্দেশনাসমূহ অনুসরণীয় হবে।

৩। গ্রাহক পরিচিতি

মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে এবং আর্থিক প্রতিষ্ঠান খাতকে এ বিষয়ক ঝুঁকি হতে মুক্ত রাখার জন্য গ্রাহক পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংগ্রহ করতে হবে। আর্থিক প্রতিষ্ঠানসমূহ যাতে মানিলভারিং বা সন্ত্রাসী কার্যে অর্থায়নের ঝুঁকির সম্মুখীন না হয় তা নিশ্চিত করার জন্য প্রতিটি আর্থিক প্রতিষ্ঠানকে গ্রাহকের যথাযথ পরিচিতি গ্রহণ এবং যাচাই প্রক্রিয়া (Know Your Customer-KYC) সম্পাদন করতে হবে।

৩.১ গ্রাহকের সংজ্ঞা

মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন ঝুঁকি ব্যবস্থাপনায় গ্রাহক পরিচিতি ও যাচাই প্রক্রিয়ার ক্ষেত্রে গ্রাহক বলতে নিম্নোক্ত ব্যক্তি বা সত্তাকে বুঝাবে :

- (১) আর্থিক প্রতিষ্ঠানের সাথে কোনরূপ আমানত/ঋণ বা বিনিয়োগ হিসাব পরিচালনা বা সংরক্ষণ করে এমন যে কোন ব্যক্তি বা সত্তা;
- (২) হিসাব বা ব্যবসায়িক সম্পর্কের প্রকৃত সুবিধাভোগী (Beneficial Owner) বা তৃতীয় কোন ব্যক্তি বা সত্তা যার পক্ষে হিসাব পরিচালিত হয়;
- (৩) বিদ্যমান আইনী কাঠামোর আওতায় হিসাব/ব্যবসায়িক সম্পর্ক কোন পেশাদার মধ্যস্থতাকারী কর্তৃক পরিচালিত হলে উক্ত হিসাব বা ব্যবসায়িক সম্পর্কের প্রকৃত সুবিধাভোগী।

৩.২ Customer Due Diligence

১) Customer Due Diligence (CDD) বলতে নির্ভরযোগ্য ও স্বাধীন উৎস হতে প্রাপ্ত তথ্য, উপাত্ত ও দলিলাদির ভিত্তিতে গ্রাহকের পরিচিতি যাচাইকরণ ও সনাক্তকরণসহ হিসাবের লেনদেন মনিটরিং করাকে বুঝাবে। উল্লেখ্য যে, গ্রাহকের যথাযথ পরিচিতি গ্রহণ এবং যাচাইকরণ (KYC), CDD প্রক্রিয়ার একটি অংশ।

২) গ্রাহকের ঝুঁকি বিবেচনায় নিম্নবর্ণিত বিভিন্ন পর্যায়ে CDD সম্পাদন করতে হবে-

- (ক) গ্রাহকের সাথে সম্পর্ক স্থাপনের সময়;
- (খ) বিদ্যমান গ্রাহকের সাথে আর্থিক লেনদেন সংঘটনের সময়;
- (গ) যখন সন্দেহ করার যথেষ্ট কারণ থাকবে যে ইতোপূর্বে গ্রাহকের পরিচিতির স্বপক্ষে যে তথ্য বা দলিলাদি সংগ্রহ করা হয়েছে তা পর্যাপ্ত নয় বা সঠিক নয়; এবং
- (ঘ) কোন লেনদেন মানিলভারিং বা সন্ত্রাসী কার্যে অর্থায়নের সাথে জড়িত এরূপ সন্দেহ হলে।

৩) গ্রাহকের পরিচিতি এবং আর্থিক প্রতিষ্ঠানের সাথে সম্পর্ক স্থাপনের অন্তর্নিহিত উদ্দেশ্য সম্পর্কে নিশ্চিত হওয়ার জন্য প্রত্যেক সংস্থা তাদের সন্তুষ্টি সাপেক্ষে পর্যাপ্ত (পূর্ণাঙ্গ ও সঠিক) তথ্য সংগ্রহ করবে। “সংস্থার সন্তুষ্টি সাপেক্ষে” বলতে বিদ্যমান নির্দেশনার

আলোকে গ্রাহকের ঝুঁকি বিবেচনায় নিয়ে প্রয়োজনীয় তথ্য, উপাত্ত ও দলিলাদি সংগ্রহপূর্বক CDD সম্পন্ন করা হয়েছে মর্মে যথাযথ কর্তৃপক্ষকে সন্তুষ্ট করাকে বুঝাবে। “পূর্ণাঙ্গ (Complete)” বলতে প্রয়োজ্য ব্যক্তি/সংস্থার পরিচিতি যাচাইকল্পে প্রয়োজনীয় সকল তথ্যের সন্নিবেশকে বুঝাবে। উদাহরণস্বরূপঃ ব্যক্তির (সত্তার নামে পরিচালিত হিসাবের ক্ষেত্রে সংশ্লিষ্ট ব্যক্তি/ব্যক্তিবর্গের) নাম ও বিস্তারিত ঠিকানা, পাসপোর্ট/জাতীয় পরিচয়পত্র/জন্ম নিবন্ধন সনদ/গ্রহণযোগ্য পরিচিতিমূলক ছবিযুক্ত আইডি কার্ড, ফোন/মোবাইল নম্বর ইত্যাদি। “সঠিক (Accurate)” বলতে পূর্ণাঙ্গ এরূপ তথ্যকে বুঝাবে যার সঠিকতা যাচাই করা হয়েছে।

- ৪) যদি গ্রাহকের পক্ষে অন্য কোন ব্যক্তি হিসাব পরিচালনা করে/ব্যবসায়িক সম্পর্ক স্থাপন করে সেক্ষেত্রে উক্ত ব্যক্তি যথাযথভাবে ক্ষমতাপ্রাপ্ত কিনা তা নিশ্চিত হয়ে তার পরিচিতির পূর্ণাঙ্গ ও সঠিক তথ্য সংগ্রহ করতে হবে।
- ৫) ট্রাস্টি ও পেশাদার মধ্যস্থতাকারী কর্তৃক গ্রাহকের পক্ষে পরিচালিত হিসাবের ক্ষেত্রে/ব্যবসায়িক সম্পর্ক স্থাপনের ক্ষেত্রে তাদের আইনগত অবস্থান পর্যালোচনা ও তার যথার্থতা নিরূপণপূর্বক সংশ্লিষ্ট সকলের পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংগ্রহ করতে হবে।
- ৬) যেসব দেশ মানিলাভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের আন্তর্জাতিক মান পূরণ করেনি বা তাৎপর্যপূর্ণ/উল্লেখযোগ্য পরিমাণ ঘাটতি রয়েছে (যেমন : ফাইন্যান্সিয়াল অ্যাকশন টাঙ্কফোর্সের পাবলিক ডকুমেন্টে High Risk and Non-Cooperative Jurisdictions হিসেবে তালিকাভুক্ত দেশ) সেসব দেশের কোন ব্যক্তি বা সত্তার (আইনগত প্রতিনিধি, আর্থিক প্রতিষ্ঠানসহ যে কোন প্রতিষ্ঠান) সাথে ব্যবসায়িক সম্পর্ক স্থাপন ও বজায় রাখা এবং লেনদেন সম্পাদনের ক্ষেত্রে অধিকতর সতর্কতামূলক Enhanced Due Diligence (৩.৪ নং অনুচ্ছেদ অনুযায়ী) সম্পন্ন করতে হবে।
- ৭) হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সনাক্তকরণপূর্বক সংস্থার সন্তুষ্টি সাপেক্ষে নির্ভরযোগ্য সূত্র হতে সংগৃহীত তথ্যের ভিত্তিতে নিম্নোক্ত ক্ষেত্রে পরিচিতি নিশ্চিত করতে হবে :
 - ক) যদি কোন গ্রাহক অন্য কোন ব্যক্তির পক্ষে হিসাব/ব্যবসায়িক সম্পর্ক পরিচালনা করে, সে ক্ষেত্রে গ্রাহক ছাড়াও উক্ত ব্যক্তির পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংগ্রহ ও সংরক্ষণ করতে হবে;
 - খ) যদি কোন হিসাবের অর্থের উৎস হিসাবধারী ব্যতীত অন্য কোন ব্যক্তি হয় সে ক্ষেত্রে হিসাবের অর্থ যোগানদাতার পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংগ্রহ ও সংরক্ষণ করতে হবে; এবং
 - গ) কোম্পানীর ক্ষেত্রে নিয়ন্ত্রণকারী শেয়ার হোল্ডার অথবা ২০% বা তদুর্ধ্ব একক শেয়ারহোল্ডারকে হিসাবের প্রকৃত সুবিধাভোগী বিবেচনায় তার/তাদের পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংগ্রহ ও সংরক্ষণ করতে হবে।

৩.৩ Customer Due Diligence সম্পাদন করা সম্ভব না হলে রিপোর্ট প্রদানকারী সংস্থার করণীয়

গ্রাহকের অসহযোগিতাপূর্ণ আচরণের কারণে অথবা গ্রাহকের বিষয়ে সংগৃহীত তথ্য/উপাত্ত নির্ভরযোগ্য না হলে অর্থাৎ গ্রাহক পরিচিতির সন্তোষজনক তথ্য প্রাপ্তি এবং তা যাচাই সাপেক্ষে CDD সম্পাদন করা সম্ভব না হলে আর্থিক প্রতিষ্ঠানসমূহ নিম্নরূপ ব্যবস্থা গ্রহণ করবেঃ

- ১) আর্থিক প্রতিষ্ঠানগুলো উক্তরূপ গ্রাহকের হিসাব খুলবে না বা প্রয়োজনে বিদ্যমান হিসাব বন্ধ করে দিবে অথবা কোন ব্যবসায়িক সম্পর্ক স্থাপন করবে না;
- ২) বিদ্যমান এরূপ হিসাব বন্ধ করার ক্ষেত্রে উর্ধ্বতন কর্তৃপক্ষের অনুমোদন গ্রহণ করতে হবে এবং হিসাব বন্ধ করার পূর্বে হিসাব বন্ধকরণের কারণ ব্যাখ্যাপূর্বক গ্রাহককে নোটিশ প্রদান করতে হবে;
- ৩) ক্ষেত্রমত এরূপ গ্রাহকের বিষয়ে সন্দেহজনক লেনদেন রিপোর্ট দাখিল করতে হবে।

৩.৪ Enhanced Due Diligence

প্রতিটি আর্থিক প্রতিষ্ঠান এর গ্রাহক/ব্যবসায়িক সম্পর্ক স্থাপনকারী ব্যক্তির সকল জটিল, অস্বাভাবিক বা বৃহদাংকের লেনদেন (যেসব ক্ষেত্রে যথাযথ আর্থিক বা আইনগত উদ্দেশ্য অনুপস্থিত) নিয়মিতভাবে পর্যবেক্ষণ করবে। যেসকল ক্ষেত্রে মানিলাভারিং ও সন্ত্রাসে অর্থায়নের ঝুঁকি অধিকতর মর্মে প্রতীয়মান হয় সেসব ক্ষেত্রে আর্থিক প্রতিষ্ঠানকে Enhanced CDD সম্পাদন করতে হবে। এক্ষেত্রে আর্থিক প্রতিষ্ঠানগুলো অস্বাভাবিক/সন্দেহজনক লেনদেন চিহ্নিতকরণের নিমিত্তে গ্রাহকের হিসাব/ব্যবসায়িক সম্পর্ক/লেনদেন নিয়মিত ও নিবিড়ভাবে পর্যবেক্ষণ করবে। Enhanced CDD এর জন্য রিপোর্ট প্রদানকারী সংস্থাগুলো নিম্নবর্ণিত নির্দেশনা অনুসরণ করবে-

- ১) গ্রাহক/ব্যবসায়িক সম্পর্ক স্থাপনকারী ব্যক্তি/সত্তার সম্বন্ধে অতিরিক্ত তথ্য (পেশা, সম্পদের পরিমাণ, লেনদেনের ব্যাখ্যা ইত্যাদি) সংগ্রহ করবে এবং নিয়মিত বিরতিতে তা হালনাগাদ করবে;
- ২) আর্থিক প্রতিষ্ঠানের উপযুক্ত উর্ধ্বতন কর্তৃপক্ষের অনুমোদন সাপেক্ষে ব্যবসায়িক সম্পর্ক স্থাপন করতে হবে।

৩.৫ গ্রাহকের হিসাব পরিচালনা সংক্রান্ত নিয়মাবলী

- (১) প্রতিটি আর্থিক প্রতিষ্ঠান গ্রাহকের হিসাব খোলার ক্ষেত্রে ‘পরিশিষ্ট-খ’ এ সংযুক্ত হিসাব খোলার ফরমের আলোকে প্রণীত নিজস্ব ফরম ব্যবহার করবে। গ্রাহক পরিচিতি এবং Customer Due diligence (CDD) যথাযথভাবে সম্পাদন করার জন্য উক্ত হিসাব খোলার

ফরম ব্যবহারপূর্বক প্রত্যেক আর্থিক প্রতিষ্ঠান তার গ্রাহকের পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংগ্রহ করবে এবং গ্রাহকের ঝুঁকি বিবেচনায় ৩.২ অনুচ্ছেদে উল্লিখিত CDD সম্পন্ন করার নির্দিষ্ট সময়ের মধ্যে সংগৃহীত তথ্যের সঠিকতা যাচাইসহ CDD সম্পাদনপূর্বক তথ্য ও দলিলাদি সংরক্ষণ করবে। এক্ষেত্রে আর্থিক প্রতিষ্ঠান কোনক্রমেই উক্ত ফরমে উল্লিখিত তথ্যের কম তথ্য সংগ্রহ করবে না। তবে প্রত্যেক আর্থিক প্রতিষ্ঠান যথাযথভাবে গ্রাহকের পরিচিতি ও CDD সম্পাদন করার উদ্দেশ্যে প্রতিষ্ঠানের সম্ভ্রুতি সাপেক্ষে উক্ত ফরমে বর্ণিত তথ্যের অতিরিক্ত তথ্য সংগ্রহ করতে পারবে। “সংস্থার সম্ভ্রুতি সাপেক্ষে” এর ব্যাখ্যা ৩.২ (৩) অনুচ্ছেদে প্রদান করা হয়েছে।

