

Premier Bank
service first



2022

**Policy Guidelines on Anti
Money Laundering and
Combating Financing of
Terrorism**

Foreword

As for Banking Business taking risk is an integral part, therefore, financial institutions should be required to have policies, guidelines, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. Bank should be required to monitor the implementation of those controls and to enhance them, if necessary. Failure to assess and manage risks adequately may lead to losses and affecting the stability of the overall financial system.

For banks in emerging markets, the regulatory requirement is more complicated than ever. Rules designed to fight money laundering and root out terrorist financing have made the financial system safer and more resilient but have also increased the cost and complexity of doing business in developing countries.

In recent years, Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) compliance requirements have created a marked increase in cost and complexity to banks globally. These regulatory changes have increased financial system resilience and helped battle financial crime. These regulatory changes have also put increased pressure on correspondent banking relationships and cross border financial networks.

Bangladesh Bank as the apex regulatory body for the country's monetary and financial system plays a pivotal role to stabilize and enhance the efficiency of the financial system. Bangladesh Financial Intelligence Unit (BFIU) as the central agency of Bangladesh has taken several initiatives to establish an effective system for anti money laundering, combating financing of terrorism and proliferation of weapons of mass destruction. Issuance of circulars/circular letters, Guidance Notes under Money Laundering Prevention Act (MLPA) 2012 (Amendment 2015) and Anti-Terrorism Act (ATA) 2009 (amendment 2012 & 2013) are some of the examples.

To make the Bank free from the Risk of Money Laundering & Terrorist Financing and to prepare the Bank to comply with the legal and regulatory framework Premier Bank Limited has prepared this "Policy and Guidelines on Anti Money Laundering and Combating Financing of Terrorism" that will interpret the requirements of the relevant laws and regulations, and how they might be implemented in practice. Premier Bank instructs all the Branches/Divisions/Departments to follow the guideline in order to mitigate Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) risks.



CORPORATE INFORMATION

CORPORATE OFFICE

42, Kemal Ataturk Avenue
Iqbal Center
Banani,
Dhaka-1213

FAX

+8802-2222-74849
+8802-2222-74808

PABX

+8802-222274844-8

EMAIL

info@premierbankltd.com

SWIFT

PRMRBDDH

WEBSITE

www.premierbankltd.com

PREVIOUS EDITION

"ML & TF Policies and Guidelines"

First Edition published on 27 November 2019

REVISED EDITION

Policy Guidelines on Anti Money Laundering and Combating Financing of Terrorism

Published date -

The Premier Bank Limited, Corporate Office, Dhaka.



CONTRIBUTOR

Chief Coordinator

Mohd. Jamil Hossain CMA

SEVP & CAMLCO

REVIEW TEAM

Mohammad Zakir Hossain, AML & CFT Division

Md. Saiful Islam, AML & CFT Division

Md. Ramjan Ali, AML & CFT Division



M. Saiful Islam

LIST OF ABBREVIATIONS

ACC	Anti-Corruption Commission
ADB	Asian Development Bank
AML & CFT	Anti-Money Laundering and Combating Financing of Terrorism
AMC	Adverse Media Screening
APG	Asia Pacific Group
ARS	Alternative Remittance Systems
ATA	Anti-Terrorism Act
BAMLCO	Branch Anti-Money Laundering Compliance Officer
BACH	Bangladesh Automated Clearing House
BB	Bangladesh Bank
BEFTN	Bangladesh Electronic Fund Transfer Network
BFIU	Bangladesh Financial Intelligence Unit
CAMLCO	Chief Anti-Money Laundering Compliance Officer
CCC	Central Compliance Committee
CDD	Customer Due Diligence
CPV	Contact Point Verification
CSR	Corporate Social Responsibility
CTR	Cash Transaction Report
DAMLCO	Deputy Anti-Money Laundering Compliance Officer
DNFBP	Designated non-financial businesses and professions
EDD	Enhanced Due Diligence
E-KYC	Electronic Know Your Customer
E-TIN	Electronic Tax Identification Number
FARF	Financial Action Task Force
FERA	Foreign Exchange Regulation Act
FI	Financial Institution
FIU	Financial Intelligence Unit
FSRB	FATF Style Regional Body
GFET	Guideline for Foreign Exchange Transactions
HRD	Human Resources Division
ICCD	Internal Control & Compliance Division
IMF	International Monetary Fund
ITP	Independent Testing Procedure
IP	Influential Person
KYC	Know Your Customer
KYE	Know Your Employee
MD & CEO	Managing Director & Chief Executive Officer
MER	Mutual Evaluation Report
MIS	Management Information System
ML	Money Laundering
MLPA	Money Laundering Prevention Act
MOU	Memorandum of Understanding
NRA	National ML & TF Risk Assessment
NCC	National Coordination Committee
NGO	Non-Government Organisation
NPO	Non-Profit Organisation






LIST OF ABBREVIATIONS

NRB	Non-Residentail Bangladeshi
OECD	Organization for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control
PBL	Premier Bank Limited
PEP	Politically Exposed Person
PF	Proliferation Financing
SAP	Self-Assessment Procedure
SAR	Suspicious Activity Report
SIP	Strategic Implementation Plan
SRO	Statutory Regulatory Order
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TP	Transaction Profile
UN	United Nations
UNODC	United Nations Office of Drug and Crime
UNSCR	United Nations Security Council Resolution
WMD	Weapons of Mass Destruction





m. emsa

Table of Contents

CHAPTER I: BACKGROUND 13

Preamble..... 13

Policy Guideline Objective 14

Policy Statement 14

Scope and Enforcement 16

Clarifications of the Policy Guidelines..... 16

What is Money Laundering? 16

Money Laundering Definition..... 17

Property Definition..... 18

Stages of Money Laundering 18

The Economic and Social Consequences of Money Laundering 20

Control Lose/Mistakes in Decisions Regarding Economic Policy 22

Risk to Privatization Efforts..... 22

Definition of Terrorist Financing..... 23

The Link between Money Laundering and Terrorist Financing 24

The difference Between Money Laundering and Terrorist Financing 24

Why We Must Combat Money Laundering and Terrorist Financing 25

Vulnerability of the Financial System to Money Laundering 26

How Financial Institutions Can Combat Money Laundering 27

How Premier Bank Can Combat Money Laundering 28

Compliance Program Development of Premier Bank..... 29

Communication of Compliance Program 29

Targeted Financial Sanctions..... 29

CHAPTER II: INTERNATIONAL INITIATIVES..... 31

Introduction 31

The United Nations..... 31

The Vienna Convention..... 31

The Palermo Convention..... 31

International Convention for the Suppression of the Financing of Terrorism 32

The convention requires ratifying states to criminalize terrorism, terrorist..... 32

Security Council Resolution 1267 and Successors..... 32

Security Council Resolution 1373 33

Security Council Resolution 1540 33

The Counter-Terrorism Committee..... 33

The Counter-Terrorism Implementation Task Force (CTITF)..... 34

[Handwritten signature]

[Handwritten signature]



m. aubwa

Global Program against Money Laundering 34

The Financial Action Task Force..... 34

FATF 40+9 Recommendations 34

FATF New Standards 35

Summary of new FATF 40 Standards 35

Some highlights of the 40 Recommendations are: 36

Monitoring Members Progress..... 52

The NCCT List..... 52

ICRG..... 53

The Basel Committee on Banking Supervision 53

Statement of Principles on Money Laundering 53

Basel Core Principles for Banking 54

Customer Due Diligence..... 54

International Organization of Securities Commissioners 54

The Egmont Group of Financial Intelligence Units 54

Asia Pacific Group on Money Laundering (APG) 55

CHAPTER III: NATIONAL INITIATIVES..... 56

National Initiatives 56

Founding Member of APG..... 56

Legal Framework..... 56

Central and Regional Taskforce 57

Anti Money Laundering Department 57

Bangladesh Financial Intelligence Unit 57

National ML & TF Risk Assessment (NRA) 58

National Strategy for Preventing ML, TF & PF 58

Chief Anti Money Laundering Compliance Officers (CAMLCO) Conference..... 59

Egmont Group Memberships 59

Anti Militants and De-Radicalization Committee 59

Memorandum of Understanding (MOU) Between ACC and BFIU..... 59

NGO/NPO Sector Review 59

Implementation of TFS 60

Coordinated Effort on the Implementation of the UNSCR 60

Risk Based Approach 60

ML and TF Risk Assessment Guidelines..... 61

Memorandum of Understanding (MOU) and Other FIUs 61

CHAPTER IV: VULNERABILITIES OF FINANCIAL INSTITUTIONS 62

Vulnerability of the Financial System to Money Laundering 62





Handwritten signature

Vulnerabilities of Products and Services63

Private Placement of Equity/Securitization of Assets65

Personal Loan/Car Loan/Home Loan65

SME/Women Entrepreneur Loan65

Deposit Scheme.....65

Loan Backed Money Laundering.....65

Electronic Transfers of Funds66

Correspondent Banking66

Crypto-Currencies.....67

Structural Vulnerabilities68

CHAPTER V: COMPLIANCE REQUIREMENTS -LAW, CIRCULAR, AND PENALTIES.....69

Compliance Requirements under the Laws.....69

Responsibilities of Bank in Prevention of Money Laundering69

Penalties of Money Laundering69

Powers and Responsibilities of BFIU.....72

Responsibilities of Reporting Organizations.....74

Offences Committed by an Entity.....74

Anti-Terrorism Act 2009 (Amendment 2012 & 2013).....75

Penalties of Terrorist Financing75

Offences Relating to Financing for Terrorist Activities.....76

Powers of BFIU77

Duties of Reporting Organizations.....78

Compliance Requirements under Circulars79

Appointment and Training79

Suspicious Transaction Reporting (STR)81

Targeted Financial Sanctions.....81

Automated Screening Mechanism of UNSCRs.....81

Self-Assessment82

Independent Testing Procedure83

ICCD’s Obligations Regarding SAP/ITP84

Obligations Regarding SAP or ITP of AML & CFT Division.....84

“Safe Harbor” Provision for Reporting under MLP Act.....84

CHAPTER VI: AML & CFT COMPLIANCE PROGRAM IN PREMIER BANK.....85

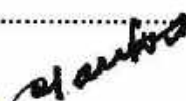
AML & CFT Division85

Requirement for Compliance Program87

Senior Management Commitment88

Roles and Responsibilities of Board of Directors:.....89



Statement of Commitment of CEO or MD includes the followings89

Senior Management90

The Board of Directors.....91

The written AML & CFT Policy91

Customer Acceptance Policy91

Policy for Rejection of Customer92

ML & TF Risk Assessment.....92

CHAPTER VII: COMPLIANCE STRUCTURE & HR INITIATIVES.....93

Central Compliance Committee (CCC):.....93

Formation of CCC.....93

Responsibilities of CCC.....94

AML & CFT Division95

Responsibilities of AML & CFT Division.....97

Authorities of AML & CFT Division.....97

Functions of Chief Anti Money Laundering Compliance Officer (CAMLCO):.....97

Authorities and Responsibilities of CAMLCO.....100

The Chief Anti Money Laundering Compliance Officer (CAMLCO)100

Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)100

Branch Level Organization Structure101

Branch Anti Money Laundering Compliance Officer (BAMLCO)102

Responsibilities of BAMLCO103

Responsibilities of BAMLO107

Internal Control & Compliance Division110

Managing Director & CEO111

Initiatives by Human Resources Division111

CHAPTER VIII: CUSTOMER DUE DILIGENCE.....113

Introduction113

Legal Obligation of CDD114

Know Your Customer (KYC) Policies and Procedures118

Customer Acceptance Policy121

Risk Perception.....123

Acceptance of Customer123

Policy for Rejection of a Customer.....125

Customer Type Wise Account Opening and Operating Procedure:.....127

Document or Strategy for Verification of Address.....133

Transaction Monitoring Process151

CHAPTER IX: TRADE BASED MONEY LAUNDERING153

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

Introduction 153

Definition & Process 153

The International Trade System 154

Trade Based Money Laundering 154

Basic Trade-Based Money Laundering Techniques 155

Red Flag Indicators 157

Preventive Measures to Combat Trade Based Money Laundering 160

Sanction Control 162

Trade Based Money Laundering Controls 163

Policies and Procedures & Training 165

Branches and Subsidiaries Situated/Located in Foreign Jurisdiction 165

CHAPTER X: RECORD KEEPING..... 166

Statutory Requirement 166

Retrieval of Records..... 168

Wire Transfer Transactions 170

Cross Border Wire Transfer 170

CHAPTER XI: TRANSACTION MONITORING & REPORTING 172

Reporting requirements..... 172

Cash Transaction Report (CTR) 172

Suspicious Transaction Report (STR)..... 172

Reasons for Reporting of STR/SAR 174

Identification and Evaluation STR/SAR 174

Identification of STR/SAR..... 174

Recognition of Suspicious Transactions 176

Reporting of STR/SAR 177

Suspicious Activity Reporting Process 177

Transaction Monitoring Mechanism..... 177

Reporting Lines..... 179

Grading of the scores 181

Red Flags or Indicators of STR 182

CHAPTER XII: EDUCATION, TRAINING, & AWARENESS..... 185

Statutory Controls 185

FATF recommendation for Employee Awareness & Training 185

Training..... 186

Training Procedures..... 188

CHAPTER XIII: BANKING RELATIONSHIP 190

Correspondent Banking Relationship 190





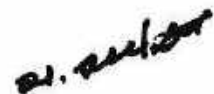
Handwritten signature

Non-Profit Organizations (NPO) and NGO..... 191
KYC requirement for High Net Worth Customer..... 191
Source of Wealth..... 191
Annual Review of Customer Profile..... 191
Model questions to be asked when obtaining source of wealth 192
References 194



CHAPTER I: BACKGROUND**Preamble**

- 1.1 This Policy Guidelines on Anti Money Laundering and Combating Financing of Terrorism of The Premier Bank Limited (PBL) has been developed keeping in consistency with the existing Money Laundering Prevention Act (MLPA) 2012 (Amendment 2015) and Anti-Terrorism Act (ATA) 2009 (amendment 2012 & 2013), Money Laundering and Terrorist Financing Risk Management Guideline, Money Laundering and Terrorist Financing Risk Assessment Guideline, Circulars issued by Bangladesh Financial Intelligence Unit (BFIU) time to time, Guidance Notes, the revised Financial Action Task Force (FATF) Recommendations and the international best practices.
- 1.2 Money laundering is concealing the true source of illegally obtained money. Money launderers often use variety of transactions to launder money and that has become increasingly complex. They are involving numerous financial institutions from many jurisdictions, and increasingly using nonbank financial institutions, as well as nonfinancial businesses and professions. Money laundering methods are diverse and constantly evolving.
- 1.3 Money laundering and Terrorist Financing can have potentially negative consequences for a country's macroeconomic performance, it can impose welfare losses, and may also have negative cross-border externalities. For example, it could compromise bank's soundness with potentially large fiscal liabilities, could lessen the ability to attract foreign investments. Economic damage can arise not only from direct financial system abuse but also from allegations that affect the reputation of a country.
- 1.4 The challenge of terrorist financing is not new. Financial Intelligence Units (FIUs) play an important role in identifying the financial operations of terrorist networks across borders and in detecting their financial backers. Banks need to be more proactive to further detect and prevent terrorist organisations and their backers to move funds and other assets and help law enforcement to trace terrorists and stop them from committing crimes. Recently, another issue has come up and that is proliferation of financing.
- 1.5 The Premier Bank Limited has prepared this handbook giving the title "Policy Guidelines on Anti Money Laundering and Combating Financing of Terrorism". It is expected that each employee of The Premier Bank Limited must exercise the anti-money laundering activities with due care and diligence for the sake of his / her carrier and for the interest of the institution itself.



Policy Guideline Objective

- 1.1 **Broad Objective** - Setting a mechanism to control money laundering and terrorist financing in complying with the Bangladesh's money laundering regulations in order to discharge legal and moral duties and ensure sustainable compliance of the bank.
- 1.2 **Specific Objective**
- 1.2.1 To enable PBL to ensure that only legitimate and bona fide customers are accepted.
 - 1.2.2 To prevent the bank's products, services and deliver channels from being used for money laundering and financing of terrorism
 - 1.2.3 To enable PBL in implementing processes to effectively manage the risks posed by customers trying to misuse facilities.
 - 1.2.4 To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws and regulations, and procedural guidelines.
 - 1.2.5 To take necessary steps to ensure that the relevant staff are adequately trained in AML & CFT procedures.
 - 1.2.6 To prevent financial, reputational and legal damage to the bank by ensuring that the institution has procedures in place to detect and report activities that may be involved with money laundering or terrorist financing or proliferation financing of weapons of mass destruction.
 - 1.2.7 To assist regulators/law enforcement agencies in their efforts to investigate and track money launderers and terrorist financiers.

Policy Statement

The Premier Bank Limited (PBL) pays special attention on Anti-Money Laundering and Combating Financing of Terrorism. This comprehensive Anti Money Laundering and Combating Financing of Terrorism policy guideline has been approved by the Board of Directors and implemented accordingly. These policy and procedures comply with the relevant acts, orders and the Circulars of the appropriate regulators.

This policy statement, a brief description of general principles to which Premier Bank will adhere to, is as follows:

- 1.1 To comply with applicable anti-money laundering and combating the financing of terrorism rules and regulations as established by the Bangladesh Financial Intelligence Unit (BFIU) and respective Financial Intelligence Units in each jurisdiction that is in accordance with the recommendation of the Financial Action Task Force (FATF) on Money Laundering and Terrorist Financing.
- 1.2 Administer and maintain a written policy guideline on anti money laundering and combating financing of terrorism in compliance with relevant acts, rules, guidelines, and circulars, and apply it to all business units.
- 1.3 To obtain all account opening documentation requirements as per laws.



- 1.4 To obtain necessary documents while conducting transaction for Non-Account holders.
- 1.5 To apply the Risk Based Approach & Framework in dealing with the AML & CFT activities as per the set policies and procedures of the Bank.
- 1.6 Ensure that the Policy Guidelines on Anti Money Laundering and Combating Financing of Terrorism of the bank establishes clear responsibilities and accountabilities within PBL and those policies, procedures and controls are maintained which can deter criminals from using PBL for money laundering and financing of terrorist activities.
- 1.7 Constitute CCC and appoint CAMLCO, DeputyCAMLCO, BAMLCO, and SBAMLCO who will have the responsibility for oversight of compliance with relevant legislations, rules and regulations.
- 1.8 Develop a customer acceptance policy entailing the regularity requirements and industry practice and ensure compliance of the same.
- 1.9 Ensure having technologically advanced systems in place for monitoring transactions and reporting as well as submitting various returns.
- 1.10 Cooperate fully with law enforcement and regulatory agencies.
- 1.11 Review policy at regular intervals, at least annually, and update/revise, as necessary, based on any legal/regulatory or business/operational changes, such as additions or amendments to existing AML & CFT related rules and regulations.
- 1.12 Ensure having independent and fair internal control mechanism.
- 1.13 To apply appropriate screening process while on boarding the customers.
- 1.14 PBL will not conduct business or maintain any business relationship with any Shell Bank. In addition to that, PBL will not offer any service to open anonymous accounts.
- 1.15 PBL will comply with the due processes like conducting CDD, EDD, KYC, E-KYC, TP Update, periodic review of high and low risk customers, adverse media news screening etc. for keeping the bank free from any threats that may arise from money laundering or terrorist financing.
- 1.16 To retain all custome related documents for a period specified as per local laws in each jurisdiction.
- 1.17 To report all identified suspicious activities.
- 1.18 To train all staff on AML & CFT and new AML & CFT laws and regulations.
- 1.19 To maintain a system of internal controls to ensure ongoing AML & CFT compliance by a designated person(s) and take appropriate action once suspicious activity is detected, a proper and thorough process for filing Suspicious Transaction Report (STR) is followed as per the requirements of Bangladesh Financial Intelligence Unit (BFIU) and applicable laws.