- (২) সকল আর্থিক প্রতিষ্ঠান অভিন্ন হিসাব খোলার ফরম ও KYC ফরম যথাশীঘ্র প্রচলন করবে, তবে ১৫ জুলাই, ২০১৫ তারিখের মধ্যে অবশ্যই তা সম্পন্ন করতে হবে এবং নতুনভাবে মুদ্রিত ফরমের এক সেট এ ইউনিটে দাখিল করতে হবে।
- (৩) একই প্রতিষ্ঠানে একই গ্রাহকের একাধিক হিসাব পরিচালিত হলে গ্রাহক পরিচিতির পুনরাবৃত্তি পরিহারের সুবিধার্থে প্রতিষ্ঠান উক্ত গ্রাহকের জন্য একটি Unique Customer Identification Code (UCIC) বরাদ্দ করবে। উক্ত UCIC গ্রাহককে চিহ্নিত করতে সাহায্য করবে, নির্দিষ্ট গ্রাহককে প্রতিষ্ঠান কর্তৃক কী কী সেবা প্রদান করা হচ্ছে তা চিহ্নিত (Track) করতে সাহায্য করবে।
- (৪) প্রতিটি আর্থিক প্রতিষ্ঠান নির্দিষ্ট সময় অন্তর অন্তর গ্রাহকের পরিচিতিমূলক তথ্য (KYC) হালনাগাদকরণের ক্ষেত্রে প্রয়োজনীয় ব্যবস্থা গ্রহণ করবে। নিম্ন ঝুঁকি সম্পন্ন গ্রাহকের ক্ষেত্রে এরূপ প্রক্রিয়া প্রতি দুই বছর অন্তর সম্পন্ন করতে হবে। এছাড়া, উচ্চ ঝুঁকি সম্পন্ন গ্রাহকের ক্ষেত্রে এরূপ প্রক্রিয়া এক বছর অন্তর সম্পন্ন করতে হবে। তবে গ্রাহকের পরিচিতিমূলক তথ্যের যে কোন পরিবর্তন অবগত হওয়ার সাথে সাথেই তা হালনাগাদ করতে হবে। এছাড়া নির্দিষ্ট কোন প্রয়োজন অনুভূত হলে যে কোন সময়েই গ্রাহকের পরিচিতিমূলক তথ্য হালনাগাদ করতে হবে। হালনাগাদকৃত তথ্যের ভিত্তিতে পুনরায় অবিলম্বে এসব হিসাবের ঝুঁকি নির্ণয় করতে হবে।
- (৫) এপ্রিল ৩০, ২০০২ তারিখের পূর্বে খোলা যে সকল হিসাবের KYC প্রক্রিয়া সম্পন্ন করা সম্ভব হয়নি সে সকল হিসাব ‘সুপ্ত’ (Dormant) হিসেবে চিহ্নিত হবে। তবে গ্রাহক কর্তৃক শাখা ব্যবস্থাপক/প্রতিষ্ঠানের নিকট লিখিত আবেদনের প্রেক্ষিতে আর্থিক প্রতিষ্ঠান উক্ত গ্রাহকের KYC প্রক্রিয়া সম্পন্ন করলে গ্রাহক হিসাবটিতে স্বাভাবিক লেনদেন সম্পাদন করতে পারবেন। কেন্দ্রীয় পরিপালন ইউনিট এরূপ সুপ্ত হিসাবের তথ্য সংরক্ষণ করবে এবং প্রতিষ্ঠানিক রীতি-নীতির বাইরে কোন হিসাব বন্ধ করবে না।

৩.৬ সশরীরে অনুপস্থিত বা দূরবর্তী গ্রাহকের (Non face to face customer) ক্ষেত্রে করণীয়

আর্থিক প্রতিষ্ঠান তাদের সশরীরে অনুপস্থিত বা দূরবর্তী গ্রাহককে সেবা প্রদানের ক্ষেত্রে মানিলভারিং ও সম্ভ্রাসী কার্যে অর্থায়নের ঝুঁকি নিরূপণ এবং ঝুঁকি নিরসনের নীতি ও পদ্ধতি প্রণয়ন করবে এবং সময় সময় তা পর্যালোচনা করবে।

সশরীরে অনুপস্থিত বা দূরবর্তী গ্রাহক বলতে এ সকল গ্রাহককে বুঝাবে যারা সশরীরে উপস্থিত না হয়ে প্রতিষ্ঠানের এজেন্টের মাধ্যমে বা নিজের পেশাদার প্রতিনিধির (আইনজীবী, একাউন্টেন্ট ইত্যাদি) মাধ্যমে হিসাব খুলে থাকে এবং পরিচালনা করে থাকে।

৩.৭ Politically Exposed Persons (PEPs) এর ক্ষেত্রে করণীয়

Politically Exposed Persons (PEPs) এর হিসাব খোলা ও হিসাব পরিচালনার ক্ষেত্রে এ সার্কুলারের ৩.২, ৩.৩, ৩.৪ ও ৩.৫ নম্বর অনুচ্ছেদে বর্ণিত নির্দেশনা অনুসরণের পাশাপাশি নিম্নের নির্দেশনাসমূহ অনুসরণ করতে হবে :

- ক) রিপোর্ট প্রদানকারী সংস্থাকে তাদের গ্রাহক বা হিসাবের প্রকৃত সুবিধাভোগী PEPs কিনা তা নির্ধারণ করার জন্য ঝুঁকি ব্যবস্থাপনা পদ্ধতি গ্রহণ করতে হবে;
- খ) রিপোর্ট প্রদানকারী সংস্থার উপযুক্ত উর্ধ্বতন কর্তৃপক্ষের অনুমোদন সাপেক্ষে তাদের সাথে ব্যবসায়িক সম্পর্ক স্থাপন করতে হবে;
- গ) কোন PEP এর হিসাবের অর্থ বা সম্পদের উৎস জানার জন্য যথোপযুক্ত ব্যবস্থা গ্রহণ করতে হবে;
- ঘ) তাদের হিসাবের লেনদেন নিয়মিতভাবে মনিটর করতে হবে; এবং
- ঙ) Foreign Exchange Regulation Act, 1947 ও এর আওতায় বাংলাদেশ ব্যাংক কর্তৃক জারীকৃত অনিবাসীদের হিসাব খোলা সংক্রান্ত যাবতীয় বিধিবিধান যথারীতি পরিপালন করতে হবে।

উল্লেখ্য, Politically Exposed Persons (PEPs) বলতে “individuals who are or have been entrusted with prominent public functions by 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” কে বুঝাবে।

PEPs এর পরিবারের সদস্য ও তাদের সাথে নিবিড়ভাবে সম্পর্কিত ব্যক্তির (close associates) ক্ষেত্রেও উপরোক্ত নির্দেশনাসমূহ প্রযোজ্য হবে। তবে এ অনুচ্ছেদে উল্লিখিত ‘PEPs’ হিসেবে কোন মধ্যম বা অধস্তন (Middle ranking or more junior individuals) পর্যায়ের ব্যক্তি বিবেচিত হবেন না।

৩.৮ প্রভাবশালী ব্যক্তির (Influential Persons) ক্ষেত্রে করণীয়

রিপোর্ট প্রদানকারী সংস্থাকে তাদের গ্রাহক বা হিসাবের প্রকৃত সুবিধাভোগী প্রভাবশালী কোন ব্যক্তি কিনা তা নির্ধারণ করতে হবে। এ ধরনের গ্রাহকের সাথে ব্যবসায়িক সম্পর্ক ঝুঁকিপূর্ণ প্রতীয়মান হলে ৩.২, ৩.৩, ৩.৪ ও ৩.৫ নম্বর অনুচ্ছেদে বর্ণিত নির্দেশনা অনুসরণের পাশাপাশি অনুচ্ছেদ ৩.৭ এর খ হতে ও ক্রমিক বর্ণিত নির্দেশনা পরিপালন করতে হবে।

উল্লেখ্য, প্রভাবশালী ব্যক্তি বলতে “individuals who are or have been entrusted domestically with prominent public functions, for example Head of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials” কে বুঝাবে।

প্রভাবশালী কোন ব্যক্তির ক্ষেত্রে প্রযোজ্য নির্দেশনা তাদের পরিবারের সদস্য ও তাদের সাথে নিবিড়ভাবে সম্পর্কিত ব্যক্তির (close associates) ক্ষেত্রেও প্রযোজ্য হবে। তবে এ অনুচ্ছেদে উল্লিখিত ‘প্রভাবশালী ব্যক্তি’ হিসেবে কোন মধ্যম বা অধস্তন (Middle ranking or more junior individuals) পর্যায়ের ব্যক্তি বিবেচিত হবেন না।

৩.৯ আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার ক্ষেত্রে করণীয়

রিপোর্ট প্রদানকারী সংস্থাকে তাদের গ্রাহক বা হিসাবের প্রকৃত সুবিধাভোগী কোন আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তা কিনা তা নির্ধারণ করতে হবে। এ ধরনের গ্রাহকের সাথে ব্যবসায়িক সম্পর্ক ঝুঁকিপূর্ণ প্রতীয়মান হলে ৩.২, ৩.৩, ৩.৪ ও ৩.৫ নম্বর অনুচ্ছেদে বর্ণিত নির্দেশনা অনুসরণের পাশাপাশি অনুচ্ছেদ ৩.৭ এর খ হতে ও ক্রমিক বর্ণিত নির্দেশনা পরিপালন করতে হবে।

উল্লেখ্য, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তা বলতে “persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions” কে বুঝাবে।

আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার ক্ষেত্রে প্রযোজ্য নির্দেশনা তাদের পরিবারের সদস্য ও তাদের সাথে নিবিড়ভাবে সম্পর্কিত ব্যক্তির (close associates) ক্ষেত্রেও প্রযোজ্য হবে। তবে এ অনুচ্ছেদে উল্লিখিত ‘আন্তর্জাতিক সংস্থার প্রধান’ বা ‘উচ্চ পর্যায়ের কর্মকর্তা’ হিসেবে কোন মধ্যম বা অধস্তন (Middle ranking or more junior individuals) পর্যায়ের ব্যক্তি বিবেচিত হবেন না।

৪। ঝুঁকি ভিত্তিক এপ্রোচ (Risk Based Approach) অনুসরণ

আর্থিক প্রতিষ্ঠানসমূহ তাদের গ্রাহক বা তৃতীয় পক্ষ, বিভিন্ন স্টেকহোল্ডার, পণ্য/সেবা ইত্যাদির ভিত্তিতে তাদের নিজ নিজ প্রতিষ্ঠানের মানিলন্ডারিং ও সন্ত্রাসে অর্থায়নের ঝুঁকি নিরূপণ করবে এবং সময়ে সময়ে উক্ত ঝুঁকি নিরসনের লক্ষ্যে প্রয়োজনীয় পদক্ষেপ গ্রহণ করবে।

৫। নতুন সেবা বা প্রযুক্তি গ্রহণের ক্ষেত্রে করণীয় (New Service or Technology)

আর্থিক প্রতিষ্ঠানসমূহ কর্তৃক প্রযুক্তি নির্ভর নতুন কোন সেবা বা পদ্ধতি (যেমন- ইন্টারনেটের মাধ্যমে লেনদেন, ইলেকট্রনিক কার্ড ইত্যাদি) প্রচলন বা প্রচলিত সেবা বা পদ্ধতির উন্নয়নের ক্ষেত্রে সংশ্লিষ্ট প্রতিষ্ঠান উক্ত সেবা বা পদ্ধতির মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন ঝুঁকি চিহ্নিত করবে, তার মাত্রা নিরূপণ করবে এবং এরূপ সেবা বা পদ্ধতি হতে সৃষ্ট ঝুঁকি মোকাবেলার জন্য যথাযথ ব্যবস্থা গ্রহণ করবে।

৬। নগদ লেনদেন রিপোর্ট (Cash Transaction Report-CTR)

(১) প্রতিটি আর্থিক প্রতিষ্ঠান তার দৈনন্দিন লেনদেন পর্যালোচনা করে একটি হিসাবে একটি নির্দিষ্ট দিনে এক বা একাধিক লেনদেনের মাধ্যমে জমা বা উত্তোলনের (অনলাইনসহ যে কোন ধরনের নগদ জমা বা উত্তোলন) পরিমাণ যদি ১০,০০,০০০.০০ (দশ লক্ষ) টাকা বা তদূর্ধ্ব অংকের হয় তবে স্ব স্ব কেন্দ্রীয় পরিপালন ইউনিটের মাধ্যমে বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইউনিট (বিএফআইইউ) বরাবরে নগদ লেনদেন রিপোর্ট (Cash Transaction Report-CTR) হিসেবে দাখিল করবে। এক্ষেত্রে নগদ লেনদেন বলতে আর্থিক প্রতিষ্ঠানের ব্যাংক হিসাবে আর্থিক প্রতিষ্ঠানে পরিচালিত হিসাবের অনুকূলে তাদের গ্রাহক বা তৃতীয় পক্ষ কর্তৃক সম্পাদিত নগদ লেনদেনকে বোঝাবে।

(২) এরূপ বিবরণী মাসিক ভিত্তিতে প্রদেয় হবে। সে মোতাবেক প্রতি মাসের নগদ লেনদেন রিপোর্ট পরবর্তী মাসের ২১ তারিখের মধ্যে goAML web এর মাধ্যমে বিএফআইইউ এর নিকট দাখিল করতে হবে। goAML সংশ্লিষ্ট প্রয়োজনীয় ডকুমেন্ট <http://www.bb.org.bd/eservices.php> ওয়েবলিংক হতে ডাউনলোড করা যাবে।

(৩) সামগ্রিক পরিস্থিতি পর্যালোচনাপূর্বক মানিলন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ কার্যক্রম নিবিড়ভাবে পর্যবেক্ষণের সুবিধার্থে নগদ লেনদেন রিপোর্টিং পদ্ধতি চালু করা হলো। পূর্বে প্রবর্তিত সন্দেহজনক লেনদেন রিপোর্টিং একটি সম্পূর্ণ পৃথক ব্যবস্থা। কোন হিসাবে নগদ লেনদেন রিপোর্টযোগ্য লেনদেন সম্পাদিত হলেই তা সন্দেহজনক লেনদেন হিসেবে বিবেচিত হবে না। তবে কেন্দ্রীয় পরিপালন ইউনিট আর্থিক প্রতিষ্ঠানটির নগদ লেনদেন রিপোর্টযোগ্য সকল লেনদেন পর্যালোচনা করে কোন সন্দেহজনক লেনদেন

সংঘটিত হয়েছে কিনা তা চিহ্নিত করবে ও সন্দেহজনক লেনদেন পরিলক্ষিত হলে পৃথকভাবে “সন্দেহজনক লেনদেন রিপোর্ট” হিসেবে বিএফআইইউ বরাবর দাখিল করবে। সন্দেহজনক লেনদেন পরিলক্ষিত না হলে “সন্দেহজনক লেনদেন পাওয়া যায়নি” মর্মে প্রধান মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা হতে প্রত্যয়ন পত্র গ্রহণ করতঃ মাসিক নগদ লেনদেন রিপোর্টের সাথে goAML Web এর Message Board এর মাধ্যমে বিএফআইইউকে অবহিত করতে হবে।

- (৪) সংশ্লিষ্ট মাসে আর্থিক প্রতিষ্ঠানে রিপোর্টযোগ্য নগদ লেনদেন সংঘটিত না হলে “নগদ লেনদেন রিপোর্টযোগ্য কোন লেনদেন নেই” মর্মে প্রত্যয়নপত্র goAML Web এর Message Board এর মাধ্যমে বিএফআইইউকে অবহিত করতে হবে।
- (৫) সরকারী হিসাব (বিভিন্ন মন্ত্রণালয়, বিভাগসহ), সরকারী মালিকানাধীন প্রতিষ্ঠান, আধা সরকারী বা স্বায়ত্তশাসিত প্রতিষ্ঠানের হিসাবে নগদ জমার ক্ষেত্রে নগদ লেনদেন রিপোর্ট দাখিল করার প্রয়োজন হবে না, তবে নগদ উত্তোলনের ক্ষেত্রে যথানিয়মে নগদ লেনদেন রিপোর্ট দাখিল করতে হবে।
- (৬) প্রতিটি শাখা মাসিক ভিত্তিতে উক্ত শাখার নগদ লেনদেন রিপোর্ট সংরক্ষণ করবে।
- (৭) আর্থিক প্রতিষ্ঠানসমূহ নগদ লেনদেন রিপোর্ট এর তথ্যাদি বিএফআইইউ এ দাখিলের মাস হতে কমপক্ষে ৫(পাঁচ) বছর সংরক্ষণ করবে।
- (৮) জুন, ২০১৫ মাসে সম্পাদিত নগদ লেনদেনের প্রথম রিপোর্ট জুলাই, ২০১৫ মাসের নির্ধারিত তারিখের মধ্যে বিএফআইইউতে দাখিল করতে হবে।

৭। সন্দেহজনক লেনদেন রিপোর্ট (Suspicious Transaction Report-STR)

- (১) মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২৫(১)(ঘ) ধারা এবং সন্ত্রাস বিরোধী আইন, ২০০৯ এর ১৬(১) ধারায় বর্ণিত নির্দেশনা বাস্তবায়নের নিমিত্তে প্রতিটি আর্থিক প্রতিষ্ঠানের সকল কর্মকর্তা দৈনন্দিন লেনদেন বা কার্যক্রমে সন্দেহজনক লেনদেন সনাক্তকরণে সচেতন ও সতর্ক থাকবেন।
- (২) সন্দেহজনক লেনদেন সনাক্তকরণে আর্থিক প্রতিষ্ঠানের কর্মকর্তাগণ মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২(ঘ) ধারা এবং সন্ত্রাস বিরোধী আইন, ২০০৯ এর ২(১৬) ধারায় বর্ণিত সংজ্ঞা বিবেচনা করবেন।
- (৩) আর্থিক প্রতিষ্ঠানের শাখার কোন কর্মকর্তা কর্তৃক সন্দেহজনক লেনদেন বা কার্যক্রম চিহ্নিত হওয়ার সাথে সাথে তা শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তাকে লিখিতভাবে অবহিত করতে হবে। শাখা মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা রিপোর্টকৃত লেনদেন বা কার্যক্রম অবিলম্বে যথাযথভাবে বিশ্লেষণ করবেন এবং পর্যবেক্ষণসমূহ বিশদভাবে লিপিবদ্ধ করে সংরক্ষণ করবেন। বর্ণিত লেনদেন বা কার্যক্রমটি সন্দেহজনক হিসেবে বিবেচিত হলে তা অবিলম্বে প্রয়োজনীয় দলিলাদিসহ কেন্দ্রীয় পরিপালন ইউনিটে প্রেরণ করতে হবে।
- (৪) কেন্দ্রীয় পরিপালন ইউনিট শাখা হতে প্রাপ্ত সন্দেহজনক লেনদেন বা কার্যক্রমটি যথাযথভাবে ও প্রয়োজনীয় তথ্য-উপাত্ত বা দলিলাদি সন্নিবেশিত করে রিপোর্ট করা হয়েছে কিনা তা পর্যালোচনা করে অবিলম্বে goAML web ব্যবহার করে এবং goAML Manual এর নির্দেশনা অনুসারে বিএফআইইউ বরাবর সন্দেহজনক লেনদেন রিপোর্ট দাখিলের পাশাপাশি ‘পরিশিষ্ট-গ’ তে সংযুক্ত ফরম ব্যবহার করে প্রয়োজনীয় তথ্য-উপাত্ত বা দলিলাদিসহ বিএফআইইউ বরাবর সন্দেহজনক লেনদেন রিপোর্ট দাখিল করবে। নির্ধারিত ফরমে সন্দেহজনক লেনদেন রিপোর্ট দাখিলের ক্ষেত্রে সীলকৃত খামের উপরে ‘গোপনীয় STR’ লিখে খামটি সরাসরি মহাব্যবস্থাপক, বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা বরাবর প্রেরণ করবে।
- (৫) আর্থিক প্রতিষ্ঠানসমূহ সন্দেহজনক লেনদেন রিপোর্ট এর তথ্যাদি বিএফআইইউ কর্তৃক পরবর্তী নির্দেশনা না দেয়া পর্যন্ত সংরক্ষণ করবে।
- (৬) সন্দেহজনক লেনদেন বা কার্যক্রম সনাক্তকরণ বা রিপোর্ট করার সাথে সংশ্লিষ্ট কর্মকর্তাগণ বিষয়টির গোপনীয়তা নিশ্চিত করবেন এবং এমন কোন আচরণ করবেন না যাতে সংশ্লিষ্ট গ্রাহক হিসাবের লেনদেনের বিষয়ে সতর্ক হতে পারেন।
- (৭) শাখা পর্যায়ে কোন লেনদেন বা কার্যক্রম সন্দেহজনক হিসেবে চিহ্নিত না হলেও কেন্দ্রীয় পরিপালন ইউনিট কর্তৃক কোন লেনদেন বা কার্যক্রম সন্দেহজনক প্রতীয়মান হলে অনুচ্ছেদ ৭(৪) মোতাবেক সন্দেহজনক লেনদেন রিপোর্ট বিএফআইইউ বরাবর দাখিল করতে হবে।

৮। Self Assessment এবং Independent Testing Procedures

মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে একটি কার্যকরী ব্যবস্থা প্রতিষ্ঠার লক্ষ্যে আর্থিক প্রতিষ্ঠানের অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক শাখাসমূহ হতে প্রাপ্ত Self Assessment Report পর্যালোচনা এবং Independent Testing Procedures যথাযথভাবে সম্পন্ন

করার জন্য উক্ত বিভাগটিতে পর্যাপ্ত লোকবল নিশ্চিত করতে হবে যাদের মানিলভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ এর নির্দেশনা এবং এ বিষয়ক নিজস্ব নীতিমালা সম্পর্কে সম্যক জ্ঞান রয়েছে।

৮.১ শাখাসমূহের করণীয়

- (১) প্রতিটি শাখা কর্তৃক Self Assessment এর জন্য নির্ধারিত চেকলিস্ট (পরিশিষ্ট 'ঘ') এর উপর ভিত্তি করে ষাণ্মাসিক ভিত্তিতে নিজেদের শাখার মূল্যায়ন করতে হবে;
- (২) আলোচ্য মূল্যায়ন প্রতিবেদন চূড়ান্ত করার পূর্বে শাখা ব্যবস্থাপকের সভাপতিত্বে শাখার সংশ্লিষ্ট কর্মকর্তাদের নিয়ে সভা করতে হবে। উক্ত সভায় খসড়া শাখা মূল্যায়ন প্রতিবেদনের উপর আলোচনা করতে হবে, চিহ্নিত সমস্যা শাখা পর্যায়ে সমাধান করা সম্ভবপর হলে শাখা কর্তৃক অবিলম্বে ব্যবস্থা গ্রহণপূর্বক চূড়ান্ত করতে হবে এবং চূড়ান্ত প্রতিবেদনে সুপারিশ লিপিবদ্ধ করতে হবে। পরবর্তী মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক ত্রৈমাসিক সভাগুলোতে এতদসংশ্লিষ্ট বিষয়ের অগ্রগতি নিয়ে আলোচনা করতে হবে; এবং
- (৩) প্রতিটি ষাণ্মাসিককাল সমাপ্ত হওয়ার পরবর্তী মাসের ১৫ তারিখের মধ্যে শাখা মূল্যায়ন প্রতিবেদন, এ বিষয়ে শাখা কর্তৃক গৃহীত/গৃহীতব্য কার্যক্রম ও সুপারিশসহ প্রধান কার্যালয়ের অভ্যন্তরীণ নিরীক্ষা বিভাগ ও কেন্দ্রীয় পরিপালন ইউনিটে প্রেরণ করতে হবে।

৮.২ অভ্যন্তরীণ নিরীক্ষা বিভাগের করণীয়

- (১) অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক শাখাসমূহ হতে প্রাপ্ত শাখা মূল্যায়ন প্রতিবেদন যাচাই করে কোন শাখায় কোন ঝুঁকিপূর্ণ বিষয় পরিলক্ষিত হলে তাৎক্ষণিকভাবে শাখাটি পরিদর্শনের ব্যবস্থা করতে হবে এবং বিষয়টি কেন্দ্রীয় পরিপালন ইউনিটকে অবহিত করতে হবে।
- (২) অভ্যন্তরীণ নিরীক্ষা বিভাগ তাদের নিজস্ব এবং নিয়মিত বার্ষিক পরিদর্শন/নিরীক্ষা কর্মসূচী অনুসারে বিভিন্ন শাখার পরিদর্শন/নিরীক্ষা কার্যক্রম সম্পাদনকালে Independent Testing Procedures এর নির্ধারিত চেকলিস্ট (পরিশিষ্ট 'ঙ')-এর ভিত্তিতে সংশ্লিষ্ট শাখার মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রম সংশ্লিষ্ট বিষয়াদি পরীক্ষা করবে ও শাখার রেটিং নির্ণয়করতঃ সংশ্লিষ্ট শাখার প্রতিবেদন প্রণয়ন করবে।
- (৩) অভ্যন্তরীণ নিরীক্ষা বিভাগ পরিদর্শিত/নিরীক্ষিত শাখাসমূহের রেটিং সম্বলিত প্রতিবেদনের কপি আর্থিক প্রতিষ্ঠানের কেন্দ্রীয় পরিপালন ইউনিট বরাবরে প্রেরণ করবে।

৮.৩ কেন্দ্রীয় পরিপালন ইউনিটের করণীয়

- (১) কেন্দ্রীয় পরিপালন ইউনিট শাখাসমূহ হতে প্রাপ্ত শাখা মূল্যায়ন প্রতিবেদন এবং আর্থিক প্রতিষ্ঠানের অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক দাখিলকৃত পরিদর্শন/নিরীক্ষা প্রতিবেদনের উপর ভিত্তি করে বিবেচ্য ষাণ্মাসিকে পরিদর্শিত শাখাসমূহের চেকলিস্ট ভিত্তিক মূল্যায়ন প্রতিবেদন প্রস্তুত করবে। উক্ত প্রতিবেদনে অন্যান্য বিষয়ের সাথে আবশ্যিকভাবে নিম্নের বিষয়সমূহ অন্তর্ভুক্ত থাকবে :
 - (ক) মোট শাখার সংখ্যা এবং শাখা হতে প্রাপ্ত মোট সেলফ অ্যাসেসমেন্ট রিপোর্টের সংখ্যা;
 - (খ) রিপোর্টকালে অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক পরিদর্শিত/নিরীক্ষিত শাখার সংখ্যা এবং শাখাসমূহের অবস্থা (শাখাওয়ারী প্রাপ্ত নম্বর);
 - (গ) প্রাপ্ত সেলফ অ্যাসেসমেন্ট রিপোর্টে অধিক সংখ্যক শাখায় একই ধরনের যে সকল অনিয়মের বিষয় উল্লেখ রয়েছে তা উল্লেখপূর্বক ঐ সকল অনিয়ম রোধে কেন্দ্রীয় পরিপালন ইউনিট কর্তৃক গৃহীত ব্যবস্থা;
 - (ঘ) অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক দাখিলকৃত প্রতিবেদনে উল্লিখিত সাধারণ ও বিশেষ অনিয়মসমূহ এবং ঐ সকল অনিয়ম রোধে কেন্দ্রীয় পরিপালন ইউনিট কর্তৃক গৃহীত ব্যবস্থা; এবং
 - (ঙ) প্রাপ্ত রিপোর্টে “অসন্তোষজনক” ও “প্রান্তিক” হিসেবে মূল্যায়িত শাখাসমূহের পরিপালন নিশ্চিত করতঃ রেটিং উন্নয়নকল্পে গৃহীত ব্যবস্থা।আলোচ্য প্রতিবেদনটি ১.৩(৬) এ উল্লিখিত প্রতিবেদনে অন্তর্ভুক্ত হবে।
- (২) শাখাসমূহ হতে প্রাপ্ত শাখা মূল্যায়ন প্রতিবেদন যাচাই করে কোন শাখায় কোন ঝুঁকিপূর্ণ বিষয় পরিলক্ষিত হলে তাৎক্ষণিকভাবে শাখাটি অভ্যন্তরীণ নিরীক্ষা বিভাগের মাধ্যমে পরিদর্শনের ব্যবস্থা করতে হবে এবং বিষয়টি উপযুক্ত কর্তৃপক্ষের নজরে আনতে হবে।

৯। সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়ন প্রতিরোধ (Prevention of Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction)

- (১) প্রত্যেক আর্থিক প্রতিষ্ঠান পরিচালনা পর্ষদের অনুমোদনক্রমে সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়ন সংক্রান্ত লেনদেন প্রতিরোধ ও সনাক্ত করার লক্ষ্যে একটি পদ্ধতি প্রতিষ্ঠা করবে, প্রতিষ্ঠানের কর্মকর্তাদের দায়দায়িত্ব সম্পর্কিত