Scope and Enforcement

- 1.1 This Policy Guideline shall be applicable for all branches, sub-branches, agent banking outlets, departments, divisions, bill collection booths, of PBL.
- 1.2 Copies of the Policy Guideline shall be distributed to all employees of the bank including to those of the agents of the bank so that it can be readily available to all employees, agents and agent-employees.
- 1.3 All employees, contractual employees, agents, agent employees of the bank shall comply with the Policy Guideline and all relevant employees must be thoroughly familiar with and make use of the material contained in the Guideline.
- 1.4 Annual revision or any changes/updates to this Policy Guidelines shall require approval of the Board of Directors.
- 1.5 Changes in any operating procedures, standards and technologies, may be authorized by the MD & CEO and/or CAMLCO.
- 1.6 Senior Management shall be responsible for ensuring the directives implemented and administered in compliance with the approved Policy Guidelines.

Clarifications of the Policy Guidelines

- 1.1 Requests for clarifications to any point of this policy to be made by the CAMLCO or Deputy CAMLCO.
- 1.2 This is basically a revised policy manual combating of the AML-CFT. This policy guideline is adopted to fulfill the requirements laid down by BFIU. In case of any ambiguity developed due to English version of related BFIU regulations, original Bangla text is to be considered. CAMLCO is the custodian of this policy manual and preserves the right to explain and clarify any ambiguity that arises from this policy manual.

What is Money Laundering?

- 1.1 Money laundering can be defined in several ways. However, the fundamental concept of money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Most countries subscribe to the following definition which was adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

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



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

Money Laundering Definition

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

"Money Laundering" means -

- 1.1 Knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes: -
 - 1.1.1 concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
 - 1.1.2 assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
- 1.2 Smuggling money or property earned through legal or illegal means to a foreign country;
- 1.3 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
- 1.4 Concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
- 1.5 Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
- 1.6 Acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
- 1.7 Performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
- 1.8 Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;
- 1.9 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

Handwritten signature

Handwritten signature



Handwritten signature

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."

- 1.10 **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."
- 1.11 **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."
- 1.12 **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".
- 1.13 **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".
- 1.14 **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.

Property Definition

Property has been defined in section 2(bb) of the MLP Act, 2012 as "Property means-

- 1.1 any type of tangible, intangible, movable, immovable property or
- 1.2 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 our outside the country.

Stages of Money Laundering

- 1.1 There is no single method of money laundering. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewellery, art piece) for passing money through a complex international web or legitimate business 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

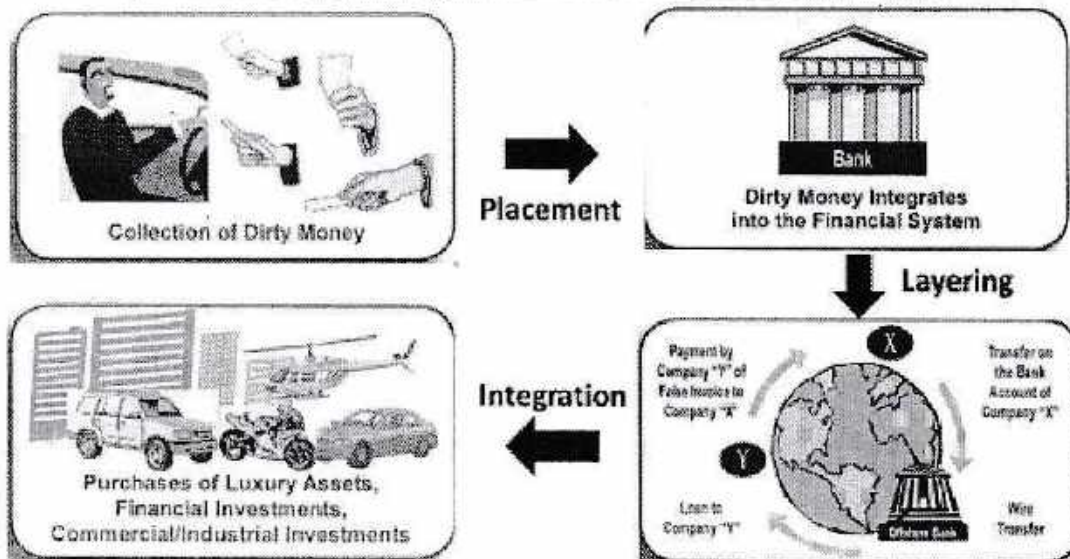
purchases of drugs are almost always made in cash. This has a need to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated.

1.1.1 Traditionally, it has been accepted that the money laundering process comprises three stages:

- a) Placement – The initial stage of money laundering is placement that occurs when the launderer introduces their illegal profits into the financial system. Placement is the first stage of the money laundering process, in which illegal funds are brought first into the financial system directly or indirectly.
- b) Layering – Layering is the second stage of the money laundering process, in which illegal funds or assets are moved, dispersed and disguised to conceal their origin. Funds can be hidden in the financial system through a web of complicated transactions. Layering is performed to make the money as hard to detect as possible. At this layering stage illicit money is blended with legitimate money, or placed in constant motion from one account to another.
- c) Integration – Integration is the third stage of the money laundering process, in which the illegal funds or assets are successfully cleaned and appeared legitimate in the financial system. At this stage the cash re enters into the legitimate economy. This final stage of money laundering successfully puts the so-called 'cleaned' money back into the economy.

1.1.2 The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap.

A Typical Money Laundering Scheme



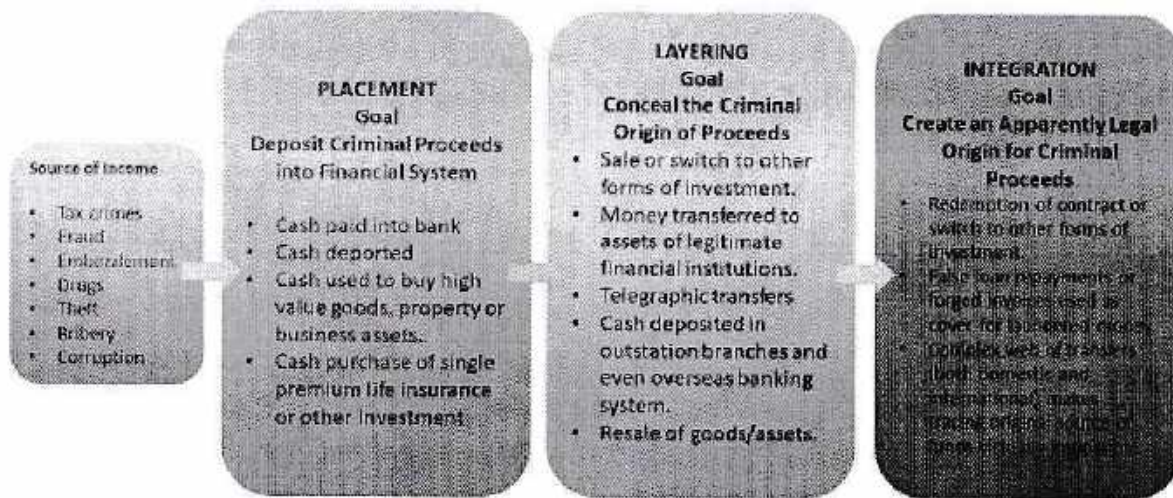
[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

1.1.3 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:



Why Money Laundering is done?

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

- 1.1 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.
- 1.2 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 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.

The Economic and Social Consequences of Money Laundering

One of the greatest risks that threatens the world economy is considered to be the money laundering, which is rapidly spreading around the world. Different countries are facing challenges, especially developing ones which are not qualified to have strong control systems as the developed countries. They are suffering strongly from its negative effects on

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

the economic and social level precisely. Some of the effects of money laundering and terrorist financing are:

1.1 **Increased Crime and Corruption:** Successful money laundering helps enhance the profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it will attract people who commit crime. If money laundering is prevalent, there is likely to be more corruption. Criminals may try to bribe government officials, lawyers and employees of financial or non-financial institutions so that they can continue to run their criminal businesses.

1.2 **Undermining the Legitimate Private Sector:** One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers are known to use front companies, or businesses that appear legitimate and engage in legitimate business, but are in fact controlled by criminals who commingle 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. Thus, front companies have a competitive advantage over legitimate firms that draw capital funds from financial markets. This makes it difficult for legitimate business to compete against front companies, resulting in further negative macroeconomic effects.

Therefore, by using front companies and other investments in legitimate companies, money laundering proceeds can be used to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxation, thus depriving the country of revenue.

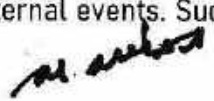
1.3 **Weakening Financial Institutions:** Money laundering and terrorist financing can harm the soundness of a country's financial sector. Financial institutions that rely on the proceeds of crime have additional challenges in adequately managing their assets, liabilities and operations. The adverse consequences of money laundering are generally described as reputational, operational, legal and concentration risks. They are interrelated, and each has financial consequences, such as:

- 1.3.1 Loss of profitable business
- 1.3.2 Liquidity problems through withdrawal of funds
- 1.3.3 Termination of correspondent banking facilities
- 1.3.4 Investigation costs and fines
- 1.3.5 Asset seizures
- 1.3.6 Loan losses
- 1.3.7 Reduced stock value of financial institutions

1.4 Reputational risk is described as the potential that adverse publicity regarding an organizations's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organizations.

1.5 Operational risk is described as the potential for loss resulting from inadequate internal processes, personnel or systems or from external events. Such losses occur



when institutions incur reduced or terminated inter-bank or correspondent banking services or an increased cost for these services. Increased borrowing or funding costs are also a component of operational risk.

Control Lose/Mistakes in Decisions Regarding Economic Policy

Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets, resulting in a loss of control of economic policy by governments.

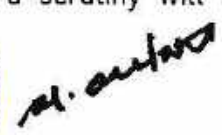
- 1.1 Money laundering can adversely affect currencies and interest rates as launderers reinvest funds where their schemes are less likely to be detected, rather than where rates of return are higher. Volatility in exchange and interest rates due to unanticipated cross-border transfers of funds can also be seen. Money laundering can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.
- 1.2 **Economic Distortion and Instability:** Money launderers are not primarily interested in profit generation from their investments, rather in protecting their proceeds and hiding the illegal origin of the funds. Thus, they "invest" their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, but economic growth can suffer. In some countries, entire industries, such as construction and hotels, have been financed not because of actual demand, but because of the short-term interests of money launderers. When these industries no longer suit the needs of the money launderers, they abandon them, causing a collapse of these sectors and immense damage to economies that could ill-afford these losses.
- 1.3 **Loss of Revenue:** Of the underlying forms of illegal activity, tax evasion is, perhaps, the one with the most obvious macroeconomic impact. 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.

Risk to Privatization Efforts

Money laundering threatens the efforts of many states trying to introduce reforms into their economies through privatization. Criminal organizations can outbid legitimate purchasers for formerly state-owned enterprises. Furthermore, while privatization initiatives are often economically beneficial, they can also serve as a vehicle to launder funds. In the past, criminals have been able to purchase marinas, resorts, casinos and other businesses to hide their illicit proceeds and to further their criminal activities.

- 1.1 **Reputation Risk for the Country:** A reputation as a money laundering or terrorist financing haven could cause negative effects for development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial institutions may decide to limit their transactions with institutions located in money laundering havens because the necessary extra scrutiny will make them more



expensive. Legitimate businesses located in money laundering havens may suffer from reduced access to world markets (or may have to pay more to have access) due to extra scrutiny of ownership and control systems. Once a country's financial reputation is damaged, reviving it is very difficult and requires significant resources to rectify a problem that could have been prevented with proper anti-money laundering controls.

- 1.2 **Social Costs:** Significant social costs and risks are associated with money laundering. Money laundering is integral to maintaining the profitability of crime. It also enables drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures (for example, increased health care costs for treating drug addicts) to combat the serious consequences that result.

Definition of Terrorist Financing

Terrorist financing can be defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF as follows:

- 1.1 If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that are to be used, in full or in part, in order to carry out:
- 1.1.1 An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below¹; or
 - 1.1.2 Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or abstain from doing an act.
- 1.2 For an act to constitute an offense set forth in the preceding paragraph 1.1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1.1, subparagraph (1.1.1) or (1.1.2) Bangladesh has ratified this convention and criminalized terrorism or terrorist activities under section 6(1) of Anti Terrorism Act, 2009 in line with the requirement set out in 9 (nine) conventions and protocols that were annexed in the convention. Section 7(1) of Anti Terrorism Act (ATA), 2009, defines terrorist financing as follows-
- 1.2.1 If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, in full or in part be used
 - a) to carry out terrorist activity;

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

- b) by terrorist person or entity for any purpose, or in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.

1.3 According to Anti Terrorism Act (ATA), 2009 conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act. The penalties for the offences for money laundering are-

1.3.1 In case of a TF offence made by a person, he/she shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or taka 10 (ten) lac, whichever is greater, may be imposed.

1.3.2 In case of TF offence made by an entity, the Government may list the entity in the Schedule or proscribe and list the entity in the Schedule, by notification in the official Gazette and in addition to that, a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed. Moreover, the head of that entity, whether he is designated as Chairman, Managing Director, Chief Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is greater, may be imposed unless he/she is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

The Link between Money Laundering and Terrorist Financing

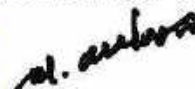
The techniques used to launder money are essentially the same as those used to conceal the sources and uses for terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate source may include donations or gifts of cash or other assets of organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

The difference Between Money Laundering and Terrorist Financing

Money laundering and terrorist financing are often mentioned in the same breath, without much consideration to the critically important differences between the two. Many of the



controls that businesses should implement are meant to serve the dual purposes of combating both money laundering and terrorist financing. Money Laundering and Terrorist Financing are two separate crimes, and, while no one has been able to create a workable financial profile for operational terrorists, there are key distinctions that can help compliance officers to understand the differences and can help distinguish suspicious terrorist financial activity from money laundering. The most basic difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. On the other hand, money laundering always involves the proceeds of illegal activity. The purpose of laundering is to enable the money to be used legally.

Particulars	Money Laundering	Terrorist Financing
Motivation	<ul style="list-style-type: none"> • Profit 	<ul style="list-style-type: none"> • Ideological
Source of Funds	<ul style="list-style-type: none"> • Internally from within criminal organizations 	<ul style="list-style-type: none"> • Internally from self-funding cells (increasingly centered on terrorist activity) • Externally from benefactors and fundraisers
Conduits	<ul style="list-style-type: none"> • Favors from financial system 	<ul style="list-style-type: none"> • Favors cash couriers or informal financial systems such as hawala and currency exchange firms
Detection Focus	<ul style="list-style-type: none"> • Suspicious transactions, such as deposits uncharacteristic of customer's wealth or the expected activity 	<ul style="list-style-type: none"> • Suspicious relationships, such as wire transfers between seemingly unrelated parties.
Transaction Amounts	<ul style="list-style-type: none"> • Large amounts often structured to avoid reporting requirements 	<ul style="list-style-type: none"> • Small amounts usually below reporting thresholds
Financial Activity	<ul style="list-style-type: none"> • Complex web of transactions often involving shell or front companies, bearer shares, and offshore secrecy havens 	<ul style="list-style-type: none"> • No workable financial profile of operational terrorists exists, according to U.S. 9/11 Commission
Money Trail	<ul style="list-style-type: none"> • Circular- money eventually ends up with person who generated it. 	<ul style="list-style-type: none"> • Linear – money generated is used to propagate terrorist group and activities.

Why We Must Combat Money Laundering and Terrorist Financing

- 1.1 *The following section contains excerpts from "The consequences of money laundering and financial crime," by John McDowell and Gary Novis, which appeared in the U.S. State Department publication "Economic Perspectives" in May 2001, and from the World Bank and International Monetary Fund's "Reference Guide to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT)." issued in January 2007.*
- 1.2 The officials – senior policy adviser John McDowell and program analyst Gary Novis of the Bureau of International Narcotics and Law Enforcement Affairs – say the practice distorts business decisions, increases the risk of bank failures, takes control of economic policy away from the government, harms a country's reputation, and exposes its people to drug trafficking, smuggling, and other criminal activity. Given





the technological advantages money launderers now employ, they say, a high level of international cooperation is necessary to keep them in check.

- 1.3 It provides the fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. Crime has become increasingly international in scope, and the financial aspects of crime have become more complex due to rapid advances in technology and the globalization of the financial services industry. Modern financial systems, in addition to facilitating legitimate commerce, also allow criminals to order the transfer of millions of dollars instantly using personal computers and satellite dishes. Because money laundering relies to some extent on existing financial systems and operations. Money is laundered through currency exchange houses, stock brokerage houses, gold dealers, casinos, automobile dealerships, insurance companies, and trading companies. Private banking facilities, offshore banking, shell corporations, free trade zones, wire systems, and trade financing all can mask illegal activities. In doing so, criminals manipulate financial systems. Unchecked, money laundering can erode the integrity of a nation's financial institutions. Due to the high integration of capital markets, money laundering can also adversely affect currencies and interest rates. Ultimately, laundered money flows into global financial systems, where it can undermine national economies and currencies. Money laundering is thus not only a law with subsidized funding, a situation that can result in the crowding out of private sector business by criminal organizations. Clearly, the management principles of these criminal enterprises are not consistent with traditional free market principles of legitimate business, which results in further negative macroeconomic effects.
- 1.4 The negative impacts of money laundering tend to be magnified in developing countries, emerging markets and countries with fragile financial systems because they tend to have less stable financial systems, a lack of banking regulations and effective law enforcement, and, therefore, are more susceptible to disruption from criminal or terrorism influences.
- 1.5 It is generally recognized that effective efforts to combat ML, TF & PF cannot be carried out without the co-operation of financial institutions, and their supervisory authorities. A financial institution tainted by money laundering accusations from regulators, law enforcement agencies, may lose their good market reputation and damage the reputation of the country. Moreover, if it is found that an FI was used for ML & TF activities, and it did not take proper action against that ML & TF as per the laws of the country, the FI will have to face legal risk. Finally, the reputation of an FI can also be heavily affected through its involvement with ML & TF activities.

Vulnerability of the Financial System to Money Laundering

- 1.1 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.
- 1.2 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.

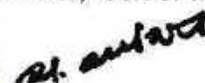


- 1.3 Certain points of vulnerability have been identified in the laundering process, which the money launderer considers difficult to avoid, and where their activities are therefore more susceptible for being recognized. These are:
- 1.3.1 Entry of cash into the financial system
 - 1.3.2 Cross-border flows of cash; and
 - 1.3.3 Transfers within and from the financial system.
- 1.4 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.
- 1.5 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.
- 1.6 Electronic fund transfer system increases the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.
- 1.7 All banks and non-banking financial institutions, as providers of a wide range of money transmission and lending services, are vulnerable to being used in the placement, layering and integration stages. Other loan accounts may be used as a part of this process to create complex layers of transactions.
- 1.8 Although it may not appear obvious that 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.
- 1.9 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.
- 1.10 Payment in cash should merit further investigation, particularly where it cannot be supported by evidence of a cash-based business as source of funds.
- 1.11 Insurance and investment product providers and intermediaries should therefore keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.
- 1.12 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.
- 1.13 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 Financial Institutions Can Combat Money Laundering

- 1.1 The financial risks arising from money laundering are quite high, and there are sound banking practices that reduce these risks. These risks include the potential for individuals or financial institutions to suffer due to fraud, lack of internal controls, or





violations of laws and regulations that result directly from criminal activities. "Know Your Customer" (KYC) rules and due diligence procedures are an essential part of an effective AML / CFT regime. These rules ensure the safe and healthy operations of institutions that are at risk of money laundering.

- 1.2 Policies and procedures are an effective risk management tool. An effective AML / CFT regime also reduces the potential for fraudulent damage to the organization. Proper customer identification procedures and the beneficial owner's determinations provide special due diligence for higher-risk accounts and monitor suspicious activity. Such prudent internal controls are consistent with the safe and sound operation of a financial institution.
- 1.3 The risk-based approach is key to effective AML programs. Organizations can determine customer risk levels with AML screening service while opening a customer account for an accurate risk assessment. With Sanction Scanner solutions, organizations can create an appropriate AML control program that can identify their new customers' risks with comprehensive global enforcement, PEP, and Adverse media data.
- 1.4 In complying with the requirements of the Act and in following different Guidance Notes of BFIU, Banks 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 financial institutions and their staff will recognize attempts at money laundering.

How Premier Bank Can Combat Money Laundering

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

- 1.1 One of the best methods of preventing deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. "Know Your Customer" is the key-policy to know what our customers do, how much their transactions are legitimate, how much not. Thus, a prudent Banker can identify the transactions relating to money launder and can take the necessary measures to prevent it.
- 1.2 Money laundering activities are susceptible to recognition and have therefore to a large extent concentrated on the deposit taking procedures of Banks i. e. the placement stage. Therefore, if a Banker analysis the withdrawal pattern of an Account holder, he/she can understand whether the concerned transactions are money laundering related or not.
- 1.3 Bank and Financial Institutions must keep transaction records that are comprehensive enough to establish an Audit trail. The Premier Bank Limited maintains it. So that analyzing the transaction records, we can ascertain primarily about the people and organizations involved in laundering schemes.



- 1.4 In complying with the requirements of the Act and in following those Guidance Notes, we should at all-time pay particular attention to the fundamental principle of 'good business practice'- know your customer'. If Bankers have sound knowledge of their customers business and pattern of financial transactions and commitments, they will easily understand which transaction is the outcome of money laundering.
- 1.5 Bank's Agent Banking Outlet must keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information of the people and organizations involved in laundering schemes.
- 1.6 AML & CFT Division and Learning and Talent Development Center of the Premier Bank Limited also deal with employees training programs which are designed to make awareness about money laundering techniques and tools that are required to combat ML, TF & PF.
- 1.7 If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, Premier Bank's own initiative shall send the details of the accounts (if any is found with them) of any persons who are engaged in those activities to BFIU immediately.
- 1.8 Premier Bank shall maintain and update the listed individuals and entities in electronic form to run on regular basis a system checking at the website of United Nations for updated list. Premier Bank shall run regular check on the given parameters, including transactional review, to verify whether individuals or entities listed by the respective UNSCR Committee are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.

Compliance Program Development of Premier Bank

Bank has involved all its relevant stakeholders like business units, Credit, Foreign Exhcnage, ICC, Information Technology, ADC, Operations, Human Resources, AMLD and CCC. Bank shall communicate the compliance program immediately after the approval from the board of directors to all of its employees, members of the board of the directors and other relevant stakeholders through email and Premier Bank's dedicated server.

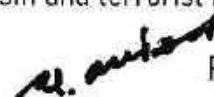
Communication of Compliance Program

The office of CAMLCO shall communicate this compliance program immediately after the approval from the Board/Highest authority to all of employees and other relevant stakeholders. The compliance manual shall also be available at the following location:

Targeted Financial Sanctions

The term Targeted Financial Sanctions (TFS) means both asset freezing and prohibition to prevent funds on other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. This TFS is a smart solution to combat terrorism, terrorist financing and proliferation financing of weapons of mass destruction (WMD) by state actors or non-state actors from the UN Security Council. In contrast with the economic sanction on a jurisdiction, TFS is imposed on only suspected person or entities while innocent person or entities remain safe. TFS related to terrorism and terrorist financing-



- 1.1 FATF recommendation 6 requires '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)'
- 1.2 TFS related to Proliferation-
 - 1.2.1 FATF recommendation 7 requires '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.'
 - 1.2.2 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'.



sp. author

CHAPTER II: INTERNATIONAL INITIATIVES

Introduction

In response to the growing concern about money laundering and terrorist activities, the initiatives taken by international community has acted on many fronts. This part of this Guidelines discusses the various international organizations and their initiatives relating to Anti-Money Laundering (AML) and combating the financing of terrorism (CFT). It further describes the documents and instruments that have been developed for AML & CFT purposes.

The United Nations

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

- 1.1 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.
- 1.2 second, the UN actively operates a program to fight money laundering; the Global Program against Money Laundering, headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).
- 1.3 third, and perhaps most important that 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.

The Vienna Convention

Due to growing concern about the increased international drug trafficking and the tremendous amount 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 193 countries including Bangladesh are members to the convention. The convention has come into force from November 11, 1990.

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:

- 1.1 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;
- 1.2 Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
- 1.3 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
- 1.4 Promote international cooperation.

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

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.

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 took 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.



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 as 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:

- 1.1 deny all forms of support for terrorist groups;
- 1.2 suppress the provision of safe haven or support for terrorist, including freeing funds or assets of persons, organizations or entities involved in terrorist acts;
- 1.3 prohibit active or passive assistance to terrorists; and
- 1.4 cooperate with other countries in criminal investigations and share information about planned terrorist acts.

Security Council Resolution 1540

UNSCR 1540 (2004) imposes binding obligations on all States to adopt legislation to prevent the proliferation of nuclear, chemical and biological weapons, and their means of delivery, and establish appropriate domestic controls over related materials to prevent their illicit trafficking. It also encourages enhanced international cooperation on such efforts. The resolution affirms support for the multilateral treaties whose aim is to eliminate or prevent the proliferation of WMDs and the importance for all States to implement them fully; it reiterates the none of the obligations in resolution 1540 (2004) shall conflict with or alter the rights and obligations of States Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, the Chemical Weapons Convention, or the Biological Weapons Convention or alter the responsibilities of the International Atomic Energy Agency (IAEA), and Organisation for the Prohibition of Chemical Weapons (OPCW).

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.

The Counter-Terrorism Implementation Task Force (CTITF)

The Counter-Terrorism Implementation Task Force (CTITF) was established by the Secretary-General in 2005 and endorsed by the General Assembly through the United Nations Global Counter-Terrorism Strategy, which was adopted by consensus in 2006. The mandate of the CTITF is to enhance coordination and coherence of counter-terrorism efforts of the United Nations system. The Task Force consists of 36 international entities which by virtue of their work have, have a stake in multilateral counter-terrorism efforts. Each entity makes contributions consistent with its own mandate. While the primary responsibility for the implementation of the Global Strategy rests with Member States, CTITF ensures that the UN system is attuned to the needs of Member States, to provide them with the necessary policy support and spread in-depth knowledge of the Strategy, and wherever necessary, expedite delivery of technical assistance.

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.

The Financial Action Task Force

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

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 were 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.

FATF New Standards

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

Summary of new FATF 40 Standards

Group	Topic	Recommendations
I	AML/CFT Policies and Coordination	1-2
	<ul style="list-style-type: none"> ▪ Assessing risks & applying a risk-based Approach ▪ National cooperation and coordination 	
II	Money Laundering and Confiscation	3-4
	<ul style="list-style-type: none"> ▪ Money Laundering offence ▪ Confiscation and provisional measures 	

Group	Topic	Recommendations
III	Terrorist Financing and Financing of Proliferation	5-8
	<ul style="list-style-type: none"> ▪ Terrorist financing offence ▪ Targeted financial sanctions related to terrorism & terrorist financing ▪ Targeted financial sanctions related to proliferation ▪ Non-profit organizations 	
IV	Financial and Non-Financial Institution Preventative Measures	9-23
	<ul style="list-style-type: none"> ▪ Financial institution secrecy laws ▪ Customer due diligence and record keeping ▪ Additional measures for specific customers and activities ▪ Reliance, Controls and Financial Groups ▪ Reporting of suspicious transactions ▪ Designated non-financial Businesses and Professions 	



V	Transparency and Beneficial Ownership of Legal Persons and Arrangements	24-25
	<ul style="list-style-type: none"> ▪ Transparency and beneficial ownership of legal persons ▪ Transparency and beneficial ownership of legal arrangements 	
VI	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	26-35
	<ul style="list-style-type: none"> ▪ Regulation and Supervision ▪ Operational and Law Enforcement ▪ General Requirements ▪ Sanctions 	
VII	International Cooperation	36-40
	<ul style="list-style-type: none"> ▪ International Instruments ▪ Mutual legal assistance ▪ Mutual legal assistance: freezing and confiscation ▪ Extradition ▪ Other forms of international cooperation 	

Some highlights of the 40 Recommendations are:

1.1 AML/CFT Policies and Coordination

1.1.1 Assessing risks and applying a risk-based approach: Countries should start by identifying, assessing and understanding the money laundering and terrorist financing risks they face. Then they should take appropriate measures to mitigate the identified risks. The risk-based approach allows countries to target their limited resources in a targeted manner to their own particular circumstances, thereby increasing the efficiency of the preventive measures. Financial institutions should also use the risk-based approach to identify and mitigate the risks they face.

1.1.2 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

[Handwritten signatures and stamps]





[Handwritten signature]



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 the financing of proliferation of weapons of mass destruction.

1.2 Money Laundering and Confiscation

1.2.1 Money Laundering offence: The Recommendations specify crimes, called "designated categories of offenses," that should serve as money laundering predicates - meaning that trying to conceal them through financial subterfuge would constitute criminal money laundering. Countries should also put in place provisions to allow for the confiscation of the proceeds of crime or otherwise prevent criminals from having access to their criminal proceeds.

1.2.2 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 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 organizations, 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.

1.3 Terrorist Financing and Financing of Proliferation

1.3.1 Terrorist Financing Offence: Countries should criminalize terrorist financing, including the financing of terrorist acts, organizations and individual terrorists, even if no terrorist activity can be directly attributed to the provision of financing. Countries should impose sanctions regimes that will allow them to freeze assets of persons designated by the United Nations Security Council for involvement in terrorism or the proliferation of weapons of mass destruction. Countries should also establish sufficient



controls to mitigate the misuse of non-profit organizations to provide support to terrorist.

- 1.3.2 Targeted financial sanctions related to terrorism and terrorist financing:** Countries should implement targeted financial sanctions regimes to comply with the 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).
- 1.3.3 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.
- 1.3.4 Non-profit Organizations:** Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:
- by terrorist organizations posing as legitimate entities;
 - to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
 - to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

1.4 Financial and Non-Financial Institution Preventive Measures

- 1.4.1 Financial institution secrecy laws:** Countries should ensure that financing institution secrecy laws do not inhibit implementation of the FATF Recommendations.
- 1.4.2 Knowledge and Criminal Liability:** The Recommendations include the concept that knowledge required for the offense of money laundering may be inferred from objective factual circumstances. This is similar to what is known, in some countries, as "willful blindness," or deliberate avoidance of knowledge of the facts. In addition, the Recommendations urge that criminal liability and, where that is not possible, civil or administrative liability, should apply to legal persons as well.
- 1.4.3 Customer Due Diligence (CDD) measures:** Financial institutions should conduct customer due diligence when they:



at subject

- a) Establish business relations
- b) Carry out an occasional transaction or a wire transfer above the specified threshold
- c) Have a suspicion of money laundering or terrorist financing.
- d) Have doubts about the veracity or adequacy of previously obtained customer identification information

1.4.4 Financial institutions must use the risk-based approach:

- a) Identify the customer and verify that customer's identity using reliable, independent source documents, data or information. Establishing accounts in anonymous or obviously fictitious names should be prohibited.
- b) Identify the beneficial owner and take 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 understanding the ownership and control structure of the customer.
- c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
- d) Conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken in the course of that relationship to ensure that the transactions are consistent with the institution's knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds.
- e) Maintain records of the above customer information as well as all transactions to enable them to comply with requests from competent authorities.

Financial institutions should be required to apply each of the CDD measures under (V) to (VIII) 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 10.

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 paragraph (V) to (VIII) 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.

- 1.4.5 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 licenses 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.

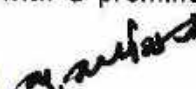
- 1.4.6 Additional Customer Due Diligence on Specific Customers and Activities:** Some customer types and activities pose heightened risks, especially:

- 1.4.7 Politically Exposed Persons (PEPs):** 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 organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to a paragraphs (b), (c) and (d).

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

Definition of PEPs

1.4.8 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:

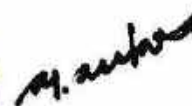
- a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering 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 customer 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.

1.4.9 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.



- 1.4.10 **New Technologies:** Countries and financial institutions should assess the risks associated with developments of new products, business practices, delivery mechanisms and technology. Financial institutions should assess these risks prior to launching new products; they should also take appropriate measures to mitigate the risks identified.
- 1.4.11 **Wire Transfer:** Countries should require financial institutions to obtain and send required and accurate originator, intermediary and beneficiary information with wires. Financial institutions should monitor wires for incomplete information and take appropriate measures. They should also monitor wires for those involving parties designated by the United Nations Security Council and take freezing actions or otherwise prohibit the transactions from occurring.
- 1.4.12 **Reliance, Controls, and Financial Groups**

Reliance on Third Parties -Countries may permit financial institutions to rely on third parties to perform elements (v), (vi), (vii) 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.

- a) The criteria that should be met are as follows:
- b) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (v)-(vii) of the CDD measures set out in Recommendation 10
- c) Financial institutions should take adequate steps to satisfy themselves that copies of identification that data and other relevant documentation relating to the CDD requirements will be made available from third party upon request without delay.
- d) 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
- e) 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.



1.4.13 Internal Controls and Foreign Branches and Subsidiaries: Financial institutions should be required to implement program against money laundering and terrorist financing. Financial groups should be required to implement group-wide program 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 programs against money laundering and terrorist financing.

1.4.14 Higher-risk Countries: Financial institutions should be required to apply Enhanced Due Diligence (EDD) 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 counter measures when called upon to do so by the FATF. Countries should also be able to apply counter measures independently of any call by the FATF to do so. Such counter measures should be effective and proportionate to the risks.

1.4.15 Reporting of Suspicious Transactions

- a) **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 immediately its suspicions to the financial intelligence unit (FIU).
- b) **Tipping-off and Confidentiality:** Financial institutions, their directors, officers and employees should be: (i)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 (ii)Prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

1.4.16 Designated Non-Financial Business and Professions

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.



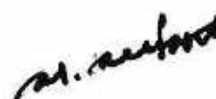



- b. Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.
- c. Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
- d. Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:
 - i. buying and selling of real estate;
 - ii. managing of client money, securities or other assets;
 - iii. management of bank, savings or securities accounts;
 - iv. organization of contributions for the creation, operation or management of companies;
 - v. 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:
 - i. acting as a formation agent of legal persons;
 - ii. 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;
 - iii. providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
 - iv. 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;
 - v. acting as (or arranging for another person to act as) a nominee shareholder for another person.

DNFBPs: Other Measures

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



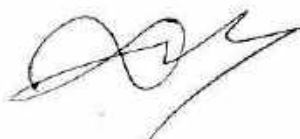



- i. Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (iv) of Recommendation 22. Countries are strongly encouraged to extend reporting requirement to the rest of the professional activities of accountants, including auditing.
- ii. 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.
- iii. 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 (v) of Recommendation 22.

1.5 Transparency and Beneficial Ownership of Legal Persons and Arrangements

1.5.1 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 in time 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 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 DNFBCs undertaking the requirements set out in Recommendations 10 and 22.

1.5.2 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 in time 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 DNFBCs undertaking the requirements set out in Recommendations 10 and 22.





M. Arafat



1.6 Powers and Responsibilities of Competent Authorities, and Other Institutional Measures Regulation and Supervision

1.6.1 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.

1.6.2 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 authorized 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.

1.6.3 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:
 - i. Casinos should be licensed;
 - ii. 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



m. aubos

interest, holding a management function in, or being an operator of, a casino; and

- iii. Competent authorities should ensure that casinos are effectively supervised for compliance with AML & CFT requirements.

Countries should ensure that the other categories of DNFBPs are subject to effective 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. 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.

1.6.4 Operational and Law Enforcement

- a) **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.

- b) **Responsibilities of Law Enforcement and Investigative Authorities** - Countries should ensure that designative 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-



Handwritten signature in black ink.

disciplinary groups specialized in financial or asset investigations. Countries should ensure that, when necessary, cooperative investigations with appropriate component authorities in other countries take place.

- c) **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.

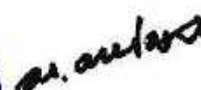
Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, 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.

- 1.6.5 **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.



1.6.6 General Requirements

- a) **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.
- b) **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.

1.6.7 **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.

1.7 International Cooperation

1.7.1 **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 of 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.

1.7.2 **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 prioritization and execution of mutual legal assistance requests. Countries should use a central authority, or another established



m. arif

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 to maintain secrecy or confidentiality.
- 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.
- f) 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.
- g) 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 criminalize the conduct underlying the offence.
- h) 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;

These 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.

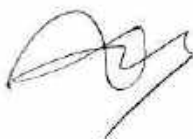
The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards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

- 1.8 **Mutual Legal Assistance: Freezing and Confiscation** -Countries should ensure that they have the authority to take expeditious action in response to, with requests to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended to 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 coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.
- 1.9 **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 or terrorism, terrorist acts or terrorist organizations. In particular, countries should:
- 1.9.1 ensure money laundering and terrorist financing are extraditable offences;
 - 1.9.2 ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritization where appropriate. To monitor progress of requests a case management system should be maintained;
 - 1.9.3 not place unreasonable or unduly restrictive conditions on the execution of requests; and
 - 1.9.4 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 criminalize the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission or 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.

- 1.10 **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 authorize 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 prioritization and timely execution of requests, and for safeguarding the information received.

Monitoring Members Progress

Monitoring the progress of members to comply with the requirements of 40+9 recommendations is facilitated by 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 and 3rd round ME was conducted by APG team in October, 2015.

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).



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 and conducted properly, there should be no duplication or conflict within the FATF family and between the follow up processes.

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 supervisor 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 standard and guideline concern money laundering issues.

Statement of Principles on Money Laundering

In 1988, the Basel Committee issued its Statement of Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement of 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:

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



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.

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.

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 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.

The Egmont Group of Financial Intelligence Units

In 1995, a number of government 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 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.


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:

- 1.5 To assess compliance by APG members with the global standards through a robust mutual evaluation program;
- 1.6 To coordinate bi-lateral and donor-agency technical assistance and training in the Asia Pacific region in order to improve compliance by APG member with the global standards;
- 1.7 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;
- 1.8 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



- 1.9 To contribute to the global policy development of Anti Money Laundering (AML) and Counter Financing on Terrorism (CFT) 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 or terrorism offences.

CHAPTER III: NATIONAL INITIATIVES

National Initiatives

In line with international efforts, Bangladesh has also taken many initiatives to prevent money laundering and combating financing of terrorism and proliferation of weapons of mass destructions considering their severe effects on the country.

Founding Member of APG

Bangladesh is 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. Bangladesh has formally endorsed by the APG Membership out-of-session in September 2014 as the Co-Chair for 2018-2020. Bangladesh hosted the 13th APG Typologies Workshop in 2010 and APG Annual Meeting of 2016.