নির্দেশনা জারী করবে, সময় সময় তা পর্যালোচনা করবে এবং বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা যথাযথভাবে প্রতিপালন করা হচ্ছে কিনা তা নিশ্চিত করবে।

- (২) প্রতিটি আর্থিক প্রতিষ্ঠান জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার হালনাগাদ তথ্য ইলেক্ট্রনিক পদ্ধতিতে সংরক্ষণ করবে। জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় তালিকাভুক্ত ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার সংজ্ঞা এ সার্কুলারের ২(২) অনুচ্ছেদে প্রদান করা হয়েছে।
- (৩) প্রতিটি আর্থিক প্রতিষ্ঠান জাতিসংঘের নিরাপত্তা পরিষদের কোন রেজুলেশনের আওতায় বা বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার নামে অথবা প্রত্যক্ষ বা পরোক্ষভাবে তাদের নিয়ন্ত্রণাধীন/স্বার্থসংশ্লিষ্ট কোন ব্যক্তি বা সত্তার নামে হিসাব (আমানত/ঋণ) রয়েছে কিনা বা কোন লেনদেন সংঘটিত হয়েছে কিনা তা চিহ্নিত করার জন্য নিয়মিত লেনদেন মনিটর করবে এবং প্রয়োজনে লেনদেন পর্যালোচনা করবে। তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তা অথবা প্রত্যক্ষ বা পরোক্ষভাবে তাদের নিয়ন্ত্রণাধীন/স্বার্থসংশ্লিষ্ট কোন ব্যক্তি বা সত্তার কোন হিসাব (আমানত/ঋণ) বা লেনদেন চিহ্নিত হওয়ার সাথে সাথে সংশ্লিষ্ট আর্থিক প্রতিষ্ঠান উক্ত হিসাবের লেনদেন বা লেনদেনটি স্থগিত করে পরবর্তী কর্ম দিবসের মধ্যে এ বিষয়ক বিস্তারিত তথ্য বিএফআইইউকে অবহিত করবে।
- (৪) জাতিসংঘের নিরাপত্তা পরিষদ কর্তৃক গৃহীত রেজুলেশন ১৩৭৩ (২০০১) এর আওতায় বিদেশী সরকার বা বিদেশী এফআইইউ এর অনুরোধে বিএফআইইউ হতে প্রেরিত বা উক্ত রেজুলেশনের আওতায় বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার সাথে হিসাব (আমানত/ঋণ) বা অন্য কোন সম্পর্ক রয়েছে কিনা তা চিহ্নিত করার জন্য আর্থিক প্রতিষ্ঠান নিয়মিত লেনদেন মনিটর করবে এবং প্রয়োজনীয় পদক্ষেপ গ্রহণ করবে। তালিকাভুক্ত বা নিষিদ্ধ ঘোষিত কোন ব্যক্তি বা সত্তার কোন হিসাব (আমানত/ঋণ) চিহ্নিত হওয়ার সাথে সাথে সংশ্লিষ্ট প্রতিষ্ঠান উক্ত হিসাব (আমানত/ঋণ) লেনদেন স্থগিত করে পরবর্তী কর্ম দিবসের মধ্যে বিস্তারিত তথ্য বিএফআইইউকে অবহিত করবে।

১০। নিয়োগ ও প্রশিক্ষণ

১০.১ নিয়োগ

মানিলভারিং, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়নের ঝুঁকি নিরসনের লক্ষ্যে আর্থিক প্রতিষ্ঠান তাদের বিভিন্ন নিয়োগ প্রক্রিয়ায় যথাযথ যাচাই প্রক্রিয়া (Screening Mechanism) অনুসরণ করবে যাতে কোন স্তরের কর্মকর্তার মাধ্যমে প্রতিষ্ঠান এ ধরনের ঝুঁকির সম্মুখীন না হয়।

১০.২ প্রশিক্ষণ- আর্থিক প্রতিষ্ঠানের কর্মকর্তা

মানিলভারিং, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়ন প্রতিরোধ কার্যক্রমের যথাযথ পরিপালন নিশ্চিত করার লক্ষ্যে প্রত্যেক আর্থিক প্রতিষ্ঠান তাদের সকল কর্মকর্তাদের মানিলভারিং, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়ন প্রতিরোধ সংশ্লিষ্ট বিষয়ে উপযুক্ত প্রশিক্ষণ প্রদানের ব্যবস্থা করবে এবং এ সংক্রান্ত তথ্য ও দলিলাদি সংরক্ষণ করবে।

১০.৩ শিক্ষণ- আর্থিক প্রতিষ্ঠানের গ্রাহক

(১) আর্থিক প্রতিষ্ঠান তাদের গ্রাহকদের হিসাব (আমানত/ঋণ) খোলার প্রাক্কালে যাচিত বিভিন্ন তথ্য সন্নিবেশ ও দলিলাদি দাখিলের যৌক্তিকতার বিষয়ে গ্রাহককে অবহিত করবে এবং মানিলভারিং, সন্ত্রাসী কার্যে অর্থায়ন ও ব্যাপক ধ্বংসাত্মক অস্ত্রের বিস্তারে অর্থায়ন প্রতিরোধ বিষয়ে গ্রাহকদের সচেতনতা বৃদ্ধির লক্ষ্যে সময় সময় লিফলেট বিতরণ এবং প্রতিটি শাখার দৃশ্যমান স্থানে এ বিষয়ক পোস্টার স্থাপনের ব্যবস্থা করবে।

(২) এছাড়া Corporate Social Responsibility (CSR) এর আওতায় মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে বিভিন্ন গণমাধ্যমসহ অন্যান্য মাধ্যমে এ বিষয়ক সচেতনতামূলক বিজ্ঞাপন, তথ্যচিত্র ইত্যাদি প্রচারের ব্যবস্থা করবে।

১১। রেকর্ড এবং প্রয়োজনীয় তথ্য/দলিলাদি সংরক্ষণ

- (১) গ্রাহকের হিসাব (আমানত/ঋণ) এবং হিসাবের লেনদেন সংক্রান্ত সকল প্রয়োজনীয় তথ্য বা দলিলাদি হিসাব/ব্যবসায়িক সম্পর্ক বন্ধ হওয়ার তারিখ হতে অন্ত্যন ৫ (পাঁচ) বৎসর পর্যন্ত সংরক্ষণ করতে হবে;
- (২) গ্রাহকের KYC সহ CDD প্রক্রিয়া সম্পাদনকালে সংগৃহীত সকল তথ্য ও দলিলাদি, হিসাব (আমানত/ঋণ) সংক্রান্ত দলিলাদি, ব্যবসায়িক পত্র যোগাযোগ এবং কোন গ্রাহকের বিষয়ে কোন প্রতিবেদন প্রণীত হলে এ সকল তথ্যাদি/দলিলাদি গ্রাহকের হিসাব/আমানত/ঋণ বন্ধ হওয়ার তারিখ হতে অন্ত্যন ৫ (পাঁচ) বৎসর পর্যন্ত সংরক্ষণ করতে হবে।

(৩) সংরক্ষিত তথ্যাদি অপরাধ কার্যক্রমের বিচারিক প্রক্রিয়ায় দালিলিক প্রমাণ হিসেবে উপস্থাপন করার ক্ষেত্রে যথেষ্ট হতে হবে।

(৪) গ্রাহকের KYC সহ CDD প্রক্রিয়া সম্পাদনকালে গৃহীত সকল তথ্য ও দলিলাদি এবং লেনদেন সংক্রান্ত তথ্য ও দলিলাদি বিএফআইইউ এর চাহিদা বা নির্দেশনা মোতাবেক সরবরাহ করবে।

১২। আর্থিক প্রতিষ্ঠানের জন্য ইতোপূর্বে জারীকৃত নিম্নোক্ত সার্কুলার/সার্কুলার লেটারসমূহের নির্দেশনা বলবৎ থাকবে।

সার্কুলার/সার্কুলার লেটার নং	জারীর তারিখ	বিষয়
এএমএল সার্কুলার নং-২২	২১ এপ্রিল, ২০০৯	সন্ত্রাস বিরোধী আইন, ২০০৯ জারী প্রসঙ্গে।
বিএফআইইউ সার্কুলার লেটার-০১	৩০ জানুয়ারি, ২০১২	বিএফআইইউ নামকরণ প্রসঙ্গে।
বিএফআইইউ সার্কুলার নং-০২	১৫ মার্চ, ২০১২	মানিলাভারিং প্রতিরোধ আইন, ২০১২ ও সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১২ জারী প্রসঙ্গে।
বিএফআইইউ সার্কুলার নং-০৪	১৬ সেপ্টেম্বর, ২০১২	আর্থিক প্রতিষ্ঠানের জন্য Guidance Notes on Prevention of Money Laundering and Terrorist Financing জারীকরণ প্রসঙ্গে।
বিএফআইইউ সার্কুলার নং-০৭	১৪ জুলাই, ২০১৩	সন্ত্রাস বিরোধী (সংশোধন) আইন, ২০১৩ জারী প্রসঙ্গে।
বিএফআইইউ সার্কুলার লেটার-০৩/২০১৫	০৯ এপ্রিল, ২০১৫	মানিলাভারিং প্রতিরোধ বিধিমালা, ২০১৩ এবং সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ জারী প্রসঙ্গে।

১৩। অনুচ্ছেদ ১২ এ উল্লিখিত সার্কুলার ও সার্কুলার লেটার ব্যতীত এ মাস্টার সার্কুলার জারীর পূর্বে আর্থিক প্রতিষ্ঠানসমূহের জন্য মানিলাভারিং প্রতিরোধ বিভাগ বা বিএফআইইউ কর্তৃক জারীকৃত অন্য সকল সার্কুলার ও সার্কুলার লেটারের নির্দেশনা এ মাস্টার সার্কুলারের নির্দেশনা দ্বারা প্রতিস্থাপিত মর্মে বিবেচিত হবে।

এ সার্কুলারের নির্দেশনাসমূহ অবিলম্বে কার্যকর হবে।

আপনাদের বিশ্বস্ত,



(মোঃ নাসিরুজ্জামান)

মহাব্যবস্থাপক

ফোনঃ ৯৫৩০১১৮

সংযোজনী : মোট ২২ (বাইশ) পৃষ্ঠা।

প্রতিলিপি নং-বিএফআইইউ(পলিসি)-০৩/২০১৫-

তারিখ : উল্লিখিত

অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য প্রতিলিপি প্রেরণ করা হলো (জ্যেষ্ঠতার ক্রমানুসারে নয়):

১. গভর্নর মহোদয়ের ব্যক্তিগত কর্মকর্তা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
২. ডেপুটি গভর্নর মহোদয়গণের সাথে সংযুক্ত উপ-পরিচালক/সহকারী পরিচালক, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৩. সকল নির্বাহী পরিচালক/অর্থনৈতিক উপদেষ্টা, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়/মতিঝিল/চট্টগ্রাম/রাজশাহী/খুলনা।
৪. নির্বাহী পরিচালক, বাংলাদেশ ব্যাংক ট্রেনিং একাডেমী, মিরপুর-২, ঢাকা।
৫. সকল বিভাগীয় প্রধান, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা।
৬. মহাব্যবস্থাপক, বাংলাদেশ ব্যাংক, মতিঝিল, ঢাকা/চট্টগ্রাম/রাজশাহী/খুলনা/বগুড়া/সিলেট/সদরঘাট, ঢাকা/বরিশাল/রংপুর/ময়মনসিংহ।
৭. চেয়ারম্যান, বাংলাদেশ লিজিং এন্ড ফাইন্যান্স কোম্পানীজ এসোসিয়েশন, (বিএলএফসিএ), সারা টাওয়ার, ১১/এ টয়েনবি সার্কুলার রোড, মতিঝিল, ঢাকা-১০০০।



(আবুল জান্নাত জীবন)

সহকারী পরিচালক

ফোনঃ ৯৫৩০০১০-৭৫/২৪৯৭

ই-মেইল- abul.jannat@bb.org.bd

আর্থিক প্রতিষ্ঠানের নাম

প্রধান মানিল্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (CAMLCO) সম্পর্কিত তথ্যাদি

নাম	বাংলায় :
	ইংরেজীতে :
পদবী	
ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা থেকে কত ধাপ নিচের পদ	
শিক্ষাগত যোগ্যতা	
এএমএল/সিএফটি বিষয়ক প্রশিক্ষণ	
জন্ম তারিখ	
জাতীয় পরিচয় পত্র/পাসপোর্ট নম্বর	
পিতার নাম	
মাতার নাম	
ঠিকানা	বর্তমান :
	স্থায়ী :
ফ্যাক্স নং	
ল্যান্ড ফোন নং	
মোবাইল ফোন নং	
ই-মেইল	

উপ-প্রধান মানিল্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (D-CAMLCO) সম্পর্কিত তথ্যাদি

নাম	বাংলায় :
	ইংরেজীতে :
পদবী	
শিক্ষাগত যোগ্যতা	
এএমএল/সিএফটি বিষয়ক প্রশিক্ষণ	
জন্ম তারিখ	
জাতীয় পরিচয় পত্র/পাসপোর্ট নম্বর	
পিতার নাম	
মাতার নাম	
ঠিকানা	বর্তমান :
	স্থায়ী :
ফ্যাক্স নং	
ল্যান্ড ফোন নং	
মোবাইল ফোন নং	
ই-মেইল	

.....আর্থিক প্রতিষ্ঠানের নাম

.....শাখা

হিসাব খোলার আবেদন ফরম

ব্যক্তি হিসাব

তারিখঃ.....

হিসাব নম্বর :

ইউনিক গ্রাহক আইডি কোড :.....

ব্যবস্থাপক

----- (আর্থিক প্রতিষ্ঠানের নাম)

----- ।

জনাব,

আমি/আমরা আপনার প্রতিষ্ঠানে নিম্নরূপ একটি মেয়াদী আমানত হিসাব খোলার জন্য আবেদন করছি। আমার/আমাদের বিস্তারিত তথ্যাদি নীচে প্রদান করলাম :

১. আবেদনকারী/দের নাম :

	বাংলায়	ইংরেজীতে
প্রথম আবেদনকারী		
দ্বিতীয় আবেদনকারী		
তৃতীয় আবেদনকারী		
চতুর্থ আবেদনকারী		

২. হিসাবের প্রকার (টিক দিন):

 স্থায়ী স্কিম-১ স্থায়ী স্কিম-২ স্থায়ী স্কিম-৩ অন্যান্য৩. হিসাব পরিচালনা সংক্রান্ত ঘোষণা (টিক দিন): এককভাবে যৌথভাবে যে কোন একজন অন্যান্য..... বিশেষ নির্দেশনা (যদি থাকে)

৪. জমা আমানত সংক্রান্ত তথ্য:

মেয়াদকাল : _____ বছর _____ মাস _____ দিন । মেয়াদপূর্তির তারিখঃ.....

(প্রদেয় অর্থ ব্যাংকিং চ্যানেলে ইনস্ট্রুমেন্ট অর্থাৎ চেক, ড্রাফট ইত্যাদির মাধ্যমে হতে হবে)

নবায়নের ক্ষেত্রে : আসল এবং সুদ নবায়ন করণ শুধুমাত্র আসল নবায়ন করণ
প্রয়োজ্য নহে

প্রদেয় অর্থের পরিমাণ : টাকা _____, কথায় (টাকা _____)

চেক নম্বর/পে অর্ডার নম্বর _____ তারিখ _____

ব্যাংকের নাম ও শাখা _____

৫. বিশেষ স্কিম সংক্রান্ত তথ্য:

স্কিমের নামঃ.....

স্কিমের মেয়াদঃ..... এককালীন জমা/ কিস্তির পরিমাণঃ..... কিস্তির সংখ্যা (বার্ষিক) :.....

মেয়াদান্তে প্রদেয়ঃ..... মাসিক প্রদেয়ঃ.....

৬. প্রদেয় অর্থের উৎস (বিস্তারিত ভাবে উল্লেখ করণ):

৭. এক বা একাধিক হিসাবধারী নাবালক হলে :

আমি নিম্নবর্ণিত হিসাবধারীর বৈধ অভিভাবক হিসেবে এই মর্মে ঘোষণা করছি যে, হিসাবধারী নাবালক। তার প্রয়োজনীয় তথ্য সংযুক্ত ফরমে প্রদান করা হলো। হিসাবধারী সাবালক না হওয়া পর্যন্ত কিংবা আমার পরবর্তী ঘোষণা না দেয়া পর্যন্ত বৈধ অভিভাবক হিসাবে হিসাবটি আমার স্বাক্ষরে পরিচালিত হবে।

(ক) হিসাবধারী (নাবালক) এর নাম :.....

(খ) অভিভাবকের নাম :..... নাবালকের সাথে সম্পর্ক :

(নাবালক এবং অভিভাবক উভয়ের জন্যই ব্যক্তি সংক্রান্ত তথ্যাবলী ফরম পূরণ করতে হবে এবং উভয় ফরমেই অভিভাবক কর্তৃক স্বাক্ষর করতে হবে।)

নমিনীর আলোকচিত্র (গ্রাহক কর্তৃক সত্যায়িত)	নমিনীর আলোকচিত্র (গ্রাহক কর্তৃক সত্যায়িত)
--	--

৮. নমিনী সংক্রান্ত তথ্যঃ

আমি/আমরা এই হিসাবের অর্থ আমার/আমাদের মৃত্যুর পর নিম্নোক্ত ব্যক্তি/ব্যক্তিসমূহকে প্রদানের জন্য মনোনীত করলাম। আমি/আমরা উল্লিখিত মনোনয়ন যে কোন সময় বাতিল বা পরিবর্তনের অধিকার সংরক্ষণ করি। আমি/আমরা এই মর্মে আরো সম্মতি জ্ঞাপন করছি যে, আমার/আমাদের নির্দেশনা মোতাবেক লেনদেনে ----- (আর্থিক প্রতিষ্ঠানের নাম) কোনোভাবে দায়বদ্ধ হবেনা।

নমিনীর নাম : ১.

ও প্রাপ্য অংশ : ২.

জন্ম তারিখ : ১..... ২.....

পিতার নাম : ১..... ২.....

মাতার নাম : ১..... ২.....

স্বামী/স্ত্রীর নাম : ১..... ২.....

নমিনীর স্থায়ী ঠিকানাঃ ১.

২.....

পেশা : ১..... ২.....

হিসাবধারীর সাথে সম্পর্ক : ১..... ২.....

জন্ম নিবন্ধন নম্বর ও ইস্যুকারী কর্তৃপক্ষ (যদি থাকে) : ১..... ২.....

জাতীয় পরিচয়পত্র নম্বর (যদি থাকে) : ১..... ২.....

*(কোন অনিবাসীকে নমিনী করা হলে ঐ অনিবাসী সংশ্লিষ্ট হিসাবের অর্থ প্রাপ্য হলে প্রাপ্ত অর্থ বিদেশে প্রেরণের ক্ষেত্রে বিদ্যমান বৈদেশিক মুদ্রা নিয়ন্ত্রণ আইনের বিধি বিধান প্রযোজ্য হবে।)

৯. ঘোষণা ও স্বাক্ষরঃ

আমি/আমরা এই মর্মে নিশ্চয়তা প্রদান করছি যে, আমি/আমরা হিসাব সংক্রান্ত যাবতীয় নিয়মাবলী/শর্তাবলী পড়েছি এবং উক্ত নিয়মাবলী/শর্তাবলী মেনে চলতে বাধ্য থাকব। আমি/আমরা সজ্ঞানে ঘোষণা করছি যে, উপরোল্লিখিত তথ্যাদি সত্য ও নির্ভুল। আপনার চাহিদা মোতাবেক প্রদত্ত তথ্যের অতিরিক্ত সংশ্লিষ্ট যে কোন প্রয়োজনীয় তথ্যাদি/দলিলাদি সরবরাহ করবো।

আবেদনকারী/দের নাম, স্বাক্ষর ও তারিখ

.....

অফিসের ব্যবহারের জন্য

মন্তব্য :

.....
হিসাব খোলার কর্মকর্তা

নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ

.....
অনুমোদনকারী কর্মকর্তা

নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ

..... আর্থিক প্রতিষ্ঠানের নাম

..... শাখা

হিসাব খোলার আবেদন ফরম

অ-ব্যক্তিক হিসাব

তারিখঃ.....

হিসাব নম্বর :

ইউনিক গ্রাহক আইডি কোড :.....

ব্যবস্থাপক

----- (আর্থিক প্রতিষ্ঠানের নাম)

----- ।

জনাব,

আমি/আমরা আপনার প্রতিষ্ঠানে নিম্নরূপ একটি মেয়াদী আমানত হিসাব খোলার জন্য আবেদন করছি। আমার/আমাদের বিস্তারিত তথ্যাদি নিম্নে প্রদান করলাম :

১. হিসাবের নাম : (বাংলা).....
(ইংরেজী).....

২. প্রতিষ্ঠানের ধরণ (টিক দিন):

প্রাইভেট/পাবলিক লিঃ যৌথ উদ্যোগ অংশীদারী একক মালিকানা
 এনজিও/এনপিও সরকারী ক্লাব/সোসাইটি অন্যান্য(লিখুন).....

৩. হিসাবের প্রকার (টিক দিন):

স্থায়ী স্কিম-১ স্থায়ী স্কিম-২ স্থায়ী স্কিম-৩ অন্যান্য

৪. হিসাব পরিচালনা সংক্রান্ত ঘোষণা (টিক দিন): এককভাবে যৌথভাবে যে কোন একজন
 অন্যান্য

বিশেষ নির্দেশনা (যদি থাকে)

৫. প্রতিষ্ঠানের ঠিকানা :

ক. রেজিস্টার্ড ঠিকানা :.....

খ. ব্যবসাস্থল/অফিসের ঠিকানা :.....

গ. কারখানা/শিল্প প্রতিষ্ঠানের ঠিকানা :.....

৬. ট্রেড লাইসেন্স নম্বর : তারিখ :

ইস্যুকারী কর্তৃপক্ষ :.....

৭. নিবন্ধন কর্তৃপক্ষ ও দেশ :.....
(দেশী/বিদেশী উভয় ধরণের জন্য)

৮. নিবন্ধন নম্বর :..... তারিখ :

৯. ট্যাক্স আইডি নম্বর (TIN) :.....

১০. ভ্যাট রেজিঃ নম্বর (যদি থাকে) :.....

১১. ব্যবসায়ের প্রকৃতি (বিস্তারিত বর্ণনা) :.....

১২. জমা আমানত সংক্রান্ত তথ্যঃ

মেয়াদকাল : _____ বছর _____ মাস _____ দিন । মেয়াদপূর্তির তারিখঃ.....

(প্রদেয় অর্থ ব্যাংকিং চ্যানেলে ইনস্ট্রুমেন্ট অর্থাৎ চেক, ড্রাফট ইত্যাদির মাধ্যমে হতে হবে)

নবায়নের ক্ষেত্রে : আসল এবং সুদ নবায়ন করণ শুধুমাত্র আসল নবায়ন করণ
 প্রযোজ্য নহে ।

প্রদেয় অর্থের পরিমাণ : টাকা _____, কথায় (টাকা _____)

চেক নম্বর/পে অর্ডার নম্বর _____ তারিখ _____

ব্যাংকের নাম ও শাখা _____

১৩. বিশেষ স্কীম সংক্রান্ত তথ্যঃ

স্কীমের নামঃ.....

স্কীমের মেয়াদঃ..... এককালীন জমা/ কিস্তির পরিমাণঃ কিস্তির সংখ্যা (বার্ষিক) :.....

মেয়াদান্তে প্রদেয়ঃ..... মাসিক প্রদেয়ঃ.....

১৪. প্রদেয় অর্থের উৎস (বিস্তারিত ভাবে উল্লেখ করণ)ঃ

১৫. ঘোষণা ও স্বাক্ষরঃ

আমি/আমরা এই মর্মে নিশ্চয়তা প্রদান করছি যে, আমি/আমরা হিসাব সংক্রান্ত যাবতীয় নিয়মাবলী/শর্তাবলী পড়েছি এবং উক্ত নিয়মাবলী/শর্তাবলী মেনে চলতে বাধ্য থাকবো। আমি/আমরা সজ্ঞানে ঘোষণা করছি যে, উপরোল্লিখিত তথ্যাদি সত্য ও নির্ভুল। আপনার চাহিদা মোতাবেক প্রদত্ত তথ্যের অতিরিক্ত সংশ্লিষ্ট যে কোন প্রয়োজনীয় তথ্যাদি/দলিলাদি সরবরাহ করবো।

গ্রাহকের স্বাক্ষর, নাম, পদবী, ও তারিখ

১. _____ ২. _____ ৩. _____

অফিসের ব্যবহারের জন্য

মন্তব্য :

.....
.....
হিসাব খোলার কর্মকর্তা
নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ

.....
.....
অনুমোদনকারী কর্মকর্তা
নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ

..... আর্থিক প্রতিষ্ঠানের নাম

..... শাখা

হিসাব খোলার ফরম : ব্যক্তি সংক্রান্ত তথ্যাবলী

আলোকচিত্র

(এই ফরমটি পূরণপূর্বক ব্যক্তি ও অব্যক্তিক হিসাবের মূল অংশের সাথে সংযুক্ত করতে হবে।)

তারিখঃ.....

হিসাব নম্বরঃ

ইউনিক গ্রাহক আইডি কোড :.....

১. ব্যক্তির নাম : (বাংলা).....
(ইংরেজী)

২. হিসাবের সাথে সম্পর্ক (নীচে প্রযোজ্য ক্ষেত্রে টিক দিন)ঃ

১ম আবেদনকারী ২য় আবেদনকারী ৩য় আবেদনকারী ডাইরেক্টর
 অংশীদার এ্যাটর্নী হোল্ডার সিগনেটারিজ প্রকৃত সুবিধাভোগী অন্যান্য

৩. পিতার নাম : (বাংলা).....
(ইংরেজী).....

৪. মাতার নাম : (বাংলা).....
(ইংরেজী).....

৫. স্বামী/স্ত্রীর নাম : (বাংলা).....
(ইংরেজী).....

৬. জাতীয়তা :.....

৭. জন্ম তারিখ ও জন্ম স্থান :.....

৮. লিঙ্গ (টিক দিন) : পুরুষ মহিলা

৯. পেশা (বিস্তারিত বিবরণ) :.....

১০. পাসপোর্ট নম্বর :.....

১১. জাতীয় পরিচয়পত্র নম্বর :.....

১২. জন্ম নিবন্ধন সনদপত্র নম্বর :.....

[১০-১২ নম্বর ক্রমিক বর্ণিত দলিলাদি হতে আবশ্যিকভাবে যে কোন একটি দলিল প্রদান করতে হবে। তবে জন্ম নিবন্ধন সনদ প্রদান পূর্বক হিসাব খোলার ক্ষেত্রে জন্ম নিবন্ধন সনদপত্রের অতিরিক্ত গ্রাহক/হিসাব পরিচালনাকারীর আলোকচিত্রসহ যে কোন পরিচিতি পত্র প্রদান করতে হবে। আলোকচিত্রসহ পরিচিতি পত্র না থাকলে সে বিষয়ে আর্থিক প্রতিষ্ঠানের সম্মতি সাপেক্ষে তাদের নিকট গ্রহণযোগ্য সমাজের গণ্যমান্য ব্যক্তি^১ কর্তৃক প্রদত্ত পরিচয়ের প্রত্যয়ন পত্র প্রদান করতে হবে। উক্ত পরিচিতি পত্র বা প্রত্যয়ন পত্র গ্রাহক/হিসাব পরিচালনাকারীর আলোকচিত্রসহ হতে হবে। এছাড়া, নিম্নের ১৩-১৪ নম্বর ক্রমিক বর্ণিত দলিলাদিসহ অতিরিক্ত আরো কোন দলিলাদি এবং এই ফরমে উল্লিখিত তথ্যাদির অতিরিক্ত তথ্য গ্রাহকের পরিচিতি নিশ্চিত হওয়ার লক্ষ্যে আর্থিক প্রতিষ্ঠানের সম্মতির জন্য আর্থিক প্রতিষ্ঠানের চাহিদা মোতাবেক প্রদান করতে হবে।]

^১ গণ্যমান্য ব্যক্তি বলতে সংসদ সদস্য, সিটি কর্পোরেশনের মেয়র, ডেপুটি মেয়র ও কাউন্সিলরগণ, প্রথম শ্রেণীর গেজেটেড কর্মকর্তা, পাবলিক বিশ্ববিদ্যালয়ের শিক্ষক, উপজেলা পরিষদের চেয়ারম্যান ও ভাইস চেয়ারম্যান, ইউনিয়ন পরিষদের চেয়ারম্যান, পৌরসভার মেয়র ও পৌর কাউন্সিলরগণ, বেসরকারী কলেজের অধ্যক্ষ, সরকারী ও বেসরকারী উচ্চ বিদ্যালয় ও সরকারী প্রাথমিক বিদ্যালয়ের প্রধান শিক্ষক, জাতীয় দৈনিক পত্রিকার সম্পাদক, নোটারী পাবলিক এবং আধাসরকারী, স্বায়ত্তশাসিত ও রাষ্ট্রায়ত্ত্ব সংস্থা ও রাষ্ট্রায়ত্ত্ব ব্যাংকের ১ম শ্রেণীর কর্মকর্তাগণকে বুঝাবে।

১৩. ট্যাক্স আইডি নম্বর (TIN) (যদি থাকে) :.....