Legal Framework

Bangladesh is the first country in the South Asia that has enacted Money Laundering Prevention Act (MLPA) in 2002. 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. Money Laundering Prevention Rules, 2013 has been framed for effective implementation of the act. Later on, MLPA-2012 has been amended on 2015 and Money Laundering Prevention Rules, 2019 has been framed for effective implementation of the act.

- 1.1 Bangladesh also enacted Anti-Terrorism Ordinance (ATO) in 2008 to combat terrorism and terrorist financing. Subsequently, ATO, 2008 has repealed by Anti-Terrorism Act (ATA), 2009 with the approval of the parliament. To address the gap identified in the Mutual Evaluation Report (MER) of Bangladesh that is adopted in 2009 by APG, some provisions of ATA 2009 have been amended in 2012 and 2013. Anti-Terrorism Rules, 2013 has also been promulgated to make the roles and responsibilities of related agencies clear specially to provide specific guidance on the implementation procedure of the provisions of the UNSCRs.



m. omdat

1.2 Bangladesh has enacted Mutual Legal Assistance in Criminal Matters Act, 2012 to enhance international cooperation on ML, TF & PF and other related offences. The Government also enacted Mutual Legal Assistance in Criminal Matters Rules, 2013 which mainly emphasize on the process of widest possible range of providing mutual legal assistance in relation to ML, TF & PF and other associated offences.

Central and Regional Taskforce

The Government of Bangladesh has formed a central and 7 regional taskforces (Chittagong, Rajshahi, Bogra, Sylhet, Rangpur, Khulna and Barisal) on 27 January, 2002 to prevent illegal hundi activities, illicit flow of fund & money laundering in Bangladesh. The Deputy Governor of Bangladesh Bank and head of BFIU is the convener of that committee. Both the task force's meeting is held bi-monthly. The meeting minutes of the regional task force are discussed in the central task force meeting. Besides, high profile cases are discussed in the central task force meeting. The central task force set out important decisions that are implemented through banks, financial institutions and Government agencies concerned.

Anti Money Laundering Department

Anti Money Laundering Department (AML) was established in Bangladesh Bank in June 2002, which worked as the FIU of Bangladesh. It was the authority for receiving, analyzing and disseminating Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs).

Bangladesh Financial Intelligence Unit

As per the provision of MLPA, 2012 Bangladesh Financial Intelligence Unit (BFIU) has been established abolishing AMLD as a national central agency to receive, analyze and disseminate STRs/SARs, CTRs and complaints. BFIU has been entrusted with the responsibility of exchanging information related to ML & TF with its foreign counterparts. The main objective of BFIU is to establish an effective system for prevention of AML, CFT & CPF and it has been bestowed with operational independence. BFIU has also achieved the membership of Egmont Group in July, 2013.

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 procured goAML software for online reporting and software based analysis of CTRs and STRs. It also has established MIS to preserve and update all the information and to generate necessary reports using the MIS.

To provide guidance for effective implementation of AML & CFT 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 Ministry of Finance were formed consisting representatives from all concerned Ministries, Agencies and regulatory authorities.



National ML & TF Risk Assessment (NRA)

Bangladesh first conducted National ML & TF Risk Assessment (NRA) in 2011-2012. The methodology used for NRA was developed by ACC, BFIU and CID of Bangladesh Police consulting with Strategic Implementation Plan (SIP) of World Bank. The report was prepared by using the last 10 years' statistics from relevant agencies and identified the vulnerabilities of sectors, limitations of legal framework and weaknesses of the institutions on ML & TF.

Second NRA has been conducted by a 'core committee' comprises of ACC, BFIU and CID of Bangladesh Police and another 'working committee' comprises of 23 members. This report considers the output of institutional, sectoral, geographical risk assessment. It covers all the sectors of the economy, legal and institutional framework. The report identifies some high risk areas for Bangladesh that are corruption, fraud-forgery, drug trafficking, gold smuggling and human trafficking. Banks, non-banks financial institutions, real estate developers and jewelers were identified as most vulnerable sectors for ML, TF & PF. The foreign donation receiving NGO/NPO working in the coastal or border area were identified as vulnerable for TF incidence.

National Strategy for Preventing ML, TF & PF

National Strategy for Preventing Money Laundering and Combating Financing of Terrorism, 2011-2013 was adopted by the NCC in April 2011. Bangladesh has completed all the action items under the 12(twelve) strategies during that time. A high level committee headed by the Head of BFIU and Deputy Governor of Bangladesh Bank has formulated the National Strategy for Preventing Money Laundering and Combating Financing of Terrorism 2015-2017 which has been approved by the National Coordination Committee (NCC) on ML & TF. The strategy identifies the particular action plan for all the Ministries, Division and Agency to develop an effective AML & CFT system in Bangladesh. The strategy consists of following 11 (eleven) strategies against 11 (eleven) strategic objectives:

- 1.1 Updating National ML & TF Risk Assessment Report regularly and introducing Risk Based Approach of monitoring and supervision of all reporting organizations.
- 1.2 Deterring corruption induced money laundering considering corruption as a high risk.
- 1.3 Modernization of Border Control Mechanism and depriving perpetrators from use of proceeds of crime to prevent smuggling of gold and drugs, human trafficking, other transnational organized crimes considering the risk thereon.
- 1.4 Tackling illicit financial flows (IFF) by preventing the creation of proceeds of crime, curbing domestic and cross-border tax evasion and addressing trade based money laundering.
- 1.5 Discouraging illicit fund transfer by increasing pace of stolen assets recovery initiatives and or recovering the evaded tax.
- 1.6 Enhancing the capacity of BFIU in identifying and analyzing emerging ML & TF cases including ML & TF risks arising from the use of new technologies.



- 1.7 Enhancing compliance of all reporting agencies with special focus on new reporting agencies like NGOs/NPOs and DNFBPs.
- 1.8 Expanding investigative capacity and improving the quality of investigation and prosecution of ML & TF cases to deter the criminals.
- 1.9 Establishing identification and tracing out mechanism of TF & PF and fully implementation of targeted financial sanctions related to TF & PF effectively.
- 1.10 Boosting national and international coordination both at policy and operational levels.
- 1.11 Developing a transparent, accountable and inclusive financial system in Bangladesh.

Chief Anti Money Laundering Compliance Officers (CAMLCO) Conference Separate annual conferences for the CAMLCOs of Banks, Financial Institutions, Insurance Companies and Capital Market Intermediaries were arranged by BFIU. It also 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.

Egmont Group Memberships

BFIU has achieved the membership of Egmont group in the Egmont plenary on July, 2013 in Sun City, South Africa. Through Egmont membership, BFIU has achieved access to a wider global platform and this will help to establish relationship with other FIUs of different countries to get benefit by exchanging views, experiences and information via Egmont Secure Web.

Anti Militants and De-Radicalization Committee

The Government of Bangladesh is very much vigilant against terrorism and violent extremism. An inter-ministerial committee headed by Minister of Home is working actively to prevent and redress of terrorism, to fight against terrorist and the terrorist organizations in a more coordinated way. The committee comprised of high officials from different ministries, law enforcement and intelligent agencies. The committee tried to find out more sensitive and sophisticated ways to create awareness among the general people about the negative impact of terrorism.

Memorandum of Understanding (MOU) Between ACC and BFIU

Anti-Corruption Commission (ACC) and the Bangladesh Financial Intelligence Unit (BFIU) has signed a Memorandum of Understanding (MoU) on 4 May, 2014 with a view to increasing the scope of cooperation for dealing with money laundering and other financial crimes. The ACC and the BFIU have jointly undertaken various initiatives to fight against money laundering and other financial crimes.






NGO/NPO Sector Review

Bangladesh first assessed the ML, TF & PF risk associated with the NGO/NPO sector in 2008. As the sector was mainly depending on foreign donation, the report identified strategic deficiencies of supervision and control of the regulator. According to the requirement of FATF Recommendation 8, BFIU has conducted NGO/NPO sector review with the help from NGO Affairs Bureau, Microcredit Regulatory Authority, Department of Social Services and Research Department of Bangladesh Bank. The review report is a very comprehensive one that covers legal & institutional aspects, supervision mechanism, compliance requirements and risk & vulnerabilities relating to ML & TF.

Implementation of TFS

UN Security Council Resolutions related to TF adopted under Chapter VII of the Charter of UN are mandatory for all jurisdictions including Bangladesh. Bangladesh has issued Statutory Regulatory Order (SRO) No. 398/2012 on 29 November 2012, which was amended and strengthened by SRO No. 188/2013 dated 18 June 2013 under the United Nations (Security Council) Act, 1948. Before the issuance of those SROs, BFIU was used to issue circular letters as a medium of instructions for the reporting organization to implement the requirements of UNSCRs on regular basis.

In addition to the SROs the UNSCRs requirements were also incorporated in the ATA, 2009. Section 20(A) of ATA, 2009 provides that the Government of Bangladesh has power of taking measures for the purposes of implementing United Nations Security Council Resolution No. 1267 and its successor resolutions and United Nations Security Council Resolution No. 1373 and United Nations Security Council resolutions related to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

Coordinated Effort on the Implementation of the UNSCR

A national committee is coordinating and monitoring the effective implementation of the United Nations Security Council Resolutions (UNSCR) relating to terrorism, terrorist financing and financing of proliferation of weapons of mass destruction. The committee is headed by the Foreign Secretary and comprises of representatives from Ministry of Home Affairs; Bank and Financial Institutions Division, Ministry of Finance; Legislative and Parliamentary Affairs Division, Ministry of Law, Justice and Parliamentary Affairs and Bangladesh Bank.

Risk Based Approach

Recommendation 1 of Financial Action Task Force (FATF), the international standard setter on AML and CFT requires financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their ML & TF risks. This requirement is reflected in the Money Laundering Prevention Rules (MLPR) 2019. Rule 10 of MLPR 2019 states that (1) As a reporting organization, every financial institution shall periodically prepare a report after considering the nature of its business, customers, products or services, country or geographical location, etc., which will be used for risk management or control of the institution.



(2) According to the risk assessment report, in cases where a high risk of money laundering, terrorism or terrorist financing is identified, the financial institution as the reporting organization shall conduct Enhanced due diligence.

(3) In cases where the financial institution as a reporting entity has been identified as a low risk, simplified customer due diligence shall be conducted, provided that they are consistent with the low risk indicators and in cases of suspicion of money laundering, terrorism or terrorist financing or would not be acceptable in certain high risk situations.

ML and TF Risk Assessment Guidelines

BFIU has issued a guidelines titled 'ML and TF Risk Assessment Guidelines for Banking Sector' in January, 2015 (Circular letter no. 01/2015) for providing the basic ideas of identifying, assessing and mitigating ML & TF risks that banks may encounter in doing their businesses. Banks were instructed to assess their own ML & TF risk considering their customers, products, delivery channels and geographical positions. They were also instructed to assess regulatory risk i.e. risk arises from non-compliance of AML & CFT measures. All the banks have submitted their ML & TF risk assessment reports to BFIU in complying with the instruction.

Memorandum of Understanding (MOU) and Other FIUs

To enhance the cooperation with foreign counterparts, BFIU signed Memorandum of Understanding (MoU) with other FIUs. BFIU has signed 60 MoU (till date) so far to exchange the information related to ML & TF with FIU of other countries.

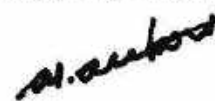


CHAPTER IV: VULNERABILITIES OF FINANCIAL INSTITUTIONS**Vulnerability of the Financial System to Money Laundering**

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.

- 1 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:
 - 1.1. entry of cash into the financial system;
 - 1.2. cross-border flows of cash; and
 - 1.3. Transfers within and from the financial system.
- 2 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.
- 3 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.
- 4 Banks and other Financial Institutions conducting relevant financial business in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. The liquidity of some products may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.
- 5 All banks and non-banking financial institutions, as providers of a wide range of money



transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.

- 6 Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.
- 7 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.
- 8 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.

Vulnerabilities of Products and Services

9 Vulnerabilities of Products and Services

- 9.1. **Lease/Term Loan Finance** - Front companies 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.
- 9.2. **Factoring** - International factoring provides a simple solution of problems faced in case of open account trade regardless of whether the exporter is a small organization or a major corporation. The role of the factor/bank is to collect money owed from abroad by approaching importers in their own country, in their own language and in the locally accepted manner. A factor can also provide exporters with 100% protection against the importer's inability to pay. As international factoring lets exporters safely offer of competitive credit terms to their foreign customers, this international financing mechanism is now popular among both exporters and importers. International factoring means the seller and buyer are in different countries. Over the years, international factoring has taken various forms due to varying needs of the exporters and security to the factors besides price bearing capacity of the former. These are (a) Direct Export Factoring (b) Direct Import Factoring (c) Back to Back Factoring.

9.2.1 Direct Export Factoring: The direct export factoring is mostly used when



handling exports to countries where the corresponding factoring network does not reach. This form of direct export factoring is often provided in combination with outside credit insurance scheme and the traditional services offered by a banking network.

- 9.2.2 The exporter ships the goods to his importer/ debtor.
- 9.2.3 The exporter assigns his invoices to the export factor.
- 9.2.4 The export factor pays the seller the agreed advance.
- 9.2.5 The export factor handles the accounts receivable in accordance with the sale contract between the exporter and the importer.
- 9.2.6 The importer pays on the due date to export factor.
- 9.2.7 The export factor settles the advance with the funds received and forwards the balance to the seller.

a) **Direct import factoring:** Factors in an exporter's country are not sometimes perceived very active in marketing international factoring services. In that case, factors in importers' country offer their services directly to foreign suppliers. The exporter may also establish direct contact with factors in the importing country. The resultant arrangement will be of direct import factoring.

- i. The exporter ships the goods to his importer.
- ii. The exporter assigns his invoices to the import factor, who assumes the credit risk, provided this has been agreed to beforehand
- iii. The import factor handles the accounts receivable in accordance with the sales contract between the exporter and the importer.
- iv. The importer pays the import factor on the due date.
- v. The import factor forwards the payment to the exporter, possibly deducting the agent's commission.

b) **Back-to-Back factoring:** This is a highly specialized form of international factoring. It is used when the supplier sells his goods through his subsidiary to the importers/ debtors in the import factor's country. This is done to avoid large volumes of sales to a few importers/ debtors for whom it is difficult for the import factor to cover the credit risk. In such a case, import factor can sign a domestic factoring agreement with the importer/ debtor. This agreement will facilitate to get debtors' receivables as security for the credit line as it has been asked to establish in favor of export factor.

- i. The parent company ships goods to its subsidiary, which sells and ships the goods to the debtors in the import factor's country.
- ii. The seller assigns his invoices on the subsidiary via export factor to import factor.
- iii. The subsidiary assigns its receivables to the import factor with or without credit risk coverage.
- iv. The export factor pays the parent company the agreed advances.



A. Subis

- v. The subsidiary's debtors pay the import factor.

The import factor distributes the funds according to the instructions from the export factor.

It is clear that 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.

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.

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.

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 into the financial system.

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.

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 launderer 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.

Electronic Transfers of Funds

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as an Automated Clearing House (ACH) computer, an automated teller machine (ATM), electronic terminals, mobile telephones, telephones or magnetic tapes. It can happen within a country or across borders, and trillions of dollars are transferred in millions of transactions each day as it is one of the fastest ways to move money. As such, illicit fund transfers can be easily hidden among the millions of legitimate transfers that occur each day.

Money launderers also use electronic transfers of funds in the second stage of the laundering process, the layering stage. The goal is to move the funds from one account to another, from one bank to another, and from one jurisdiction to another with each layer of transactions –making it more difficult for law enforcement and investigative agencies to trace the origin of the funds. To avoid detection in either stage, the money launderer may take basic precautions such as varying the amounts sent, keeping them relatively small and under reporting thresholds, and, where possible, using reputable organizations.

The processes in place to verify the electronic transfer of funds have been tightened in recent years. Many transaction monitoring software providers have sophisticated algorithms to help detect or trigger alerts that may indicate money laundering or other suspicious activity using electronic transfers of funds.

Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). By establishing multiple correspondent relationships globally, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks obtain a wide range of services through correspondent relationships, including cash management (for example, interest bearing accounts in a variety of currencies), international wire transfers of funds, check clearing, payable-through accounts and foreign exchange services.

The services offered by a correspondent bank to smaller, less well-known banks may be restricted to non-credit, cash management services.

Correspondent banking is vulnerable to money laundering for two main reasons:

- 9.3. By their nature, correspondent banking relationships create a situation in which a financial institution carries out financial transactions on behalf of customers of another institution. This indirect relationship means that the correspondent bank



provides services for individuals or entities for which it has neither verified the identities nor obtained any first-hand knowledge.

- 9.4. The amount of money that flows through correspondent accounts can pose a significant threat to financial institutions, as they process large volumes of transactions for their customers. This makes it more difficult to identify suspect transactions, as the financial institution generally does not have the information of the actual parties conducting the transaction to know whether they are unusual.

Crypto-Currencies

Crypto-currencies have no physical existence, but are best thought of as electronic accounting systems that keep track of people's transactions and hence remaining purchasing power. Crypto currencies are typically decentralized, with no central authority responsible for maintaining the ledger and no central authority responsible for maintaining the code used to implement the ledger system, unlike the ledgers maintained by commercial banks for example. As crypto-currencies are denominated in their own unit of account, they are like foreign currencies relative to traditional fiat currencies, such as dollars and pounds.

There are various Crypto-Currencies are traded in the market for example Binance Coin, Vechain, Tether, EOS, TRON, Bitcoin, Stellar, Ethereum, Ethereum Classic, Tezo5(Pre-Launch), NEO, Monero, Litecoin, Bitcoin Cash, RaiBlocks, IOTA, Dash, Cardano, Ripple, NEM etc.

The mechanics of Bitcoin - the original crypto-currency - to illustrate the fundamental elements of decentralized crypto-currencies. Transactions are implemented as messages that debit or credit account balances in duplicate ledgers. Programming protocols ensure that ledgers are synchronized, and agents are rewarded for updating and quality-assuring the ledgers with transaction data, which accumulate in 'blocks'. Cryptography is used to secure the transaction messages and the integrity of the ledgers containing account balances.

Crypto-currencies expand the mechanisms by which people can transact with each other, strengthening competitive pressures on payment systems providers. But, as noted by many international institutions and central banks, crypto- currencies facilitate a relatively small volume of transactions. These new payments mechanisms are unlikely to completely supplant traditional payments systems. People in different countries typically transact in their own local currency. Since most jurisdictions require tax obligations to be paid in domestic fiat currency, national currencies are likely to remain an important payment mechanism. Crypto-currencies are also unlikely to supplant financial institutions' role in providing credit. Banks and other financial institutions transform assets, manage risk, assess prospective creditors and monitor creditors' progress in meeting their obligations. Credit is largely incompatible with the (pseudo) anonymity that is a common element of crypto-currency design.

Ensuring price stability is likely to remain the pre-eminent monetary policy objective for






central banks, an objective unchanged by the growth of crypto-currencies. As the 'licensed distributors' of fiat currency, central banks should remain able to set interest rates in their domestic fiat currency units. The introduction of crypto-currencies should not fundamentally disrupt central banks' use of interest rates to stabilize the inflation rates of their own fiat currencies.