১৪. ড্রাইভিং লাইসেন্স নম্বর (যদি থাকে) :

১৫. বর্তমান ঠিকানা (আবাসস্থল) : (বাংলা).....
(ইংরেজী).....

১৬. স্থায়ী ঠিকানা : (বাংলা).....
(ইংরেজী).....

১৭. পেশাগত ঠিকানা :.....

১৮. যোগাযোগ :

টেলিফোনঃ বাসা :..... অফিসঃ..... মোবাইলঃ

ই-মেইলঃ..... ফ্যাক্সঃ

১৯. ক্রেডিট কার্ড সংক্রান্ত তথ্যঃ

ইস্যুকারী প্রতিষ্ঠান ও কার্ড নম্বর (যদি কার্ড ব্যবহারকারী হন) : ১।

২।

২০. রেসিডেন্স স্ট্যাটাস (টিক দিন) : রেসিডেন্ট নন-রেসিডেন্ট

(প্রয়োজনীয় ক্ষেত্রে গাইডলাইস ফর ফরেন এক্সচেঞ্জ ট্রানজেকশনস্ এর নির্দেশনা অনুসরণ করে তথ্য সংগ্রহ করতে হবে)

স্বাক্ষর (তারিখসহ)

গ্রাহক পরিচিতি সম্পর্কিত ফর্ম (KYC Profile Form) :

১. হিসাবের নাম :
২. হিসাবের ধরণ ও নম্বর :
৩. ইউনিক গ্রাহক আইডি কোড :
৪. হিসাবধারীর নাম :
৫. হিসাব খোলার কর্মকর্তার নাম :

৬. জন্ম নিবন্ধন নম্বর.....ফটোকপি গৃহীত কিনা? : হ্যাঁ / না (প্রযোজ্য ক্ষেত্রে)
৭. পাসপোর্ট নম্বর ফটোকপি গৃহীত কিনা? : হ্যাঁ / না (প্রযোজ্য ক্ষেত্রে)
৮. জাতীয় পরিচয়পত্র নম্বর..... ফটোকপি গৃহীত কিনা? : হ্যাঁ / না (প্রযোজ্য ক্ষেত্রে)
৯. টি আই এন ফটোকপি গৃহীত কিনা? : হ্যাঁ / না (প্রযোজ্য ক্ষেত্রে)
১০. ভ্যাট রেজিঃ নম্বর ফটোকপি গৃহীত কিনা? : হ্যাঁ / না (প্রযোজ্য ক্ষেত্রে)
১১. ড্রাইভিং লাইসেন্স নম্বর ফটোকপি গৃহীত কিনা? : হ্যাঁ / না (প্রযোজ্য ক্ষেত্রে)
১২. হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সম্পর্কিত তথ্যাদি (কোম্পানীর ক্ষেত্রে ২০% বা এর অধিক একক শেয়ার হোল্ডার এর বিস্তারিত তথ্যাদি সংগ্রহপূর্বক কেওয়াইসি সম্পাদন করতে হবে। এছাড়াও কোম্পানীর নিয়ন্ত্রনকারী শেয়ার হোল্ডার এর বিস্তারিত তথ্যাদি সংগ্রহপূর্বক কেওয়াইসি সম্পাদন করতে হবে। ব্যক্তিক হিসাবের ক্ষেত্রে হিসাবের অর্থের উৎস হিসাবধারী ব্যতীত অন্য কোন ব্যক্তি হলে সে ক্ষেত্রে হিসাবের অর্থ যোগানদাতার কেওয়াইসি সম্পাদন করতে হবে) :

১৩. প্রদেয় অর্থের উৎস কি? তহবিলের উৎস কিভাবে নিশ্চিত করা হয়েছে? (প্রযোজ্য ক্ষেত্রে)

১৪. গ্রাহকের পেশার সাথে প্রদেয় অর্থের উৎস সামঞ্জস্যপূর্ণ কি না ?

গ্রাহকের পেশার বিস্তারিত বর্ণনাপূর্বক সামঞ্জস্যতা নিশ্চিত করণ :

১৫.রিস্ক গ্রেডিং : উচ্চ নিম্ন

<p>মন্তব্য :</p>

(মন্তব্য অংশে Subjective বিবেচনায় গ্রাহকের ঝুঁকি সম্পর্কে আবশ্যিকভাবে মন্তব্য করতে হবে। গ্রাহকের ঝুঁকি নিরূপণের ক্ষেত্রে গ্রাহকের পেশার বিস্তারিত ধারণা বিশ্লেষণকরতঃ ব্যবসায়ের ক্ষেত্রে ব্যবসায়ের প্রকৃতি, অর্থের মাত্রা, ব্যবসায়ের এলাকা, ব্যবসায়ের আকার, হিসাবের প্রকৃত সুবিধাভোগী ইত্যাদিসহ অন্যান্য বিশেষ দিক বিবেচনায় নিয়ে গ্রাহককে উচ্চ বা নিম্ন ঝুঁকি সম্পন্ন হিসেবে শ্রেণীকরণ করতে হবে। চাকুরির ক্ষেত্রেও অনুরূপভাবে বিস্তারিত ধারণা লাভ করতঃ বিশেষ করে চাকুরির প্রকৃতি ও দায় দায়িত্বের নিরিখে ঝুঁকি নিরূপণ করতে হবে। গ্রাহক উচ্চ ঝুঁকিপূর্ণ হলে নিয়মিত তদারকি করতে হবে)

 হিসাব খোলার কর্মকর্তা/রিলেশনশীপ ম্যানেজারের নাম,
 স্বাক্ষর (সীলসহ) ও তারিখঃ

 অনুমোদনকারী কর্মকর্তার নাম , স্বাক্ষর (সীলসহ)
 ও তারিখঃ

১৬ .হিসাব ও গ্রাহক সংক্রান্ত তথ্যাদি সর্বশেষ পর্যালোচনা / হালনাগাদ করার তারিখ :

 পর্যালোচনা এবং হালনাগাদকারী কর্মকর্তার
 নাম (সিলসহ) স্বাক্ষর ও তারিখঃ

SUSPICIOUS TRANSACTION REPORT (STR) FORM

A. Reporting Institution :1. Name of the FI: 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 and ref. no **C. Suspect Account Details :**1. Account Number: 2. Name of the account: 3. Nature of the account: 4. Nature of ownership:

(Individual/proprietorship/partnership/company/other, pls. specify)

5. Date of opening/Transaction: 6. Address:

D. Account holder details :1. 1. Name of the account holder: 2. Address: 3. Profession: 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. Place of birth: 11. Passport No. 12. National Identification No. 13. Birth Registration No. 14. TIN: 2. 1. Name of the account holder: 2. Relation with the account holder mention in sl. no. D1 3. Address: 4. Profession: 5. Nationality:

6. Other account(s) number(if any):	<input type="text"/>
7. Other business:	<input type="text"/>
8. Father's name:	<input type="text"/>
9. Mother's Name:	<input type="text"/>
10. Date of birth:	<input type="text"/>
11. Place of birth:	<input type="text"/>
12. Passport No.	<input type="text"/>
13. National Identification No.	<input type="text"/>
14. Birth Registration No.	<input type="text"/>
15. TIN:	<input type="text"/>

E. Reasons for considering the transaction(s) as 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 summary of suspicion and consequence of events)
[To be filled by the BAML CIO]

F. Suspicious Activity Information

Summary characterization of suspicious activity:

- | | | |
|---|--|--|
| a. <input type="checkbox"/> Corruption and bribery | k. <input type="checkbox"/> murder, grievous physical injury | u. <input type="checkbox"/> terrorism or financing in terrorist activities |
| b. <input type="checkbox"/> counterfeiting currency | l. <input type="checkbox"/> trafficking of women and children | v. <input type="checkbox"/> adulteration or the manufacture of goods through infringement of title |
| c. <input type="checkbox"/> Counter feiting deeds and documents | m. <input type="checkbox"/> black marketing | w. <input type="checkbox"/> offences relating to the environment |
| d. <input type="checkbox"/> extortion | n. <input type="checkbox"/> smuggling of domestic and foreign currency | x. <input type="checkbox"/> sexual exploitation |
| e. <input type="checkbox"/> fraud | o. <input type="checkbox"/> Theft or robbery or dacoity or piracy or hijacking of aircraft | y. <input type="checkbox"/> insider trading and market manipulation |
| f. <input type="checkbox"/> forgery | p. <input type="checkbox"/> human trafficking | z. <input type="checkbox"/> organized crime, and participation in organized criminal groups |

- g. illegal trade of firearms
- h. illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication
- i. illegal trade in stolen and other goods
- j. kidnapping, illegal restrain and hostage taking
- q. dowry
- r. smuggling and offences related to customs and excise duties
- s. tax related offences
- t. infringement of intellectual property rights
- aa. racketeering
- bb. Other(Please _____ specify)

G. Transaction/Attempted Transaction Details:			
Sl. no.	Date	Amount	Type*

H. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the FI?

Yes No

I. Has the FI taken any action in this context? If yes, give details.

J. Documents to be enclosed

1. Account opening form along with submitted documents
2. KYC Profile
3. Account statement for last one year
4. Supporting Voucher/correspondence mention in sl. no. H
5. Others

Signature :
 (CAMLCO or authorized officer of CCU)
 Name :
 Designation :
 Phone :
 Date :

আর্থিক প্রতিষ্ঠানের নাম

----- শাখা।

শাখা কর্তৃক Self Assessment পদ্ধতির মাধ্যমে নিজস্ব অবস্থান নির্ণয়

প্রতিটি আর্থিক প্রতিষ্ঠানের শাখা মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নবর্ণিত প্রশ্নমালার বিস্তারিত উত্তর প্রদানের মাধ্যমে Self Assessment পদ্ধতিতে নিজেদের অবস্থান নির্ণয় করবে :

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
১. শাখায় মোট কর্মকর্তার সংখ্যা কত (পদানুযায়ী)? কতজন কর্মকর্তা মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? (শতকরা হার)	প্রশিক্ষণ সংক্রান্ত রেকর্ড যাচাই করতে হবে।		
২.ক) শাখার মানিলন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) জেষ্ঠ্য ও অভিজ্ঞ কিনা? বিগত দুই বছরে তিনি মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণ পেয়েছেন কি না? খ) শাখায় মানি লন্ডারিং প্রতিরোধ কার্যক্রম যথানিয়মে পরিপালিত হচ্ছে এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় মনিটরিং ও পর্যালোচনা করে থাকেন কিনা?	BAMLCO কর্তৃক – KYC কার্যক্রমের যথার্থতা মনিটরিং করা হয় কিনা? যথাযথভাবে Transaction মনিটরিং এবং সন্দেহজনক লেনদেন রিপোর্ট (ইন্টারনাল রিপোর্টসহ) করা হয় কিনা? যথাযথভাবে রেকর্ড সংরক্ষণ করা হয় কিনা? STR সনাক্তকরণে ব্যবস্থা নেয়া হয় কিনা?		
৩. BAMLCO সহ শাখার কর্মকর্তাগণ মানিলন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?	বিষয়টি যাচাইয়ের পদ্ধতি কী?		
৪. শাখা পর্যায়ে ত্রৈমাসিক ভিত্তিতে মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক সভা অনুষ্ঠিত হয় কিনা?	সভার আলোচ্যসূচি সকলের অবগতির জন্য বণ্টন করা হয় কিনা? সভায় কী কী গুরুত্বপূর্ণ সিদ্ধান্ত গৃহীত হয়েছে? সভায় গৃহীত সিদ্ধান্ত কিভাবে বাস্তবায়িত হয়?		

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
৫. সকল প্রকার হিসাব খোলা ও লেনদেন পরিচালনার ক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং সময়ে সময়ে বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ?	গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয় কিনা? হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সনাক্ত করা হয় কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরীখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কিনা?		
৬. ক) ঝুঁকির ভিত্তিতে শাখা তাদের গ্রাহকদের শ্রেণীবিন্যাস/শ্রেণীকরণ করে কিনা?	করে থাকলে এ পর্যন্ত কতটি উচ্চ ঝুঁকি সম্পন্ন হিসাব শাখায় খোলা হয়েছে? এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে শাখা কী পদক্ষেপ গ্রহণ করেছে?		
৭. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিলন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা?	এ বিষয়ক নিজস্ব নীতিমালা প্রণয়ন করা হয়েছে কিনা? হলে উক্ত নীতিমালা শাখায় কিভাবে বাস্তবায়িত হচ্ছে?		
৮. শাখা গ্রাহকের KYC Profile এর তথ্য বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা মোতাবেক নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে কিনা?	কী পদ্ধতিতে এরূপ মূল্যায়ন সম্পাদিত হয়ে থাকে?		

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
<p>৯. সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসী কার্যে অর্থাৎ প্রতিরোধের লক্ষ্যে শাখা কী ধরনের পদক্ষেপ গ্রহণ করেছে?</p>	<p>জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থাৎ জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কি না? এরূপ কোন ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা?</p>		
<p>১০. এ যাবৎ শাখা কর্তৃক কতগুলো সন্দেহজনক লেনদেন (STR) শনাক্ত করা হয়েছে?</p>	<p>শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখায় সন্দেহজনক লেনদেন রিপোর্টিং এর জন্য Internal Reporting Mechanism চালু রয়েছে কিনা? শাখা পর্যায়ে নিষ্পত্তিকৃত Internal Report সংরক্ষণ করা হয় কিনা?</p>		
<p>১১. মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন, সার্কুলার, প্রশিক্ষণ রেকর্ড, বিবরণী ও অন্যান্য এএমএল/সিএফটি সংক্রান্ত বিষয়াবলীর আলাদা নথি শাখা কর্তৃক সংরক্ষণ করা হয় কিনা? আইন, সার্কুলার ইত্যাদির কপি শাখার</p>	<p>সংরক্ষিত হয়ে থাকলে হ্যাঁ অথবা না হয়ে থাকলে না, আংশিক হলে কী কী সংরক্ষিত আছে তা লিখুন।</p>		

প্রশ্নমালা	যাচাইয়ের মানদণ্ড	শাখার বর্তমান-অবস্থা	গৃহীতব্য কার্যক্রম/সুপারিশ
সকল কর্মকর্তা/কর্মচারীদের সরবরাহ করা হয় কিনা?			
১২. বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা?	উত্তর হ্যাঁ হলে এই হিসাব খোলা ও পরিচালনার ক্ষেত্রে কী কী ধরনের সতর্কতা অবলম্বন করা হচ্ছে?		
১৩. আর্থিক প্রতিষ্ঠানের প্রধান কার্যালয়, বাংলাদেশ ব্যাংক ও বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউট-এর পরিদর্শন প্রতিবেদনে উল্লেখিত মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ পরিপালন বিষয়ক দুর্বলতা/অনিয়মসমূহ নিয়মিত করা হয়েছে কিনা?	না হয়ে থাকলে প্রতিবন্ধকতাসমূহ কী কী?		

শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তার নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ	শাখা ব্যবস্থাপকের নামযুক্ত সীলসহ স্বাক্ষর ও তারিখ
--	---

অভ্যন্তরীণ নিরীক্ষা বিভাগ
আর্থিক প্রতিষ্ঠানের নাম
প্রধান কার্যালয়

Independent Testing Procedures:
শাখা পরিদর্শনের চেকলিস্ট

আর্থিক প্রতিষ্ঠানের অভ্যন্তরীণ নিরীক্ষা বিভাগ মানিলাভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও প্রতিষ্ঠানের নিজস্ব মানি লভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ নীতিমালার আলোকে নিম্নলিখিত প্রশ্নমালার যথাযথ উত্তর (ডকুমেন্ট ভিত্তিক) অনুসারে স্কোর প্রদানপূর্বক শাখার মানি লভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ কার্যক্রমকে মূল্যায়ন করবে। অভ্যন্তরীণ নিরীক্ষা বিভাগ কর্তৃক শাখার উপর প্রণীত বার্ষিক নিরীক্ষা প্রতিবেদনে (প্রযোজ্য ক্ষেত্রে পৃথক পরিদর্শন কর্মসূচীর আওতায় শুধুমাত্র Independent Testing Procedures ভিত্তিক প্রতিবেদন প্রণীত হবে) মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়ন সংক্রান্ত আলাদা অধ্যায়ে সমুদয় বিষয়াদি সুপারিশসহ সন্নিবেশ করবে।

(যাচাইয়ের মানদণ্ড অনুসারে সম্পূর্ণরূপে পরিপালিত হলে সম্পূর্ণ স্কোর, আংশিক পরিপালনে আংশিক স্কোর এবং উত্তর নেতিবাচক হলে শূন্য স্কোর প্রদান করতে হবে।)

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	স্কোর	প্রাপ্ত স্কোর	মন্তব্য	
১.	শাখা পরিপালন ইউনিট	১.	শাখায় একজন অভিজ্ঞ ও জ্যেষ্ঠ পরিপালন কর্মকর্তা (BAMLCO) রয়েছেন কি?	অফিস অর্ডার দেখুন। শাখার দ্বিতীয় কর্মকর্তা বা অভিজ্ঞ কোন উর্ধ্বতন কর্মকর্তাকে BAMLCO মনোনীত করা সমীচীন হবে।	১		
		২.	বিগত দুই বছরে তিনি মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণে অংশগ্রহণ করেছেন কি? মানিলাভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে তিনি যথেষ্ট অবহিত কি?	সাক্ষাৎকার ও নথিপত্রের ভিত্তিতে যাচাই করুন।	২		
		৩.	মানি লভারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং এর আওতায় জারীকৃত পলিসি এবং/অথবা নির্দেশনা যথানিয়মে পরিপালিত হচ্ছে- এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় মনিটরিং ও পর্যালোচনা করে থাকেন কি?	BAMLCO কর্তৃক মনিটরিং ও পর্যালোচনার প্রক্রিয়া যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন।	৩		

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	স্কোর	প্রাপ্ত স্কোর	মন্তব্য
		<p>৪. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিলভারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা?</p> <p>BAMLCO কর্তৃক শাখায় পরিচালিত উচ্চ ঝুঁকিযুক্ত হিসাবসহ সকল হিসাবের লেনদেন মনিটরিং পর্যাপ্ত কি?</p>	<p>মানিলভারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে শাখার গৃহীত পদক্ষেপ মূল্যায়ন করণ।</p> <p>BAMLCO কর্তৃক উচ্চ ঝুঁকিযুক্ত হিসাবসহ সকল হিসাবের লেনদেন মনিটরিং পদ্ধতি যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করণ।</p>	৪		
		<p>৫. বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা?</p>	<p>এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে বিএফআইইউ মাস্টার সার্কুলার অনুসারে সতর্কতা অবলম্বন করা হচ্ছে কিনা তা যাচাই করণ। তবে PEPs প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব না থাকলেও যদি বিএফআইইউ মাস্টার সার্কুলার এ প্রদত্ত নির্দেশনা বাস্তবায়নের প্রক্রিয়া বিদ্যমান থাকে তাহলে শাখা পূর্ণ নম্বর প্রাপ্ত হবে।</p>	৩		
		<p>৬. বিএফআইইউ প্রদত্ত সেলফ অ্যাসেসমেন্ট শাখা কর্তৃক কতটুকু সঠিক ও কার্যকরভাবে সম্পাদন হচ্ছে?</p>	<p>শাখার সেলফ অ্যাসেসমেন্ট রিপোর্ট পর্যালোচনা করণ। সঠিক ও কার্যকরভাবে সেলফ অ্যাসেসমেন্ট রিপোর্ট প্রণয়ন ও বাস্তবায়নের ভিত্তিতে নম্বর প্রদান করণ।</p>	৬		
২.	মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ে কর্মকর্তাদের জ্ঞান ও সচেতনতা বৃদ্ধি এবং ঝুঁকি প্রতিরোধে গৃহীত ব্যবস্থা।	<p>১. শাখায় কতজন কর্মকর্তা মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন?</p> <p>২. শাখার কর্মকর্তাগণ মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি?</p>	<p>১০০% কর্মকর্তার প্রশিক্ষণ সম্পন্ন হলে তা সন্তোষজনক বলে বিবেচিত হবে। প্রশিক্ষণের হার অনুসারে নম্বর প্রাপ্ত হবে।</p> <p>শাখার সংশ্লিষ্ট কর্মকর্তাদের সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করণ।</p>	৩		
				৪		

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	স্কের	প্রাপ্ত স্কের	মন্তব্য
		৩. মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়নের জন্য একটি ত্রৈমাসিক ভিত্তিতে শাখা ব্যবস্থাপকের নেতৃত্বে কর্মকর্তাগণের সভা আয়োজন করা হয় কিনা?	সভার আলোচ্যসূচী সংগ্রহ ও এর কার্যকারিতা পরীক্ষা করণ।	৫		
		৪. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং ব্যাংকের নিজস্ব নীতিমালা অনুযায়ী মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা?		৩		
৩.	গ্রাহক পরিচিতি (KYC) পদ্ধতি	১. সকল প্রকার হিসাব খোলা ও লেনদেন পরিচালনার ক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং বিএফআইইউ কর্তৃক জারীকৃত মাস্টার সার্কুলারের নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ?	প্রত্যেক ধরনের ৪/৫ টি হিসাবের নমুনা পরীক্ষা করণ। নিম্নোক্ত বিষয়ে সন্তুষ্টিসাপেক্ষে নম্বর প্রদান করণ- গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয়েছে কিনা? হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সনাক্ত করা হয়েছে কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরিখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কি না?	৬		
		২. বিএফআইইউ কর্তৃক জারীকৃত মাস্টার সার্কুলারের নির্দেশনা অনুসারে শাখা যথাযথভাবে ঝুঁকির ভিত্তিতে তাদের গ্রাহকদের শ্রেণীবিন্যাস/ শ্রেণীকরণ করে কি?	বিএফআইইউ কর্তৃক জারীকৃত মাস্টার সার্কুলারের নির্দেশনা পরিপালিত হয় কিনা যাচাই করণ।	৬		
		৩. উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে প্রয়োজনীয় অতিরিক্ত তথ্য সংগ্রহ করা হয় কি?	কি ধরনের তথ্য সংগ্রহ করা হয় এবং তা যথেষ্ট কিনা পরীক্ষা করণ।	৫		
		৪. শাখা কি গ্রাহকের KYC Profile নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে থাকে?	KYC Profile পুনঃমূল্যায়ন ও হালনাগাদ পদ্ধতি মূল্যায়ন করণ।	৫		

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	স্কের	প্রাপ্ত স্কের	মন্তব্য
8.	সন্ত্রাস বিরোধী আইন, ২০০৯ এর পরিপালন	সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখা কী ধরনের কার্যকর পদক্ষেপ গ্রহণ করেছে?	নিম্নোক্ত বিষয়ে সন্তুষ্টিসাপেক্ষে নম্বর প্রদান করুন- জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কিনা? এরূপ ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা ?	৫		
৫.	সন্দেহজনক লেনদেন রিপোর্ট (STR) ও নগদ লেনদেন রিপোর্ট(CTR)	১.	শাখার কর্মকর্তাগণ সন্দেহজনক লেনদেন রিপোর্ট (STR) সম্পর্কে অবহিত আছেন কি?	শাখায় সন্দেহজনক লেনদেন Reporting এর জন্য Internal Reporting Mechanism চালু আছে কিনা? তা সকল কর্মকর্তা জানেন কিনা?	৫	
		২.	শাখায় মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত সন্দেহজনক লেনদেন চিহ্নিতকরণের কার্যকর পদ্ধতি চালু আছে কি? এ যাবৎ কতগুলো সন্দেহজনক লেনদেন (STR) BAMLCO কর্তৃক CCU এর নিকট রিপোর্ট করা হয়েছে?	শাখায় সন্দেহজনক লেনদেন সংঘটিত হওয়া সত্ত্বেও যদি BAMLCO কর্তৃক CCU এর নিকট কোন STR না করা হয়ে থাকে তাহলে তা অসন্তোষজনক বিবেচিত হবে। নথি ও সিস্টেম পরীক্ষা করে শাখায় STR সনাক্তকরণের জন্য কোন পদ্ধতির প্রবর্তন করা হয়েছে কিনা তা যাচাই করুন। নিম্নোক্ত বিষয়ে সন্তুষ্টি সাপেক্ষে নম্বর প্রদান করুন- শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখা পর্যায়ে নিষ্পত্তিকৃত Internal Report যথাযথভাবে সংরক্ষণ করা হয় কিনা?	8	

ক্রমিক নং	অঞ্চল/এরিয়া	প্রশ্নমালা	যাচাইয়ের মানদণ্ড	স্কের	প্রাপ্ত স্কের	মন্তব্য
		৩. শাখা কর্তৃক যথাযথ ও সঠিকরূপে নগদ লেনদেন রিপোর্ট (CTR) করা হয় কিনা?	এতদসংক্রান্ত নথি পরীক্ষা করণ। (কমপক্ষে এক মাসের নগদ লেনদেন) ক্যাশ রেজিস্টার/বিবরণী হতে পরীক্ষা করণ এবং এর ভিত্তিতে ঐ মাসে দাখিলকৃত CTR রিপোর্ট পরীক্ষাপূর্বক CTR রিপোর্ট এর সঠিকতার বিষয়ে মূল্যায়ন করণ।	২		
৬.	CCU বরাবর বিবরণী দাখিল	১. শাখা কর্তৃক কতটি বিবরণী (CCU বরাবর দাখিল করা হয়? শাখা কি যথাসময়ে বিবরণী দাখিল করে?	এতদসংক্রান্ত নথি পরীক্ষা করণ। বিলম্বে অথবা বিবরণী দাখিল না করলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
		২. শাখা কর্তৃক নিয়মিতভাবে সেক্ষ অ্যাসেসমেন্ট করা হয় কিনা? প্রস্তুতকৃত বিবরণী যথাযথ কিনা?	এতদসংক্রান্ত বিবরণী পরীক্ষা করণ। তথ্যাদি সঠিক ও পরিপূর্ণ না হলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
৭.	রেকর্ড সংরক্ষণ	১. গ্রাহক পরিচিতি (KYC) এবং লেনদেন সম্পর্কিত রেকর্ড যথাযথভাবে সংরক্ষণের বিধান আছে কি?	৫টি বন্ধ হিসাব পরীক্ষা করণ। এক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন এর বিধান যথাযথভাবে অনুসরণ করা হয়েছে কিনা যাচাই করণ।	৪		
		২. নিয়ন্ত্রণকারী কর্তৃপক্ষ বা CCU এর চাহিদা মোতাবেক রেকর্ডসমূহ সরবরাহ করা হয় কি?	এতদসংক্রান্ত নথি পরীক্ষা করণ। যথাসময়ে ও যথাযথ তথ্য সরবরাহ না করলে তা অসন্তোষজনক বিবেচিত হবে।	৩		
৮.	AML/CFT সম্পর্কিত শাখার সার্বিক কার্যক্রম	১. শাখা ব্যবস্থাপক (BAMLCO না হলে) মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক কর্মসূচী বাস্তবায়নে যথাযথ ভূমিকা পালন করে কি?	শাখায় আয়োজিত সভার আলোচ্যসূচি ও শাখা ব্যবস্থাপকের সাথে সাক্ষাৎকার এবং এ বিষয়ে শাখার পরিপালন অবস্থার ভিত্তিতে মূল্যায়ন করণ।	৫		
		২. পূর্ববর্তী অভ্যন্তরীণ ও বহিঃ নিরীক্ষা প্রতিবেদন পরীক্ষাকালে AML/CFT বিষয়ক কোন অনিয়ম ও দুর্বলতার উল্লেখ আছে কিনা এবং শাখা কোন সংশোধনমূলক ব্যবস্থা গ্রহণ করেছে কিনা?	সর্বশেষ নিরীক্ষা সংক্রান্ত রিপোর্ট পরীক্ষা করণ এবং কি ধরনের সংশোধনমূলক ব্যবস্থা নেওয়া হয়েছে যাচাই করণ।	৪		
		৩. শাখার সার্বিক কার্যক্রম সন্তোষজনক কি?	শাখার মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ সংক্রান্ত সার্বিক কার্যক্রম এবং শাখা ব্যবস্থাপকের পারফরম্যান্সের ভিত্তিতে মূল্যায়ন করণ।	৬		
			মোট	১০০		