Crypto-currencies also raise consumer protection, anti-money laundering, and counter-terrorism financing concerns. As niche payment systems, crypto-currencies do not currently pose material financial stability concerns, but risks could increase in materiality if crypto-currencies become more popular and/or more integrated with the activities of traditional financial institutions. Crypto-currencies are extremely volatile, and there are significant risks associated with holding such assets. There is no certainty that specific crypto-currencies, such as Bitcoin, will continue to function and be valued by transactors, and there are non-trivial risks of loss and theft.

Structural Vulnerabilities

10 Structural Vulnerabilities

- 10.1. FIs are yet to develop sufficient capacity to verify the identity and source of funds of their clients.
- 10.2. The human resources are not skilled and trained enough to trace money laundering and terrorist financing activities.
- 10.3. 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.



CHAPTER V: COMPLIANCE REQUIREMENTS -LAW, CIRCULAR, AND PENALTIES

Compliance Requirements under the Laws

In Bangladesh, compliance requirements for FIs, as reporting organization, are based on Money Laundering Prevention Act 2012 (Amendment 2015), Anti-terrorism Act 2009, (Amendment 2012 & 2013) and circulars or instructions issued by BFIU.

Responsibilities of Bank in Prevention of Money Laundering

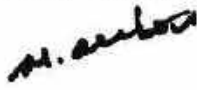
- 1.1 To maintain complete and accurate information with regard to the identity of its customers during the operation of their accounts;
- 1.2 If any account of a customer is closed, to preserve previous records of transactions of such account for at least 5(five) years from the date of such closure;
- 1.3 To provide with the information maintained under clauses (5.1.1) and (5.1.2) to BFIU from time to time, on its demand;
- 1.4 If any doubtful transaction or attempt of such transaction is observed, to report the matter as "suspicious transaction report" to the BFIU immediately on its own accord.

Penalties of Money Laundering

For the purposes of Money Laundering Prevention Act, money laundering shall be deemed to be an offence as per section 4(1) of MLPA, 2012 (Amendment 2015). Penalties for money laundering offence and non-compliance of the provisions of the law are as follows-

Offence	Reference	Penalties
Any person who commits or abets or conspires to commit the offence of money laundering	Section 4(2) (including amendments)	The accused person 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) lac, whichever is greater. However, in case of failure to pay the fine within the time limit fixed by the court, the court may order additional imprisonment in



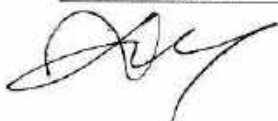



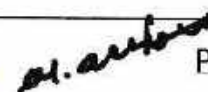
Offence	Reference	Penalties
		consideration of the amount of fine in the unpaid amount.
Committing money laundering	Section 4(3)	In addition to any fine or punishment, the court may pass an order to forfeit the property of the convicted person in favour of the State, which directly or indirectly involved in or related with money laundering or any predicate offence.
Any entity which commits or attempts or aids or conspires to commit an offense under this section	Section 4(4) (including amendments)	<p>Subject to the provisions of section 27, action shall be taken in accordance with the provisions of sub-section (2) and shall be punished with a fine of not less than twice of the value of the property or taka 20 (twenty) lac, whichever is greater and in addition to this, the registration of the said entity shall be liable to be canceled.</p> <p>However, if the entity fails to pay the fine within the time limit prescribed by the court, the court may, in the unrevised sense, order the imprisonment of the entity, chairman or director, whatever the name may be, considering the amount of the penalty.</p>
Divulge any information relating to the investigation or any other related information to any person, organization or news media.	Section 6	Shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or will both.
Obstruction or non-cooperation in investigation, failure to submit report or refusal to provide Information	Section 7	Shall be punished with imprisonment for a term not exceeding 1 (one) year or a fine not exceeding taka 25 (twenty five) thousand or will both.
Providing 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 the Account.	Section 8	Shall be punished with imprisonment for a term not exceeding 3 (three) years or a fine not exceeding taka 50 (fifty) thousand or will both.



M. Ahsan

Non-compliance	Reference	Penalties
Providing 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 the Account.	Section 8	Shall be punished with imprisonment for a term not exceeding 3 (three) years or a fine not exceeding taka 50 (fifty) thousand or will both.
Failure to provide with required information on time	Section 23(3) of MLPA, 2012 (including amendments 2015)	Maximum BDT 5 lac fine at the rate of BDT 10 thousand per day. License may be suspended if fined more than 3 times a year.
Providing wrong or false information by the institution	Section 23(4) of MLPA, 2012 (including amendments 2015)	Maximum BDT 5 lac fine with a minimum of BDT 20 thousand. License may be suspended if fined more than 3 times a year
Failure of reporting institutions to comply with the direction of BFIU.	Section 23(5) of MLPA, 2012 (including amendments 2015)	Maximum BDT 5 lac fine at the rate of BDT 10 thousand per day. License may be suspended if fined more than 3 times a year.
Failure to comply with the freezing order	Section 23(6) of MLPA, 2012 (including amendments 2015)	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.
Individual responsible in the entity for non-compliance	Section 23(8) of MLPA, 2012 (including amendments 2015)	If any reporting organization is imposed fine under sub-sections (3), (4) (5) & (6) BFIU may also impose a fine not less than BDT 10 thousand but not exceeding BDT 5 lac 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.
Failure to comply with the provision of sub-section (1) of section 25 a. Not to maintain complete and correct information of customer (KYC). b. Not to preserve records of transaction at least 5 years after termination of	Sub section (1 & 2) of section 25, MLPA, 2012 (including amendments 2015)	(a) Fine at least BDT 50 thousand but not exceeding BDT 25 lac on the reporting organization. (b) In addition to the above, license of the organization or branches, service centers, booths or agents may be revoked.



Non-compliance	Reference	Penalties
relationship. c. Not to provide with the above Information to BFIU as per their requirement d. Not to submit suspicious transaction report spontaneously to BFIU for unusual/ doubtful transaction.		

Powers and Responsibilities of BFIU

2. Powers and Responsibilities of BFIU in Preventing and Restraining the Offence of Money Laundering –as per section 23 of MLP Act 2012 (Amendment 2015)

For the purposes of this Act Bangladesh Financial Intelligence Unit (BFIU) shall have the following powers and responsibilities:

- 2.1 To analyze or review information related to cash transactions and suspicious transactions received from any reporting organizations and information obtained through any other sources and to collect necessary additional information relating to the purpose of analyzing or reviewing from the reporting organizations and maintain data and information on the same and, and investigating agency or the relevant law enforcement agencies for taking the necessary actions;
- 2.2 Notwithstanding anything contained in any other law, obtain necessary information or report from reporting organizations.
- 2.3 Issue an order to any reporting organization to suspend or freeze transactions of any account for maximum of 7(seven) times by 30 (thirty) days each if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing an offence or money of an account has been or might be used to commit a crime/an offence;
- 2.4 Provided that such order may be extended for additional period of a maximum of 6 (six) months by 30 (thirty) days each, if it appears necessary to find out correct information relating to transactions of the account;
- 2.5 Issue from time to time, any directions necessary for the prevention of money laundering to the reporting organizations;
- 2.6 Conduct on-site inspections on the reporting organizations, if necessary;
- 2.7 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 Financial Intelligence Unit (BFIU);
- 2.8 Carry out any other functions including monitoring activities of the reporting organizations necessary for the purpose of this Act.

3. 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 Financial Intelligence Unit (BFIU) shall provide with such information where no obligation for it is under any existing law or for any other reason.





M. Anwar

4. If any reporting organization fails to provide with the requested information timely under this section pursuant to this Section, Bangladesh Financial Intelligence Unit (BFIU) may impose a fine on such organization which may extend to a maximum of taka 5(five) lakhs 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, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against the organization.
5. If any reporting organization provides false information or statement requested under this Section, BFIU 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 Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches/service centers/booths/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 instruction given by Bangladesh Financial Intelligence Unit (BFIU) under this Act, BFIU 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, BFIU 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.
7. If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Financial Intelligence Unit (BFIU) under clause (c) of sub-section (1), BFIU 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.
8. If any person or entity or reporting organization fails to pay any fine imposed by BFIU under sections 23 and 25 of this Act, Bangladesh Financial Intelligence Unit (BFIU) shall inform Bangladesh Bank and BFIU may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank and in this regard if any amount of the fine remains unrealized Bangladesh Financial Intelligence Unit (BFIU) may, if necessary, make an application before the court for recovery and the court may pass such order which it deems fit (as per section 23(7) of MLP Act- 2012) While conducting enquiry and investigation of the offences under this Act an investigation agency may obtain documents and information related to the customer of a bank or financial institution through an order by the competent court or through Bangladesh Financial Intelligence Unit.
9. If any reporting organization is imposed fine under sub-section (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit (BFIU) may also impose a fine not less than taka 10(ten) thousand but not exceeding taka 5(five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.



Responsibilities of Reporting Organizations**10. Responsibilities of Reporting Organizations in Preventing the Offence of Money Laundering - as per section 25 of MLP Act 2012 (Amendment 2015)**

Reporting Organizations shall have the following duties and responsibilities including other duties and responsibilities specified by rules in the prevention of money laundering:

- 10.1 maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
- 10.2 in case of closed account of any customer, keep previous records of transactions of such account and its transactions for at least 5(five) years from the date of closure;
- 10.3 provide the information maintained under sub-sections (a) and (b) to Bangladesh Financial Intelligence Unit (BFIU) from time to time, as requested;
- 10.4 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 Financial Intelligence Unit (BFIU) proactively and immediately.

11. If any reporting organization violates the provisions contained in sub-section (1), Bangladesh Financial Intelligence Unit (BFIU) or regulatory/controlling authority of the reporting organization:

- 11.1 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
- 11.2 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.
- 11.3 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.

Offences Committed by an Entity**Offences Committed by an Entity as per section 27 of MLP Act 2012 (Amendment 2015)**

- 1.1 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.



Anti-Terrorism Act 2009 (Amendment 2012 & 2013)

1.2 Responsibilities of Bank in Combating Terrorist Financing

- 1.2.1 If any suspicious transaction is identified, bank shall spontaneously report it to BFIU without any delay.
- 1.2.2 The Board of Directors or the CEO of the bank shall approve and issue directions regarding the duties of its officers and shall ascertain whether the directions issued by BFIU under section 15, has been complied with or not.

Penalties of Terrorist Financing

Offence	Reference	Penalties
Committing the offence of financing terrorism (Individual)	Section 7(1) & 7(3) AT Act, 2009 (including amendments)	Min 4 years to 20 years of rigorous imprisonment with fine of two times of the value of the property involved with the offence or BDT 10 lac, whichever is higher.
Committing the offence of financing terrorism (Entity)	Section 7(1) & 7(4) AT Act 2009 (including amendments)	The entity can be banned by the Government with fine of three times of the amount involved with the offence or BDT 50 lac, whichever is greater; and the head of such entity, whether he is designated as Chairman, Managing Director, Chief Executive or any other name, shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than four years and in addition to that a fine may be imposed equal to twice of the value of the property involved with the offence or taka 20 (twenty) lac, whichever is greater, unless he is able to prove that the said offence was committed without his knowledge or he had tried utmost to prevent the commission of the said offence.

Non-compliance	Reference	Penalties
Failure to comply with the directions issued by BB or knowingly provide any wrong information	Section 15(B) of AT Act, 2009 (including amendments)	Maximum fine of BDT 25 lac and may suspend the registration or license
Failure to take necessary	Section 16(1)	Maximum fine BDT 25 lac and

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

Non-compliance	Reference	Penalties
measures, with appropriate caution and responsibility, to prevent and identify terrorist financing and to spontaneously report suspicious transaction if any.	& 16 (3) AT Act, 2009 (including amendments)	suspend the registration or license.
Failure to comply with the directions issued by Bangladesh Bank by any reporting organization under section 15	Section 16(4) of AT Act, 2009 (including amendments)	The chairman of the Board of Directors, or the Chief Executive Officer, by whatever name called, shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding taka 25 (twenty five) lac and Bangladesh Bank may remove the said person from his position as the case may be, shall inform the competent authority about the subject matter to take appropriate action against the person.

Offences Relating to Financing for Terrorist Activities

Offences relating to financing for terrorist activities – {(as per section 7 of ATA 2009 (Amendment 2013)}

1.1 If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, it would, in full or in part, be used-

1.1.1 to carry out terrorist activity;

1.1.2 by a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.

1.2 Conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property mentioned in sub-section (1) was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.

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

1.3.1 If any entity is convicted of any of the offences mentioned in the sub-section (1) –(a) steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of taka 50 (fifty) lac, whichever is greater, may be imposed; and (b) the head of that entity, whether he is designated as Chairman, Managing Director, Chief






Executive or by whatever name called, shall be punished with rigorous imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of taka 20 (twenty) lac, whichever is greater, may be imposed unless he is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.

Powers of BFIU

Powers of BFIU - {as per section 15 of ATA 2009 (Amendment 2013)}

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

- 1.1 to call for a report relating to any suspicious transaction from any reporting agency, analyze or review the same and to collect additional information relating there to for the purpose of analyzing or reviewing the same and maintain record or database of them and, as the case may be, provide with the said information or report to the police or other concerned law enforcement agencies for taking necessary actions;
 - 1.1.1 if there is reasonable ground to suspect that a transaction is connected to terrorist activities, to issue a written order to the respective reporting agency to suspend or freeze transactions of that relevant account for a period not exceeding 30 (thirty) days and, if it appears necessary to reveal correct information relating to transactions of the said account, such suspension or freezing order may be extended for an additional term not exceeding 6 (six) months by 30 (thirty) days at a time;
 - 1.1.2 correct information relating to transactions of the said account, such suspension or freezing order may be extended for an additional term not exceeding 6 (six) months by 30 (thirty) days at a time;
 - 1.1.3 to monitor and supervise the activities of the reporting agencies;
 - 1.1.4 to give directions to the reporting agencies to take preventive steps to prevent financing of terrorist activities and proliferation of weapons of mass destructions (WMD);
 - 1.1.5 to monitor the compliance of the reporting agencies and to carry out on-site inspection of the reporting agencies for carrying out any purpose of this Act; and
 - 1.1.6 to provide training to the officers and employees of the reporting agencies for the purpose of identification of suspicious transactions and prevention of financing of terrorist activities. BFIU, on identification of a reporting agency or any of its customers as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the police or the appropriate law enforcement agency and provide all necessary cooperation to facilitate their inquiries and investigations into the matter.
- 1.2 Bangladesh Bank, on identification of a reporting agency or any of its customers as being involved in a suspicious transaction connected to financing of terrorist activities, shall inform the same to the police or the appropriate law enforcement agency and provide



- all necessary cooperation to facilitate their inquiries and investigations into the matter.
- 1.3 If the offence is committed in another country or the trial of an offence is pending in another shall take steps to seize the accounts of any person or entity upon request of the foreign state or pursuant to any international, regional or bilateral agreement, United Nations conventions ratified by the Government of Bangladesh or respective resolutions adopted by the United Nations Security Council.
- 1.4 The fund seized under sub-section (3) shall be subject to disposal by the concerned court or pursuant to the concerned agreements, conventions or resolutions adopted by the United Nations Security Council.
- 1.5 The power and responsibilities of BFIU under the provisions of this Act shall be exercised by BFIU, and if BFIU requests to provide with any information under this Act, all the governmental, semi-governmental or autonomous bodies, or any other relevant institutions or organizations shall, on such request or, as the case may be, spontaneously provide it with such information.
- 1.6 Bangladesh Financial Intelligence Unit shall, on request or, as the cases may be, spontaneously provide the financial intelligence units of other countries or any other similar foreign counterparts with any information relating to terrorist activities or financing of terrorist activities.
- 1.7 For the interest of investigation relating to financing of terrorist activities, the law enforcement agencies shall have the right to access any document or file of any bank under the following conditions, namely: -
- 1.7.1 According to an order passed by a competent court or special tribunal; or
- 1.7.2 with the approval of the BFIU.
- 1.8 If any reporting agency fails to comply with the directions issued by BFIU under this section or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac, and BFIU may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency.
- 1.9 If any reporting agency fails to pay or does not pay any fine imposed by BFIU according to sub-section (8), BFIU may recover the amount from the reporting agency by debiting its accounts maintained in any other bank or financial institution or BFIU and in case of any unrealized or unpaid amount, BFIU may, if necessary, apply before the concerned court for recovery.

Duties of Reporting Organizations

Duties of Reporting Organizations - {as per section 16 of ATA 2009 (Amendment 2013)}

- 1.1 Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through it which is connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to BFIU without any delay.
- 1.2 The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the



directions issued by BFIU under section 15, which are applicable to the reporting agency, have been complied with or not.

- 1.3 If any reporting agency fails to comply with the provision under sub-section (1), the said reporting agency shall be liable to pay a fine, determined and directed by BFIU, not exceeding taka 25 (twenty five) lac and BFIU may suspend the registration or license with If the Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of any reporting organization fails to comply with the provision of sub-section (2), the Chairman of the Board of Directors, or the Chief Executive Officer, as the case may be, shall be liable to pay a fine, determined and directed by Bangladesh Bank, not exceeding taka 25 (twenty five) lac, and BFIU may remove the said person from his office or, as the case may be, shall inform the competent authority about the subject matter to take appropriate action against the person.
- 1.4 If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank under sub-section (3), or if the Chairman of the Board of Directors, or the Chief Executive Officer, by whatever name called, fails to pay or does not pay any fine imposed by Bangladesh Bank under sub-section (4), Bangladesh Bank may recover the amount from the reporting agency or from the account of the concerned person by debiting any account maintained by him in any bank or financial institution or in Bangladesh Bank, and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

Compliance Requirements under Circulars


In pursuance of BFIU Master Circular no. 26 dated 16.06.2020, and section 16(2) of Anti-Terrorism Act, 2009 (Amendment 2012), Premier Bank has its own policy manual approved by its Board of Directors to prevent money laundering, combating financing of terrorism and financing of proliferation of weapons of mass destruction offences. This policy manual has developed in conformity with international standard and laws and regulations in force in Bangladesh. Premier Bank will review this manual time to time and confirm the meticulous compliance of the circulars, guidelines & instructions issued by Bangladesh Financial Intelligence Unit (BFIU).

Premier Bank has designated one high level Officer as Chief Anti Money Laundering Compliance Officer (CAMLCO) in the Central Compliance Committee (CCC) at Head Office and Branch Anti Money Laundering Compliance Officer (BAMLCO) at branch level.

Appointment and Training

- 1.1 **Employee Screening:** Premier Bank shall maintain proper screening mechanism in their different appointment procedures so that they do not face ML, TF and PF risks arose by any of their staffs. ML & TF risks arose by or through its employees can be minimized if the bank follows fair recruitment procedures. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Premier Bank should follow the following measures (at least two or three from the undermentioned points):

- 1.1.1 reference check
1.1.2 background check






- 1.1.3 screening through or clearance from Law Enforcement Agency
- 1.1.4 personal interviewing
- 1.1.5 personal guarantee
- 1.1.6 personal profile check etc.

- 1.2 Bank will have a KYE Policy, which is to be complied by respective divisions/departments.
- 1.3 Know-your-customer, an essential precaution, must be coupled with know-your-employee. There are a lot of instances that highlight the involvement of employees in fraudulent transactions and in most cases in association with customers. Therefore, brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables.
- 1.4 Policies, procedures, job descriptions, internal controls, approval levels, levels of authority, compliance with personnel laws and regulations, code of conduct/ethics, accountability, dual control, and other deterrents shall be firmly in place.
- 1.5 Before assigning an employee in a particular job or desk, HR shall examine the consistence and capability of the employee and be ensured that the employee shall have necessary training on AML & CFT lessons for the particular job or desk.
- 1.6 The AML & CFT shall be conversant with these and other requirements, and see that they are constantly and uniformly updated and followed up.

1.7 Employee Training: With a view to ensuring the compliance of preventive activities regarding ML, TF and PF AML & CFT Division and Learning & Talent Development Centre (LTDC) of PBL shall jointly undertake the following:

- 1.7.1 Participation of all employees in suitable workshops/training programs to be ensured. AML & CFT training/workshop should include the following:
 - a) An overview of AML & CFT initiatives;
 - b) Relevant provisions of MLPA & ATA and the rules thereof;
 - c) Regulatory requirements as per BFIU circulars, circular letters and guidelines;
 - d) CDD & EDD procedures;
 - e) CTR and STR/SAR reporting procedures;
 - f) Self-assessment and record keeping

- 1.7.2 Besides regular and refreshers' AML & CFT training, bank shall arrange -
 - a) Job specific training or focused training, i.e.
 - i. Trade Based Money Laundering
 - ii. Credit Backed Money Laundering
 - iii. AML & CFT Training for agent banking employees
 - b) UNSCR screening related training for all employees who deal with international transactions, customer relations and account opening;
 - c) Credit fraud and ML related training for all employees who deal with advance and credit of the bank;
 - d) Customer due diligence and ongoing monitoring of transaction related training for the employees who conduct transaction of customers.

1.7.3 Participation of the CAMLCO and DCAMLCO in suitable workshops/training programs with a view to increasing their efficiency and/or attaining

professional certification.

- 1.8 Awareness of Senior Management** - Without proper concern and awareness of the senior management of a bank, it is difficult to have effective implementation of AML & CFT measures in the bank. Therefore, bank shall arrange, at least once a year, an awareness program for all the members of its board of directors and officials engaged with policy making of the bank.
- 1.9 Education and Training for Customer** - Premier Bank has been responding to customer on different matters including KYC, therefore, it informs the prospective customers about the logic behind the information and the documents sought at the time of account opening. The bank distributes leaflets time to time to make customers aware about ML, TF, and PF and has also arranged to stick posters at conspicuous places of the branch. PBL also advertises in public and other media awareness messages on ML, TF and PF.

1.10 Disclaimer

This policy guideline is intended to provide direction to the employees of the Premier Bank Limited, its agents and agent employees regarding their responsibilities pertaining to AML & CFT and in no way a substitute for Money Laundering Prevention Act, 2012 (including amendments 2015), Anti-Terrorism Act, 2009 (including amendments 2012 & 2013) and BFIU guidelines and circulars.

Suspicious Transaction Reporting (STR)

According to the provision of section 25 (1) (d) of MLPA, 2012 (amendment 2015) Premier Bank has to report to Bangladesh Financial Intelligence Unit (BFIU) 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 of Anti-Terrorism Act- 2009, (Amendment 2012 & 2013).

Targeted Financial Sanctions

BFIU has instructed all banks and FIs to take necessary action on UNSCR (targeted financial sanctions). To comply with this direction Bank should consult the UN sanction list regularly and if find any account with it, bank should inform BFIU immediately.

Bank shall ensure cautionary measures are taken while establishing and maintaining correspondent banking relationship with any person or entity from any of the list of countries that are listed as Jurisdictions under Increased Monitoring and High-Risk Jurisdictions subject to a Call for Action of FATF. Re-evaluate remaining correspondent banking relationships/accounts time to time following instruction of BFIU circular 26, dated 16 June 2020.



Automated Screening Mechanism of UNSCRs

Premier Bank has already started automated screening mechanism that prohibit any listed individuals or entities to enter into the banking channel. The bank is operating the system for detecting any listed individuals or entities prior to establish any relationship with them. In particular, bank needs to emphasize on account opening and any kind of foreign exchange transaction through an automated screening mechanism so that any listed individuals or entities could not use the formal financial channel. In short, bank shall ensure that screening has been done before -

- 1.1 any international relationship or transaction;
- 1.2 opening any account or establishing relationship domestically;
- 1.3 any international relationship or transaction;
- 1.4 opening any account or establishing relationship domestically;

Premier Bank uses AML solution namely n screen - (software provided by Nazdak) for screening sanction list while opening any account or establishing relationship with customers. Without screening through AML Solution i.e n screen no account shall be opened. Premier Bank has purchased sanction screening software titled "PBL n-screen" Screening of sanctioned lists of UNSCRs, OFAC, UN, EU and so on for all types of foreign trade related transactions as one of the important issues of our regulatory requirement. Without screening any transaction cannot be done as per regulatory requirement.

1.5 For proper implementation of UN sanction list, all officials of Premier Bank must have enough knowledge about-

- 1.5.1 legal obligation and consequences of non-compliance;
- 1.5.2 sources of information;
- 1.5.3 what to do and how to do with sanction list;
- 1.5.4 transactional review;
- 1.5.5 how to deal with 'false positives';
- 1.5.6 how to deal with actual match;
- 1.5.7 how to deal with 'aggrieved person or entity';
- 1.5.8 how to exercise 'exemption' requirements;
- 1.5.9 Listing & de-listing process etc.

Self-Assessment

Banking system in Bangladesh is mainly based on branch banking. The branches of the banks are in every corner of the country and they have an active role in stimulating the economic growth of the country. It is very difficult for the AML & CFT Division or ICC to scrutinize the activities of every single branch and hence there is a risk regarding the operation of the branches. In order to reduce that risk, BFIU has established a Self-Assessment Reporting system for the branches.

According to the instructions of BFIU, branches of bank need to conduct the Self-Assessment to evaluate them on a half yearly basis. Self-Assessment has to be done through a checklist that is circulated by BFIU circular no. 26, dated June 16, 2020. Before finalizing the evaluation report, there shall have to be a meeting presided over by the Head of Branch with all concerned officials of the branch. In that meeting, there shall be a discussion on the branch evaluation report; if the identified problems according to that report are possible to solve at the branch level, then necessary actions should be taken without any delay to finalize it; and in the final report, recommendations shall have to be



jotted down. In the subsequent quarterly meetings on preventing ML, TF & PF, the progress of the related matters should be discussed.

After the end of every half year, the branch evaluation report along with the measures taken by the branch in this regard and adopted recommendations regarding the issue should be submitted to the Internal Audit Division or ICCD of the Head Office and the AML & CFT Division within the 15th of the next month. Each branch will assess its AML & CFT activities covering the following areas on half yearly basis:

- 1.1 The percentage of officers/employees that received official training on AML & CFT;
- 1.2 Training, experiences and activities of BAMLCO;
- 1.3 The awareness of the officers/employees about the internal AML & CFT policies, procedures and programs, and Bangladesh Bank's instructions and guidelines;
- 1.4 The arrangement of AML & CFT related meeting on regular interval;
- 1.5 The effectiveness of the customer identification & source of fund verification during opening an account;
- 1.6 The risk categorization of customers by the branch;
- 1.7 Regular update of KYC profile as per BFIU circular;
- 1.8 KYC procedure for walk-in-customer, online customer etc.
- 1.9 The monitoring of customers' transactions with the TP after categorizing the customers based on risk or transactions over specific limit;
- 1.10 UN sanction screening mechanism;
- 1.11 Identification of Suspicious Transaction Reports (STRs);
- 1.12 Identification of Structuring;
- 1.13 Cash transaction reporting;
- 1.14 The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- 1.15 The measures taken by the branch during opening of account of PEPs, Influential persons (IPs), High Official of International Organization;
- 1.16 Mobile financial services or wire transfer;
- 1.17 Compliance related to Head Office, BFIU and Bangladesh Bank audit;
- 1.18 Transaction monitoring related to inward and outward remittance;

Independent Testing Procedure

The audit must be independent (i.e. performed by people not involved with the branch's AML & CFT compliance). Audit is a kind of assessment of checking of a planned activity. Independent testing is done through a checklist that is provided by BFIU Circular No. 26 dated June 16, 2020 by Internal Control and Compliance Division of the Premier Bank. The individuals conducting the audit should report directly to the Board of Directors/Senior Management. Audit function shall be done by the ICCD. At the same time external auditors could be appointed (if possible) to review the adequacy of the program. In order to comply the section 6 of Money Laundering Prevention Act 2012 (amendment 2015) i.e. the information collected, received and retrieved by the bank, may be audited/inspected to check whether the tasks of AML & CFT Division are in order. The team comprising by one or more officials of Audit Wing of AML & CFT Division (who are out of the said desk) may be appointed to review the adequacy of the task in order to maintain the confidentiality/ secrecy of the Division as per MLPA.



ICCD's Obligations Regarding SAP/ITP

ICCD's Obligations Regarding Self-Assessment or Independent Testing Procedure

The ICCD shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the AML & CFT Division while executing inspection/audit activities in various branches according to its own regular yearly inspection/audit schedule, the ICCD should examine the AML & CFT activities of the concerned branch using the specified checklists for the Independent Testing Procedure. The ICCD should send a copy of the report with the rating of the branches inspected/audited by the ICCD to the AML & CFT Division of the bank. Besides, ICCD should audit additional 10% (ten percent) of branches as per section 8.2 of BFIU circular no. 26 dated June 16, 2020. The audit team of ICCD should examine the AML & CFT related activities and determine the score of the branch and send a copy of the report to the AML & CFT Division.

Obligations Regarding SAP or ITP of AML & CFT Division

Obligations Regarding Self-Assessment or Independent Testing Procedure of AML & CFT Division

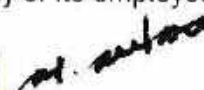
Based on the received branch evaluation reports from the branches and the inspection/audit reports submitted by the ICCD, the AML & CFT Division shall prepare a checklist based evaluation report on the inspected branches in a considered half year time. In that report, beside other topics, the following topics must be included:

- 1.1 Total number of branch and number of Self-Assessment Report received from the branches;
- 1.2 The number of branches inspected/audited by the ICCD at the time of reporting and the status of the branches (branch wise achieved number);
- 1.3 Same kinds of irregularities that have been seen in maximum number of branches according to the received Self-Assessment Report and measures taken by the AML & CFT Division to prevent those irregularities.
- 1.4 The general and special irregularities mentioned in the report submitted by the ICCD and the measures taken by the AML & CFT Division to prevent those irregularities; and
- 1.5 Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated "unsatisfactory" and "marginal" in the received report.

"Safe Harbor" Provision for Reporting under MLP Act.

- 1.1 The Money Laundering Prevention Act encourages reporting organizations to report all suspicious transactions by protecting reporting organizations and their employees from criminal and civil liability when reporting suspicious transactions in good faith to the competent authorities.
- 1.2 Section 28 of the Act provides the "Safe Harbor" for such reporting, which is, although any person may be damaged or there remains possibility to be damaged, any criminal or civil or administrative or any other legal action cannot be administered against the reporting organization, or its Board of Directors, or any of its employees.



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

CHAPTER VI: AML & CFT COMPLIANCE PROGRAM IN PREMIER BANK

1. The financial risks arising from money laundering are quite high, and there are sound banking practices that reduce these risks. There is a way to reduce all negative effects, including having effective AML/CFT applications and programs. A strong AML/CFT institutional framework, which includes broad premise crimes for money laundering, helps fight crime and corruption in general. An effective AML regime in itself is a deterrent to criminal activity. Such a regime makes it difficult for criminals to benefit from their actions. Bank can play a vital role in preventing ML, TF & PF and in this regard their roles and responsibilities are defined in MLP Act 2012 (amendment 2015), ATA, 2009 (amendment 2012 & 2013) and rules and instructions issued under this legal framework by BFIU. To prevent ML, TF & PF and to ensure the soundness, stability, and implementation of required provisions of Acts, Rules and directives of BFIU, Premier Bank has developed and maintained an effective AML, CFT and CPF compliance program. This covers senior management role, internal policies, procedures and controls, compliance structure including appointment of compliance officer, independent audit function and awareness building.

AML & CFT Division

AML & CFT Division performs secretarial duties of the Central Compliance Committee (CCC).

A. Strategic AML & CFT:

- a. Strategy, Policy Development, Design and Implementation
 - i. Review/update/design of annual strategies and programs
 - ii. Development of Standard Operating Procedures (SOP) & Departmental Operating Instructions (DOI)
 - iii. On-going assessment of strategy
- b. Training & Development
 - i. Role based workshops, trainings and e-learning
 - ii. Socialization of AML & CFT compliance culture
- c. Strategic Initiatives
 - i. Futuristic & forward looking AML&CFT strategies
 - ii. Secretariat to the Central Compliance Committee (CCC)



- iii. Strategic Guidance to different departments, projects and digitization/automation initiatives.

B. AML & CFT Systems & Assurance

- a. AML & CFT Systems Implementation
 - i. AML & CFT Compliance Solutions implementation
 - ii. On-going systems review and maintenance
- b. AML & CFT Assurance Framework
 - i. Assurance framework design & maintenance
 - ii. Application of assurance framework through implementation of Key Risk Indicators (KRI) and Control Sample Testing (CSTs)
 - iii. Review and update of assurance framework
- c. AML & CFT Analytics
 - i. Periodic dashboards/Management Information (MI) packs
 - ii. Design and Implementation of AML & CFT Assurance Scorecards.

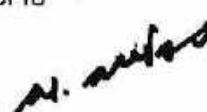
C. AML & CFT Operations

- a. System-based Monitoring
 - i. Automated rule based transaction review
 - ii. Automated rule-based activity review
- b. Manual Monitoring
 - i. Branch/Office reviews
 - ii. Correspondent relationship review
 - iii. PEP/IP, adverse media & other High Risk/EDD reviews
- c. Internal Returns, Reporting & Compliance
 - i. Internal reports and returns to other divisions/departments
 - ii. Internal reports and returns from branches/offices
 - iii. Internal audit and inspection report compliance
- d. FATCA Compliance:
 - i. Collection of data from branches/offices
 - ii. Maintenance, review and submission of FATCA reportable customers to competent authority
 - iii. Periodic certification by FATCA responsible officer (RO) to Internal Revenue Service (IRS)

D. Regulatory Reporting & Compliance

- a. Regulatory Queries:
 - i. Dealing with queries from Bangladesh Financial Intelligence Unit (BFIU) & Anti-Corruption Commission (ACC)
 - ii. Meeting any other ad-hoc requirement from regulatory bodies
- b. Regulatory Reporting
 - i. CTR, STR, SAR reporting to BFIU
 - ii. Half-yearly evaluation reporting to BFIU





Requirement for Compliance Program

Banks are the most dominant player in the financial system and in the economy of Bangladesh. Banks are the most vulnerable institutes for AML/CFT issues. Banks may face following types of risks while doing their business.

- 1.1 Reputational risk is a major threat to banks, 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 a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks 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 management, or held on a fiduciary basis, can pose particular reputational dangers.
- 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 banks' programs, ineffective control procedures and failure to practice due diligence. A public perception that a bank is not able to manage its operational risk effectively which can disrupt or adversely affect the business of the bank.
- 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 a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not practice due diligence in identifying their customers and understanding their business.
- 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 large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks.
- 1.5 Customers frequently have multiple accounts with the same bank, but in offices located in different areas. To effectively manage the reputational, compliance





and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated countrywide basis.

Senior Management Commitment

Senior Management of PBL is highly committed to the development and enforcement of the Anti Money Laundering, Anti Terrorist Financing and Proliferation Financing objectives, which can deter criminals from using their facilities for money laundering or financing of terrorism or proliferation financing, thus ensuring that they comply with their obligations under the laws. Senior Management means the Managing Director & CEO and the Board of Directors of the Bank. In the process of developing compliance program, Premier Bank has given special attention to the range of activities, complexity of operations, and the nature and the degree of ML & TF risk facing by Premier Bank Limited. This program includes:

- 1.1 Senior Management role including their commitment to prevent ML, TF & PF;
- 1.2 Internal policies, procedures and controls- it shall include Bank's AML & CFT policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self-assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;
- 1.3 Compliance structure includes establishment of central compliance committee (CCC), appointment of Chief Anti Money Laundering Compliance Officer (CAMLCO), Branch Anti Money Laundering Compliance Officer (BAMLCO);
- 1.4 Independent audit function-it includes the roles and responsibilities of internal audit on AML, CFT and CPF compliance and external audit function;
- 1.5 Awareness building program includes training, workshop, seminar for bank employees, members of the Board of Directors, owners and above all for the customers on AML, CFT and CPF issues.
- 1.6 introduce proper mechanisms and formulate procedures to effectively implement AML, CFT & CPF policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;
- 1.7 provide periodic reporting on time to the Board on the level of ML, TF & PF risks facing the bank, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML, CFT & CPF which may have an impact on the bank;
- 1.8 Senior Management of Premier Bank shall advice Human Resources Division (HRD) for inclusion of AML, CFT & CPF compliance in their manual so that it helps to adopt HR Policy in order for ensuring the compliance of AML, CFT & CPF measures by the employees of the bank.

Senior Management must convey that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of the Bank's Anti Money Laundering Policy the Managing Director & CEO, on behalf of the Senior Management, is sending a statement to all employees




every year that clearly sets forth the Bank's policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. The statement evidence indicates the strong commitment of the Bank and its senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing.

Roles and Responsibilities of Board of Directors:

- 1.1 Approve AML & CFT compliance program and ensure its implementation;
- 1.2 Issue directives to ensure compliance with the instruction of BFIU issued under section 15 of ATA, 2009;
- 1.3 Take reasonable measures through analyzing self assessment report and independent testing report summary;
- 1.4 Understand ML & TF risk of the Bank, take measures to mitigate those risks;
- 1.5 CEO or/and MD shall issue statement of commitment to prevent ML, TF & PF in the Bank and if necessary shall also observe the overall status of the compliance issue;
- 1.6 Ensure compliance of AML & CFT program;
- 1.7 Establish appropriate mechanisms to ensure the AML, CFT & CPF policies are periodically reviewed and assessed in line with changes and developments in the bank's products and services, technology as well as trends in ML, TF & PF;
- 1.8 Assess the implementation of the approved AML, CFT & CPF policies through regular reporting and updates by the Senior Management and Audit Committee;
- 1.9 Allocate enough human and other logistics to effective implementation of AML & CFT compliance program;
- 1.10 Approve policies regarding AML, CFT & CPF measures within the reporting institution, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;
- 1.11 Ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML, TF & PF;
- 1.12 Establish an effective internal control system for AML, CFT & CPF and maintain adequate oversight of the overall AML, CFT & CPF measures undertaken by the bank;
- 1.13 Establish MIS that is reflective of the nature of the bank's operations, size of business, complexity of business operations and structure, risk profiles of products and services offered as well as geographical coverage.
- 1.14 Maintain accountability and oversight for establishing AML, CFT & CPF policies and minimum standards.



Statement of Commitment of CEO or MD includes the followings

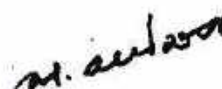
- 1.1 Banks policy or strategy to prevent ML, TF & PF;
- 1.2 Emphasize on effective implementation of Bank's AML & CFT compliance program;
- 1.3 Clear indication of balance between business and compliance, risk and mitigating measures;
- 1.4 Compliance is the responsibility of each employee during their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

Senior Management

Senior Management has accountability to ensure that the Bank's policy, process and procedures towards AML & CFT are appropriately designed and implemented, and are effectively operated to minimize the risk of the Bank being used in connection with ML & TF. **Senior Management** must need to ensure the adequacy of the human and other resources devoted to AML & CFT. Moreover, they need to ensure the autonomy of the designated officials related to AML & CFT. **Senior Management** must take the report from the AML & CFT Division into consideration which will assess the operation and effectiveness of the Bank's systems and controls in relation to manage ML & TF risk and take any necessary action to remedy the deficiencies identified by the report in a timely manner.