শাখার সার্বিক মূল্যায়ন :

স্কোর	রেটিং
৯০ ⁺ -১০০	শক্তিশালী (Strong)
৭০ ⁺ -৯০	সন্তোষজনক (Satisfactory)
৫৫ ⁺ -৭০	মোটামুটি ভাল (Fair)
৪০ ⁺ -৫৫	প্রান্তিক (Marginal)
৪০ ও এর নিচে	অসন্তোষজনক (Unsatisfactory)

বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইউনিট
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা।

ওয়েবসাইট : www.bb.org.bd

বিএফআইইউ সার্কুলার লেটার নং- ০৪/২০১৫

তারিখ : ১৫ শ্রাবণ, ১৪২২
৩০ জুলাই, ২০১৫

ব্যবস্থাপনা পরিচালক ও প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল আর্থিক প্রতিষ্ঠান

প্রিয় মহোদয়,

মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়নের ঝুঁকি নিরূপণ/চিহ্নিতকরণ ও চিহ্নিত ঝুঁকি মোকাবেলায় কার্যকর ব্যবস্থা গ্রহণের নিমিত্তে প্রণীত গাইডলাইন জারীকরণ প্রসঙ্গে।

মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধে আন্তর্জাতিক মানদণ্ড নির্ধারণকারী প্রতিষ্ঠান Financial Action Task Force (FATF) এর ১ নম্বর সুপারিশে প্রতিটি দেশের আর্থিক খাতের বিভিন্ন প্রতিষ্ঠান যেমন ব্যাংক, আর্থিক প্রতিষ্ঠান, বিমা কোম্পানী, সিকিউরিটিজ মার্কেট ইন্টারমিডিয়্যারিজ ও Designated Non Financial Businesses and Professions (DNFBPs) কে মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়নের ঝুঁকি নিরূপণপূর্বক উক্ত ঝুঁকি মোকাবেলায় কার্যকরী ব্যবস্থা গ্রহণের উল্লেখ রয়েছে। এদিকে, মানিলভারিং প্রতিরোধ বিধিমালা, ২০১৩ এর ২১(১) নম্বর বিধি মোতাবেক প্রতিটি রিপোর্ট প্রদানকারী সংস্থা নির্দিষ্ট সময় অন্তর অন্তর তাদের ঝুঁকি নিরূপণপূর্বক তা ব্যবহার/বাস্তবায়নের পূর্বে অনুপূঞ্জ পর্যালোচনার জন্য বিএফআইইউতে প্রেরণ করার আবশ্যিকতা রয়েছে।

২। আর্থিক প্রতিষ্ঠানসমূহ কর্তৃক নিজ নিজ প্রতিষ্ঠানের মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়নের ঝুঁকি মোকাবেলায় কার্যকরী ব্যবস্থা গ্রহণের নিমিত্তে “[Money Laundering and Terrorist Financing Risk Assessment Guidelines for Financial Institutions](https://www.bb.org.bd/bfiu/bfiu_lawguidelist.php)” প্রণয়ন করা হয়েছে যা মানিলভারিং প্রতিরোধ আইন, ২০১২ এর ২৩ (১)(ঘ) ধারা এবং সন্ত্রাস বিরোধী আইন, ২০০৯ এর ১৫(১)(ঘ) ধারায় প্রদত্ত ক্ষমতাবলে জারী করা হলো। গাইডলাইনটি বাংলাদেশ ব্যাংকের ওয়েব সাইট (https://www.bb.org.bd/bfiu/bfiu_lawguidelist.php) হতে ডাউনলোড করা যাবে।

৩। আলোচ্য গাইডলাইনটির আলোকে আর্থিক প্রতিষ্ঠানসমূহকে নিজ নিজ প্রতিষ্ঠানের মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়নের ঝুঁকি নিরূপণ/চিহ্নিত করণপূর্বক চিহ্নিত ঝুঁকি মোকাবেলায় প্রয়োজনীয় ব্যবস্থা গ্রহণের নিমিত্তে Risk Assessment Report প্রণয়নকরত যথাযথ কর্তৃপক্ষের অনুমোদন গ্রহণ করে আগামী ৩১ আগস্ট, ২০১৫ তারিখের মধ্যে এ ইউনিটে প্রেরণ করার জন্য নির্দেশনা প্রদান করা যাচ্ছে।

৪। আর্থিক প্রতিষ্ঠানসমূহ কর্তৃক প্রণীত Risk Assessment Report এ চিহ্নিত ঝুঁকি ও তা মোকাবেলায় গৃহীতব্য কার্যকর ব্যবস্থা বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউশন ইউনিট কর্তৃক “Managing Core Risks of Financial Institutions” এর আওতায় প্রণীত ‘Guidance Notes on Prevention of Money Laundering and Terrorist Financing’ এর হালনাগাদকরণে ইনপুট হিসেবে ব্যবহৃত হবে। উল্লেখ্য, আর্থিক প্রতিষ্ঠানসমূহকে উক্ত Guidance Notes টি আগামী ৩০ সেপ্টেম্বর, ২০১৫ তারিখের মধ্যে হালনাগাদ করতে হবে।

আপনাদের বিশ্বস্ত,

(মোঃ নাসিরুজ্জামান)

মহাব্যবস্থাপক

ফোন : ৯৫৩০১১৮

বাংলাদেশ ফাইন্যান্সিয়াল ইন্সটিটিউট

বাংলাদেশ ব্যাংক

প্রধান কার্যালয়

ঢাকা।

ওয়েবসাইট : www.bb.org.bd

বিএফআইইউ সার্কুলার লেটার নং- ০৬/২০১৫

তারিখঃ ২৪ অগ্রহায়ণ, ১৪২২
০৮ ডিসেম্বর, ২০১৫

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা

বাংলাদেশে কার্যরত সকল ব্যাংক, আর্থিক প্রতিষ্ঠান, বীমাকারী, মানি চেঞ্জার, অর্থ অথবা অর্থমূল্য প্রেরণকারী বা স্থানান্তরকারী যে কোন কোম্পানী বা প্রতিষ্ঠান, স্টক ডিলার ও স্টক ব্রোকার, পোর্টফোলিও ম্যানেজার ও মার্চেন্ট ব্যাংকার, সিকিউরিটি কাস্টডিয়ান, সম্পদ ব্যবস্থাপক, অলাভজনক সংস্থা/প্রতিষ্ঠান, বেসরকারি উন্নয়ন সংস্থা, সমবায় সমিতি, রিয়েল এস্টেট ডেভেলপার, মূল্যবান ধাতু বা পাথরের ব্যবসা প্রতিষ্ঠান, ট্রাস্ট ও কোম্পানী সেবা প্রদানকারী, আইনজীবী, নোটারী, অন্যান্য আইন পেশাজীবী এবং একাউন্টেন্ট।


মানিলভারিং প্রতিরোধ (সংশোধন) আইন, ২০১৫ জারীকরণ প্রসঙ্গে।

প্রিয় মহোদয়গণ,

বাংলাদেশ জাতীয় সংসদ কর্তৃক গৃহীত মানিলভারিং প্রতিরোধ (সংশোধন) আইন, ২০১৫ (২০১৫ সনের ২৫ নং আইন) গত ২৬ নভেম্বর, ২০১৫ তারিখে মহামান্য রাষ্ট্রপতির সম্মতি লাভের মাধ্যমে উক্ত তারিখ হতে কার্যকর হয়েছে। উক্ত আইনটি বাংলাদেশ গেজেটের অতিরিক্ত সংখ্যায় একই তারিখে প্রকাশ করা হয়েছে। জারীকৃত আইনের বিধানসমূহ পরিপালন ও সংশ্লিষ্ট সকলের অবগতিতে আনয়নের সুবিধার্থে আইনটি বিএফআইইউ এর ওয়েবসাইটে আপলোড করা হয়েছে, যা https://www.bb.org.bd/bfiu/bfiu_acts.php ওয়েবলিংক হতে ডাউনলোড করা যাবে।

এই আইনের নির্দেশনা পরিপালন নিশ্চিতকরণ ও বিষয়টি সংশ্লিষ্ট সকলের অবগতিতে আনয়নের জন্য আপনাদেরকে পরামর্শ প্রদান করা হলো।

আপনাদের বিশ্বস্ত,



(দেবপ্রসাদ দেবনাথ)

মহাব্যবস্থাপক

ফোন : ৯৫৩০১১৮

বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা।

ওয়েবসাইট : www.bb.org.bd

বিএফআইইউ সার্কুলার লেটার নং- ০১/২০১৬

তারিখ : ২৯ মাঘ, ১৪২২
১১ ফেব্রুয়ারি, ২০১৬

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা

বাংলাদেশে কার্যরত সকল ব্যাংক, আর্থিক প্রতিষ্ঠান, বীমাকারী, মানি চেঞ্জার, অর্থ অথবা অর্থমূল্য প্রেরণকারী বা স্থানান্তরকারী যে কোন কোম্পানী বা প্রতিষ্ঠান, স্টক ডিলার ও স্টক ব্রোকার, পোর্টফোলিও ম্যানেজার ও মার্চেন্ট ব্যাংকার, সিকিউরিটি কাস্টডিয়ান, সম্পদ ব্যবস্থাপক, অলাভজনক সংস্থা/প্রতিষ্ঠান, বেসরকারি উন্নয়ন সংস্থা, সমবায় সমিতি, রিয়েল এস্টেট ডেভেলপার, মূল্যবান ধাতু বা পাথরের ব্যবসা প্রতিষ্ঠান, ট্রাস্ট ও কোম্পানী সেবা প্রদানকারী, আইনজীবী, নোটারী, অন্যান্য আইন পেশাজীবী এবং একাউন্টেন্ট।

জাতিসংঘ নিরাপত্তা পরিষদের বিভিন্ন রেজুলুশনের আওতায় তালিকাভুক্ত ব্যক্তি বা প্রতিষ্ঠানের
হিসাব অবরুদ্ধকরণ ও অন্যান্য বিষয়ে অনুসরণীয় নির্দেশনা প্রসঙ্গে।

প্রিয় মহোদয়গণ,

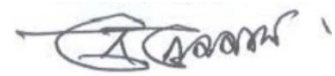
জাতিসংঘ চার্টারের ৭নং অধ্যায়ের আওতায় আন্তর্জাতিক শান্তি ও নিরাপত্তা রক্ষার নিমিত্তে জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক গৃহীত রেজুলুশনের নির্দেশনাসমূহ পরিপালনে অন্যান্য দেশের ন্যায় বাংলাদেশেরও বাধ্যবাধকতা রয়েছে। এদিকে সন্ত্রাস বিরোধী আইন, ২০০৯ এর ধারা ১৫(৩), ২০ ও ২০(ক) এর আওতায় জাতিসংঘের নিরাপত্তা পরিষদ কর্তৃক গৃহীত রেজুলুশনের নির্দেশনাসমূহ যথাযথভাবে পরিপালন ও এর আওতায় তালিকাভুক্ত ব্যক্তি অথবা প্রতিষ্ঠানের নামে অথবা প্রত্যক্ষ বা পরোক্ষভাবে তাদের নিয়ন্ত্রণাধীন/স্বার্থ সংশ্লিষ্ট কোন প্রতিষ্ঠানের নামে কোন হিসাব/লেনদেন পরিচালিত হলে তা অবিলম্বে অবরুদ্ধ করার বিধান রয়েছে। আলোচ্য আইনের উক্ত বিধান এবং সন্ত্রাস বিরোধী বিধিমালা, ২০১৩ এর সংশ্লিষ্ট বিধানসমূহ রিপোর্ট প্রদানকারী সংস্থাগুলো কর্তৃক যথাযথভাবে পরিপালনের নিমিত্তে এ ইউনিট হতে সার্কুলার, সার্কুলার লেটার, গাইডলাইন্স জারীপূর্বক সময়ে সময়ে নির্দেশনা প্রদান করা হয়েছে। উক্ত নির্দেশনাসমূহে ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তার রোধে গৃহীত রেজুলুশনে রিপাবলিক অব ইরানের বিভিন্ন ব্যক্তি ও প্রতিষ্ঠান অন্তর্ভুক্ত ছিল।

এদিকে গত ২০ জুলাই, ২০১৫ তারিখে জাতিসংঘ নিরাপত্তা পরিষদে গৃহীত ২২৩১ নং রেজুলুশন মোতাবেক ইরান Joint Comprehensive Plan of Action (JCPOA) বাস্তবায়ন করায় ১৬ জানুয়ারি, ২০১৬ হতে ইতোপূর্বে ইরান বিষয়ে জাতিসংঘ নিরাপত্তা পরিষদের গৃহীত রেজুলুশন নং ১৬৯৬, ১৭৩৭, ১৭৪৭, ১৮০৩, ১৮৩৫, ১৯২৯ ও ২২২৪ নং রেজুলুশনের কার্যকারিতা রহিত হয়েছে।

উল্লেখ্য, জাতিসংঘ নিরাপত্তা পরিষদ কর্তৃক আন্তর্জাতিক শান্তি ও নিরাপত্তা রক্ষার নিমিত্তে গৃহীত রেজুলুশনসমূহের (যে সকল রেজুলুশনে ব্যক্তি বা প্রতিষ্ঠানকে তালিকাভুক্ত করা হয়েছে) আওতায় তালিকাভুক্ত ব্যক্তি বা প্রতিষ্ঠানের নামের একটি সমন্বিত তালিকা প্রস্তুত করা হয়ে থাকে যা নিয়মিত বিরতিতে পরিবর্তিত/পরিমার্জিত হয়। উক্ত তালিকা সর্বশেষ ১৭ জানুয়ারি, ২০১৬ তারিখে পরিবর্তিত/পরিমার্জিত হয় যা নিম্নবর্ণিত ওয়েবলিংকে পাওয়া যাবেঃ <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>

উপর্যুক্ত বিষয়সমূহ সংশ্লিষ্ট সকল পক্ষের অবগতিতে আনয়ন ও বাস্তবায়নের জন্য আপনাদেরকে পরামর্শ প্রদান করা হলো।

আপনাদের বিশ্বস্ত,



(দেবপ্রসাদ দেবনাথ)

মহাব্যবস্থাপক ও অপারেশনাল হেড

ফোন : ৯৫৩০১১৮