- 1.1 **Senior Management** should adopt HR policy for ensuring the compliance of AML & CFT measures by the employees of the Bank.
 - 1.2 **Senior Management** must be responsive of the level of money laundering and terrorist financing risk when the Bank is exposed to and take a view whether the Bank is equipped to mitigate that risk effectively; this implies that decisions on entering or maintaining high-risk business relationships must be escalated to senior management.
 - 1.3 **Senior Management** should approve Anti Money Laundering & Combating of Financing Terrorism Policy
- 2 An AML & CFT Policy must include the following 4 (four) key elements:
- 2.1 High level summary of key controls;
 - 2.2 Objective of the policy (e.g. to protect the reputation of the institution);
 - 2.3 Scope of the policy (A statement confirming that the AML/CFT policy applies to all areas of the business); and
 - 2.4 Waivers and exceptions- procedures for obtaining exemptions from any aspects of the policy should be carefully controlled; and operational controls.



The Board of Directors

The Board of Directors shall develop, administer, and maintain an Anti Money Laundering Policy that ensures and monitors compliance with Anti Money Laundering legislation, including record keeping and reporting requirements. Such a compliance policy shall be written, approved by the Board of Directors, and noted as such in the Board meeting minutes.

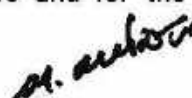
The written AML & CFT Policy

The written AML & CFT Policy at a minimum should establish clear responsibilities and accountabilities within the Bank to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using the Bank for money laundering and the financing of terrorist activities, thus ensuring that we comply with our obligations under the legislation.

- 1.1 In addition, the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and should set forth the consequence of non-compliance with the applicable laws and the institution's policy including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any Bank with money laundering and terrorist financing activity.

Customer Acceptance Policy

A clear Customer Acceptance Policy was developed by the Premier Bank Limited which was approved at the 223rd Board meeting dated November 27, 2019 with immediate effect. This customer acceptance policy integrated with Know Your Customer (KYC) policy. This policy is available at our website (website link). This customer acceptance policies and procedures have to be implemented to identify the types of customer that are likely to pose higher risk of ML and TF pursuant to the Bank's risk assessment. While assessing risk, Branch should consider the factors relevant to the situation, such as customer's background, occupation (including public or high profile position), source of income and wealth, country of origin and residence (when different), product/service used, nature and purpose of accounts, linked accounts, business activities and other customer oriented risk indicators in determining what is the level of overall risk and the appropriate measures to be applied to manage those risks. Such policies and procedures should require due diligence for all customers and commensurate due diligence as the level of risk associated with the customer varies. For the lower risk customer, basic due diligence should be followed as per regulatory circulars and laws and for the higher risk



customer, Branch should take enhanced measures to mitigate and manage those risks. Enhanced due diligence may be essential for an individual planning to maintain higher risk customer.

Policy for Rejection of Customer

- 1.1 No account shall be opened in anonymous or fictitious name
- 1.2 Premier Bank will not establish any kind of correspondence relationship with shell Bank.
- 1.3 No account should be opened or operated in the name of any person or entity listed under UNSCRs or their close alliance on suspicion of involvement in terrorist and terrorist financing activities and prescribed or enlisted by Bangladesh Government.

ML & TF Risk Assessment

Assessing AML & CFT risk is one of the most important steps in creating a good AML & CFT compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk - whether low, medium or high- must be identified and mitigated by the application of controls, such as verification of customer identity, customer due diligence policies, suspicious activity monitoring and sanctions screening. Money Laundering and Terrorist Financing risks vary across jurisdictions, geographical regions, customers, products and services, delivery channels, and over time. Considering the issues, Branch can assess their risk level and the action taken against mitigation of risk. Premier Bank has developed ML & TF risk assessment procedure including the risk register which is mentioned in our ML & TF Risk Management guideline.



CHAPTER VII: COMPLIANCE STRUCTURE & HR INITIATIVES

The Premier Bank Limited constitutes a Central Compliance Committee headed by the the Chief Anti Money Laundering Compliance Officer (CAMLCO).


Central Compliance Committee (CCC):

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

Central Compliance Committee (CCC) will arrange at least 4 (four) meetings on quarterly basis in a year. However, the Committee may call or arrange any number of meetings at any time, if necessary. The committee will review the overall status of the Bank regarding AML & CFT issues. The necessary decisions will be made and instruction will be given by the committee².

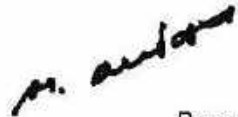
Formation of CCC

CCC (previously named CCU was first formed in July 16, 2015 with officials from concerned departments/divisions of Head Office which has been restructured upon the instructions given in the latest BFIU Master Circular No. 26 and formed a new committee with more members and better involvement of other departments/divisions of the Bank. The new committee consists of sixteen (16) senior members from different departments/divisions like as AML & CFT Division, Retail Banking Division, Credit Risk Management Division, Corporate Banking Division, SME Division, International Division, Finance & Accounts Division, IT Division, HR Division,









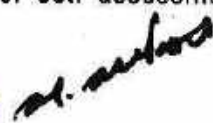
Operations Division, Remittance Division) to ensure proper involvement of those in complying with AML & CFT issues.

Responsibilities of CCC

The committee shall have the following responsibilities:

- 1.1. To develop and implement the Bank's Policy, Procedure and Strategies in Anti Money Laundering (AML), Terrorist Financing (TF) & Proliferation Financing (PF) and review thereon.
 - 1.2. To ensure a satisfactory compliance on Bank's AML & CFT as per the guidelines.
 - 1.3. To supervise AML & CFT Division for the proper implementation of yearly programs on AML & CFT.
 - 1.4. To co-ordinate and monitor Bank's AML & CFT compliance initiatives.
 - 1.5. To co-ordinate the ML & TF risk assessment of the Bank and review thereon.
 - 1.6. To arrange at least 4 meetings in a year; to make necessary decisions and give necessary instructions by reviewing the overall status of the Bank on AML & CFT issues.
 - 1.7. To submit a report to the Managing Director on Half Yearly basis related to AML & CFT issues containing action taken by Bank, implementation progress and recommendations.
 - 1.8. To instruct AML & CFT Division to issue instructions, for the Branches to follow on know Your Customer (KYC), Transaction Monitoring, Internal Compliance etc.
 - 1.9. To nominate one employee from each Branch as BAMLCO to ensure Internal Monitoring and Control System.
 - 1.10. To impart training, workshop, seminar related to AML & CFT for the employees of the Bank.
 - 1.11. Committee may incorporate any member in the committee if they feel the necessity.
 - 1.12. Formal minutes of the meeting shall be maintained to document the AML & CFT activities and decisions.
 - 1.13. Any other issues regarding AML & CFT as & when required by the Bank.
- The Central Compliance Committee is obligated to prepare a checklist based on half-yearly evaluation report based on evaluation reports received from branches and inspection/audit reports from IC&CD that includes:
- 1.14. Total number of branch, sub-branch and number of self-assessment report received from the branches/sub-branches.



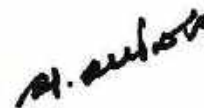



- 1.15. Total number of branch, sub-branch inspected/audited by the Internal Audit Department at the time of reporting and the status of the branches (branch wise achieved number).
- 1.16. Same kinds of irregularities that have been seen in maximum number of branches according to the received self-assessment report and measures taken by the CCC to prevent those irregularities.
- 1.17. The general and special irregularities mentioned in the report submitted by the Internal Audit department and the measures taken by the CCC to prevent those irregularities; and
- 1.18. Measures to improve the ratings by ensuring the compliance activities of the branches.

AML & CFT Division

- 1.1. The Bank shall constitute an AML & CFT Division at its Head Office.
- 1.2. The Bank shall appoint Chief Anti Money Laundering Compliance Officer (CAMLCO).
- 1.3. The Bank shall appoint Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO) & Head of AML & CFT Division.
- 1.4. The Bank shall appoint Branch Anti Money Laundering Compliance Officer (BAMLCO).
- 1.5. Formation of AML & CFT Division
- 1.6. The Bank shall constitute an AML & CFT Division at its Head Office or any suitable place as a permanent set-up with specific organogram like other department or division of a Bank.
- 1.7. AML & CFT Division shall implement and enforce corporate-wide Anti Money Laundering Policies, Procedures and Measures to the Bank and will report directly to the Managing Director & CEO through the CAMLCO.
- 1.8. AML & CFT Division's Organogram Chart of The Premier Bank Limited.
- 1.9. The Premier Bank Ltd. has already been established a separate AML & CFT Division at its Head Office. Organogram of the AML& CFT Division of The Premier Bank is given below:



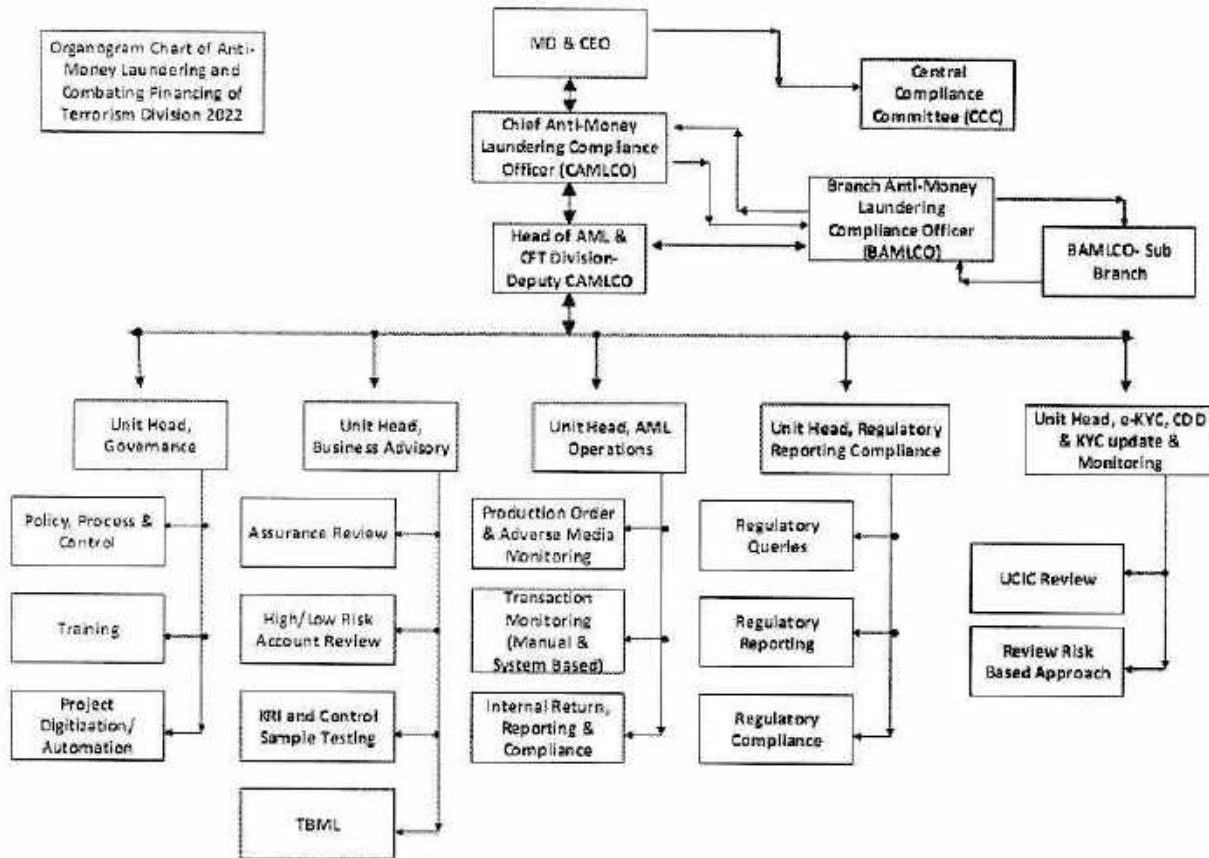


Figure: Organogram Chart

- 1.10. Manpower for Anti-Money Laundering & Combating Financing Terrorism Division
- 1.11. The Bank shall ensure adequate human resources and other logistic support based on the size and nature of the Bank. The division shall be established consisting appropriate number of employees. The Head of the Division will be the Deputy CAMLCO of the Bank. The employee of the AML& CFT Division must have enough knowledge on AML & CFT measures of Bangladesh including MLPA, ATA and rules and instructions issued by BFIU or Bangladesh Bank.
- 1.12. Separation of AML&CFT Division from Internal Control & Compliance Division (IC&CD).
- 1.13. To ensure the independent audit function in the Bank AML& CFT Division should be completely separated from the Internal Control & Compliance Division (IC&CD).
- 1.14. In this regard, ICCD also examines the performance of AML & CFT Division and the Bank's AML & CFT compliance program. To ensure this autonomy there shall not be any member from ICCD to AML& CFT Division and vis-a-vis; but there should be enough co-ordination and co-operation in performing their responsibility and information exchange. There should not be any impediment to transfer employee from ICCD to AML & CFT Division and vis-à-vis but no one

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

should be posted in these 2 (two) departments/units at the same time. Also, no official from ICCD can be a member of the CCC. Both AML & CFT Division and ICCD will independently perform their respective jobs regarding AML & CFT issues.

Responsibilities of AML & CFT Division

- 1.1. AML & CFT Division is the prime mover of the Bank for ensuring the compliance of AML & CFT measures. Main responsibilities of AML & CFT Division are to:
 - 1.1.1. develop Banks policy, procedure and strategies in preventing ML, TF & PF;
 - 1.1.2. coordinate Banks AML & CFT compliance initiatives;
 - 1.1.3. coordinate the ML & TF Risk Assessment of the Bank and review thereon;
 - 1.1.4. present the compliance status with recommendations before the CEO or MD on half yearly basis;
 - 1.1.5. forward STR/SAR and CTR to BFIU in time and in proper manner;
 - 1.1.6. report summary of Self Assessment and Independent Testing Procedure to BFIU in time and in proper manner;
 - 1.1.7. impart training, workshop, seminar related to AML & CFT for the employee of the Bank;
 - 1.1.8. take required measures to submit information, report or documents in time.
 - 1.1.9. ensure the implementation of the AML & CFT program on Yearly Basis.

Authorities of AML & CFT Division

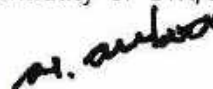
To perform the responsibilities, the AML & CFT Division has the following authorities:

- 1.1. Assign BAMLCO their specific job responsibilities;
- 1.2. Appointment of BAMLCO and assign their specific job responsibilities;
- 1.3. Requisition of human resources and logistic supports for AML & CFT Division;
- 1.4. Make suggestion or administrative sanction for non-compliance by the employees.

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

CAMLCO shall act on his own authority and shall not take mandatorily any permission or consultation from the Managing Director & CEO before submission of STR/SAR & any document or information to BFIU. However, CAMLCO will report directly to the MD & CEO of the Bank. He/she shall maintain the confidentiality of STR/SAR and any



document or information required by laws and instructions by BFIU. He/she must have access to any information of the bank. He/she shall ensure his/her continuing competence. He/she must ensure overall AML, CFT & CPF of the bank and oversee the submission of STR/SAR or any document or information to BFIU in time. He should maintain the day-to-day operations of the Bank's AML, CFT & CPF compliance. CAMLCO will inform to the Managing Director & CEO or to the Board of Directors for proper functioning of CCC/AML & CFT Division. CAMLCO shall review and update ML, TF & PF risk assessment of the bank and take corrective actions of the bank to address the deficiency identified by the BFIU. CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions. The CAMLCO will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering /terrorist financing is put into practice.

Key Responsibilities of the CAMLCO	Frequency
1. Monitor, review, coordinate application and enforcement of the Bank's compliance policies including Anti Money Laundering Policy, Customer Acceptance Policy, Know Your Customer Policy and Anti Terrorism Financing Policy. These will include: an AML Risk Assessment; practices, procedures and controls for account opening; KYC procedures; ongoing account/ transaction monitoring for detecting suspicious transactions/account activity, and a written AML & CFT training plan.	On-going
2. To monitor changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit that may require revisions to the Policies.	On-going
3. Ensure the Bank's Policies are complete and up-to-date; maintain ongoing awareness of new and changing business activities and products and identify potential compliance issues that should be considered by the Bank.	On-going
4. Respond to compliance questions and concerns of the staff and advice branches/ divisions and assist in providing solutions to potential issues involving compliance and money laundering and terrorist financing risk.	As required
5. Actively develop the compliance knowledge of all staff, especially the compliance personnel. Develop and conduct training courses in the Bank to raise the level of awareness of compliance in the Bank.	On-going
6. Develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, Branch/Division Heads and Compliance resources to assist in early identification of compliance issues.	On-going
7. Assist in review of control procedures in the Bank to ensure legal and regulatory compliance and in the development of adequate and sufficient Independent Testing Procedures to prevent and detect compliance lapses.	On-going
8. Monitor Bank's Self Assessment for AML compliance and any corrective action.	Half Yearly





9. Inspect branches and concerned divisions of Head Office regarding anti money laundering and terrorist financing compliance.	As required
10. Manage the STR & SAR Process: a. Review the transactions referred by branch or divisional compliance officers as suspicious. b. Review the Transaction Monitoring reports. c. Ensure that internal Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) - are prepared when appropriate, - are accompanied by documentation of the branch's decision to retain or terminate the account as required under the Policy, - are advised to other branches of the Bank who are known to have a relationship with the customer, - are reported to the Managing Director & CEO and/or the Board of Directors of the Bank when the suspicious activity is judged to represent significant risk to the Bank, including reputation risk. d. Manage the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultation.	On-going
11. Ensure timely Anti Money Laundering and Terrorist Financing reporting and compliance to Bangladesh Financial Intelligence Unit, including CTR, Independent Testing Procedure, Self Assessment Report etc. as per specific schedule.	Monthly, & Half-Yearly
12. Ensure timely compliance of Bangladesh Financial Intelligence Unit (BFIU) Inspection Team, Internal Audit Team and External Audit Team.	As required
13. Ensure that a message from the MD & CEO is issued on an annual basis to all officials of the Bank highlighting the commitment of senior management of the Bank to the development and enforcement of the Anti Money Laundering objectives as per the Policy.	Annually
14. Maintain communication/liaison with the delegates of foreign Banks, local Banks, Bangladesh Bank and various law enforcement agencies.	On-going
15. Collect and review KYC profiles of Correspondents through International Division at Head Office.	On-going
16. Prepare/Complete KYC Questionnaires of PBL for correspondents.	As required
17. Arrange AML training programs for the officials of different scheduled Banks of different districts as and when advised by Bangladesh Financial Intelligence Unit.	As required
18. Perform Bank Account Enquiry function as requested by Bangladesh Financial Intelligence Unit (BFIU) on different persons/companies.	As required
19. Perform Bank Account Freeze function as requested by Bangladesh Financial Intelligence Unit (BFIU) on different persons/companies.	As required



Authorities and Responsibilities of CAMLCO

Authorities-	Responsibilities-
CAMLCO shall act on his own authority;	CAMLCO must ensure overall AML, CFT & CPF compliance of the bank;
He/she shall not take mandatorily any permission or consultation from/with the President & Managing Director before submission of STR/SAR and any document or information to BFIU;	Oversee the submission of STR/SAR or any document or information to BFIU in time;
He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;	Maintain day-to-day operation of the bank's AML, CFT & CPF compliance
He/she must have access to any information of the bank;	CAMLCO will inform to President & Managing Director or Board of Director for proper functioning of CCC/AML & CFT Division ;
He/she shall ensure his/her continuing competence.	CAMLCO shall review and update ML, TF & PF risk assessment of the bank;
	Ensure corrective actions taken by the bank to address the deficiency identified by the BFIU or BB.

The Chief Anti Money Laundering Compliance Officer (CAMLCO)

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

Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO)

- 1.1. The Bank shall form an AML/CFT Division with adequate number of officials considering number of the branches, size and area of the business, number of the customers and organizational risk to perform secretarial duty of the Central Compliance Committee and ML/TF prevention related activities. Deputy Chief Anti Money Laundering Officer (DCAMLCO) will perform the duty of head of the division. Executive below Deputy General Manager (DGM) or Senior Vice President (SVP) will not be employed as D-CAMLCO³.







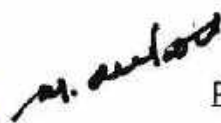
m. aub...

12. CAMLCO may choose to delegate duties or rely on the Deputy CAMLCO in absence of CAMLCO for their practical performance whilst remaining responsible and accountable for the operation of the designated functions.
13. The Deputy CAMLCO shall be the Head of AML & CFT Division and will report directly to the CAMLCO.

Branch Level Organization Structure

11. For the implementation of all existing acts, rules, BFIU's instructions and Bank's own policies on Anti Money Laundering and Terrorist Financing, CCC shall nominate an experienced Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch and a Sub-Branch Anti Money Laundering Compliance Officer (SBAMLCO) in every sub-branch.
12. Branch Manager, Branch Operations Manager (the second man) of the branch or a high official experienced in General Banking/Credit/Foreign Trade Banking shall be nominated as the BAMLCO. The BAMLCO has to have detailed knowledge in the existing acts, rules and regulations, BFIU's instructions and Bank's own policies on preventing Money Laundering and Terrorist Financing. Clear job descriptions and responsibilities of BAMLCO shall be mentioned in the appointment letter.
13. Appointment of Branch Anti Money Laundering Compliance Officer (BAMLCO) and Branch Anti Money Laundering Officer (BAMLCO) for sub-branch.
14. The Branch Manager/ Branch Operations Manager/GB Incharge/ Credit Incharge/any experienced official of every branch shall be designated as the Branch Anti Money Laundering Compliance Officer (BAMLCO). BAMLCO should have a clear understanding about MLP Act, Rules & Regulations; BFIU Instructions and Bank Policy regarding AML & CFT issues. The BAMLCO shall implement and enforce Anti Money Laundering Policies, Procedures and Measures within the branch and shall report directly to Chief Anti Money Laundering Compliance Officer (CAMLCO) at Head Office regarding all AML & CFT matters. Branch Manager shall have overall supervision ensuring that the AML & CFT program is effective within the branch. All other officials of the branch shall also assist BAMLCO to this effect. All staff engaged in each branch at all levels must be made aware of the identity of the respective BAMLCO of the branch. BAMLCO/in-charge of Sub-Branch with the assistance of rest of the employees of the Sub-branch shall implement and enforce Anti Money Laundering Policies, Procedures and Measures within the sub-branch and shall report directly to the BAMLCO of its respective mother branch.
15. **Branch Anti Money Laundering Compliance Committee (BAMLCC):** Every branch shall create a Branch Anti Money Laundering Compliance Committee (BAMLCC) consisting at least with the following members:
 - 1.5.1. Branch Manager/Head of Branch



- 1.5.2. Branch Operations Manager
- 1.5.3. General Banking In charge
- 1.5.4. Credit In charge
- 1.5.5. Foreign Exchange In charge
- 1.5.6. Cash In Charge (Teller)
- 1.5.7. In-charge of Sub Branch

1.6. **Branch Manager:**

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

Branch Anti Money Laundering Compliance Officer (BAMLCO)

Under the obligation of BFIU Circular No.26 dated June 16, 2020 "for the implementation of all existing acts, rules, BFIU's instructions and bank's own policies for Anti ML TF & PF, bank shall nominate Head of Branch or Manager Operations of the Branch or even Experienced Bank Official as Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch." BAMLCO has to have sufficient knowledge in the existing acts, rules and regulations, BFIU's instructions (circular, circular letters etc.) and our own policies on Anti Money Laundering, Terrorist Financing and Proliferation Financing.



Responsibilities of BAMLCO

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

1.7. BAMLCO will perform the following responsibilities:**1.7.1. Knowledge on AML, CFT & CPF issues:**

- a) Be familiar with laws, circulars (both BFIU and AML & CFT Division), policies, guidelines, national initiatives regarding AML, CFT & CPF issues to all members of the branch.
- b) BAMLCO must inform/update to all the members of the branch regarding laws, circulars (both BFIU and AML & CFT Division), Policies, guidelines, national & international initiatives on AML, CFT & CPF matters and ensure its meticulous compliance.

1.7.2. Make sure all the on boarding customer and transaction have been screening by the system and report to competent authority, if any.**1.8. Implementation of Branch Compliance Program:**

BAMLCO will implement all instructions of AML & CFT Division/CCC regarding AML & CFT issues time to time. He/she will keep/preserve all records/documents on AML/CFT Compliance issues in relevant files with the branches as per the instruction circular no. 03/2021, dated 13 December 2021.

1.9. Sanction Screening:

- 1.9.1. Ensure sanction list screening like UN Sanction list, OFAC, and EU list of organization banned by Bangladesh Government before opening of account and while making any transaction.



1.9.2. Ensure sanction list screening like the list of countries that are listed as Jurisdictions under increased monitoring and high-risk jurisdictions subject to a call for action of FATF in order to take cautionary measures while establishing and maintaining business relationship with any person or entity from any of those countries.

1.10. Customer Due Diligence:

- 1.10.1. Identify and verify the identity of the customer information and documents obtained from the reliable source.
- 1.10.2. Ensure the KYC of customer is done appropriately.
- 1.10.3. Ensure proper implementation of e-KYC.
- 1.10.4. Ensure that KYC is updated for high and low risk customers periodically and at the time of TP breach (if required).
- 1.10.5. Ensure due diligence while establishing relationship with the new customer and also while conducting financial transaction with the existing customer.
- 1.10.6. Ensure due diligence when there is a suspicion of ML, TF & PF.
- 1.10.7. Ensure due diligence of walk-in customer, online customers and depositors or withdrawer other than account holder.
- 1.10.8. Identify the beneficial owner of the account and conduct due diligence of the beneficial owners.
- 1.10.9. Keep information of 'dormant accounts' and take proper measures so that any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction.

1.11. Enhance Due Diligence (EDD):

- 1.11.1. Take approval from the CAMLCO before opening an account of PEP, Influential Person and Senior Official of International Organization and their family members as well as their close associates as per BIFU Circular no. 26 dated June 16, 2020.
- 1.11.2. Ensure doing EDD of PEPs, Influential Persons and Senior Officials of International Organization and their family members as well as close associates.
- 1.11.3. Comply Enhance Due Diligence (EDD) for the high risk customer and obtain additional information/documents.
- 1.11.4. Ensure EDD while establishing and maintaining business relationship and conducting financial transaction with a person or entity of the countries and territories that do not meet international (FATF) standard in combating money laundering.



m. aubon

1.12. Transaction Monitoring:

- 1.12.1. Introduce self-auditing, self-assessment and independent testing procedure in the branch and report to ICCD & AML & CFT Division in a timely manner.
- 1.12.2. Ensure regular transaction monitoring to find out any unusual transaction. Records of all transaction monitoring should be kept in the file.
- 1.12.3. Review cash transaction to find out any structuring;
- 1.12.4. Ensure monitoring of account transaction as per instruction of BFIU as well as AML & CFT Division.

1.13. Risk Grading of Customer:

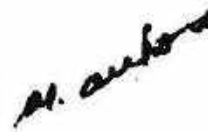
- 1.13.1. Ensure proper risk grading of any customer in comparison with his/her occupation, source of fund, transaction profile (TP) and geographical location of the customer.
- 1.13.2. Maintain a shadow file of international and local PEPs, high-risk customer, high officials of any international organization. All information about these customers should be kept in that file.

1.14. Arrangement of Quarterly Meeting:

- 1.14.1. BAMLCO shall arrange quarterly meeting to discuss issues as per BFIU circular no. 26, dated 16 June 2020 and confirms all employees of the branch are present in the meeting.
- 1.14.2. BAMLCO shall take effective measures on the following matters after reviewing all accounts in order to comply the existing rules, and acts to prevent ML, TF and PF: a) KYC, b) Transaction Monitoring, c) Identification of STR/SAR and reporting, d) Record Keeping, e) Training, f) Materialization of UN Sanction list and Local Sanction List, g) activities regarding self-assessment procedure.

1.15. Report Submission on AML & CFT Program:

- 1.15.1. Review Monthly Cash Transaction Report (CTF), Quarterly (Meeting Minutes), Half-yearly (Self-Assessment Procedures) Reports and send those to AML & CFT Division within the stipulated time without delay. Conduct meeting before finalization of Self-Assessment report.
- 1.15.2. Review information and documents before submitting those reports to AML & CFT for onward submission to BFIU.



1.16. STR/SAR Identification and Reporting:

- 1.16.1. Report STR/SAR by monitoring and analyzing transaction;
- 1.16.2. Review the CTR of each month and find out STR/SAR and send it to AML & CFT Division;
- 1.16.3. Ensure that all employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- 1.16.4. Analyze the Cash Transactions immediate below the CTR threshold limit to identify structuring.
- 1.16.5. Monitor customer unusual behavior and unusual transaction pattern.
- 1.16.6. Considering all the information of the account holder, investigate the purpose of transaction and source of fund with relevant documents, if found any suspicious transactions then report to AML & CFT Division.

1.17. Record Keeping:

- 1.17.1. Keep records of customer's identification and transactions at least (05) five years after the termination of relationships with the customers.
- 1.17.2. Ensure that the branch is maintaining AML, CFT & CPF files properly and record keeping is done as per the requirements.
- 1.17.3. Ensure confidentiality of the records preserved.

1.18. Training:

- 1.18.1. Send officials for training and make sure that all employees have training on AML & CFT.
- 1.18.2. Ensure refresher training every 02 (two) years of all employees of the branch.
- 1.18.3. Keep records of training of all employees of the branch.

1.19. Other Responsibilities:

- 1.19.1. Ensure any freezing order or stop payment order are implemented properly and without delay.
- 1.19.2. All required information and document are submitted properly to CCC/AML & CFT Division.
- 1.19.3. Follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;



- 1.19.4. Create awareness regarding AML, CFT & CPF among the customer of the branch.
- 1.19.5. Ensure that corrective actions have been taken by the branch to address the deficiency identified by the BFIU, or BB, ICCD, and AML & CFT Division;
- 1.19.6. Monitor the staff of the branch to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering and Terrorist Financing.
- 1.19.7. Any other responsibility assigned by the CCC/ AML & CFT Division.

Responsibilities of BAMLO

Premier Bank has already opened 37 (Thirthy Seven) Sub-branches where the sub-branch head will be considered as Branch Anti Money Laundering Officer (BAMLO) under the BAMLCO of its respective mother branch.

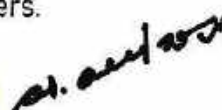
1.20. Sanction Screening:

- 1.20.1. Ensure sanction list screening like UN Sanction list, OFAC, and EU list of organization banned by Bangladesh Government before opening of account and while making any transaction.
- 1.20.2. Ensure sanction list screening like the list of countries that are listed as Jurisdictions under increased monitoring and high-risk jurisdictions subject to a call for action of FATF in order to take cautionary measures while establishing and maintaining business relationship with any person or entity from any of those countries.

1.21. Customer Due Diligence:

- 1.21.1. Identify and verify the identity of the customer information and documents obtained from the reliable source.
- 1.21.2. Ensure the KYC of customer is done appropriately.
- 1.21.3. Ensure proper implementation of e-KYC.
- 1.21.4. Ensure that KYC is updated for high and low risk customers periodically and at the time of TP breach (if required).
- 1.21.5. Ensure due diligence while establishing relationship with the new customer and also while conducting financial transaction with the existing customer.
- 1.21.6. Ensure due diligence when there is a suspicion of ML, TF & PF.
- 1.21.7. Ensure due diligence of walk-in customer, online customers and depositors or withdrawer other than account holder.
- 1.21.8. Identify the beneficial owner of the account and conduct due diligence of the beneficial owners.



1.21.9. Keep information of 'dormant accounts' and take proper measures so tht any withdrawal from these accounts shall not be allowed without compliance of BFIU's instruction.

1.22. Enhance Due Diligence (EDD):

1.22.1. Take approval from the CAMLCO before opening an account of PEP, Influential Person and Senior Official of International Organization and their family members as well as their close associates as per BIFU Circular no. 26 dated June 16, 2020.

1.22.2. Ensure doing EDD of PEPs, Influential Persons and Senior Officials of International Organization and their family members as well as close associates.

1.22.3. Comply Enhance Due Diligence (EDD) for the high risk customer and obtain additional information/documents.

1.22.4. Ensure EDD while establishing and maintaining business relationship and conducting financial transaction with a person or entity of the countries and territories that do not meet international (FATF) standard in combating money laundering.

1.23. Transaction Monitoring:

1.23.1. Introduce self-auditing, self-assessment and independent testing procedure in the branch and report to ICCD & AML & CFT Division in a timely manner.

1.23.2. Ensure regular transaction monitoring to find out any unusual transaction. Records of all transaction monitoring should be kept in the file.

1.23.3. Review cash transaction to find out any structuring;

1.23.4. Ensure monitoring of account transaction as per instruction of BFIU as well as AML & CFT Division.

1.24. Risk Grading of Customer:

1.24.1. Ensure proper risk grading of any customer in comparison with his/her occupation, source of fund, transaction profile (TP) and geographical location of the customer.

1.24.2. Maintain a shadow file of international and local PEPs, high-risk customer, high officials of any international organization. All information about these customers should be kept in that file.



1.25. Arrangement of Quarterly Meeting:

- 1.25.1. BAMLCO shall arrange quarterly meeting to discuss issues as per BFIU circular no. 26, dated 16 June 2020 and confirms all employees of the branch are present in the meeting.
- 1.25.2. BAMLCO shall take effective measures on the following matters after reviewing all accounts in order to comply the existing rules, and acts to prevent ML, TF and PF: a) KYC, b) Transaction Monitoring, c) Identification of STR/SAR and reporting, d) Record Keeping, and e) Training, f) Materialization of UN Sanction list and Local Sanction List, g) activities regarding self-assessment procedure.

1.26. STR/SAR Identification and Reporting:

- 1.26.1. Report STR/SAR by monitoring and analyzing transaction;
- 1.26.2. Review the CTR of each month and find out STR/SAR and send it to AML & CFT Division;
- 1.26.3. Ensure that all employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
- 1.26.4. Analyze the Cash Transactions immediate below the CTR threshold limit to identify structuring.
- 1.26.5. Monitor customer unusual behavior and unusual transaction pattern.
- 1.26.6. Considering all the information of the account holder, investigate the purpose of transaction and source of fund with relevant documents, if found any suspicious transactions then report to AML & CFT Division.

1.27. Other Responsibilities:

- 1.27.1. Ensure any freezing order or stop payment order are implemented properly and without delay.
- 1.27.2. All required information and document are submitted properly to CCC/AML & CFT Division.
- 1.27.3. Follow the media report on terrorism, terrorist financing or other offences, like corruption, bribery, drug trafficking, gold smuggling, human trafficking, kidnapping or other predicate offences and find out any relationship of the branch with the involved person; if so the BAMLCO should make an STR/SAR;
- 1.27.4. Create awareness regarding AML, CFT & CPF among the customer of the branch.



- 1.27.5. Ensure that corrective actions have been taken by the branch to address the deficiency identified by the BFIU, or BB, ICCD, and AML & CFT Division;
- 1.27.6. Monitor the staff of the branch to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering and Terrorist Financing.
- 1.27.7. Any other responsibility assigned by the CCC/ AML & CFT Division.

Internal Control & Compliance Division

Internal Audit or Internal Control and Compliance Division (ICCD) shall have an important role for ensuring proper implementation of Bank's AML & CFT Compliance Program. The Bank shall ensure that ICCD is equipped with enough manpower and autonomy to look after the prevention of ML&TF. The ICC has to oversee the implementation of the AML & CFT compliance program of the Bank and has to review the 'Self Assessment Report' received from the branches and to execute the 'Independent Testing Procedure' appropriately.

SL. No.	The Internal Audit Officials must:	Frequency
1	understand ML & TF risk of the Bank and check the adequacy of the mitigating measures;	On-going
2	examine the overall integrity and effectiveness of the AML/CFT Compliance Program;	On-going
3	examine the adequacy of Customer Due Diligence policies, procedures and processes, and whether they comply with internal requirements;	On-going
4	determine personnel adherence to the Bank's AML & CFT Compliance Program;	On-going
5	perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);	On-going
6	assess the adequacy of the Bank's processes for identifying and reporting suspicious activity;	On-going
7	where an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets;	On-going
8	communicate the findings to the board and/or senior management in a timely manner;	On-going
9	recommend corrective action to address the identified deficiencies;	On-going
10	track previously identified deficiencies and ensures correction made by the concerned person;	On-going
11	examine that corrective actions have taken on deficiency identified by the BFIU or BB;	On-going
12	assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;	On-going
13	Determine when assessing the training program and materials:	On-going



Sl. No.	The Internal Audit Officials must:	Frequency
	a. the importance of the Board and the Senior Management's on ongoing education, training and compliance b. the employee accountability for ensuring AML & CFT compliance c. comprehensiveness of training, in view of specific risks of individual business lines, d. training of personnel from all applicable areas of the Bank, e. frequency of training, f. coverage of Bank policies, procedures, processes and new rules and regulations, g. coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity, h. Penalties for noncompliance and regulatory requirements.	
14	Review of control procedures in the Bank to ensure legal and regulatory compliance and in the development of adequate and sufficient Independent Testing Procedures (ITP) to prevent and detect compliance lapses.	On-going
15	Perform AML Risk Assessment for the Business.	On-going
16	Perform periodic Quality Assurance on the AML program in the branches/divisions.	On-going

Managing Director & CEO

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

Initiatives by Human Resources Division

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

- 1.1.1. Revised Code of Conduct & Ethics for the employees of The Premier Bank Limited which is the integral part of the Service Rules and Regulations;
- 1.1.2. Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML & CFT measures;
- 1.1.3. Proper weight should be given in the annual performance evaluation of employees for extra ordinary preventive action vies a vies for non-compliance;



- 1.1.4. Written procedure to recover the fined amount from the concerned employee if the fine imposed on employee by the BFIU;
- 1.1.5. Other measures that shall be taken in case of non-compliance by the Bank.
- 1.2. **Know Your Employee (KYE) Procedure in Appointment of Employees:** One of the major purposes of combating money laundering activities is to protect the Bank from risks arising out of money laundering. To meet this objective, Human Resources Division shall have to undertake proper Screening Mechanism in its different appointment procedures so that The Premier Bank does not face any money laundering risk by any of its staffs.
- 1.3. **Recruitment Procedure:** To minimize ML & TF risks arise by or through its employees, Human Resources Division shall have to undertake fair recruitment procedure. This fair recruitment procedure shall not only include implementation of fairness in judging publicly declared competitive recruitment, but also include the judgment of good character. For this, Bank shall have to follow at least one from the following measures:
- 1.3.1. reference check
 - 1.3.2. background check
 - 1.3.3. screening through or clearance from Law Enforcement Agency
 - 1.3.4. personal interviewing
 - 1.3.5. personal guarantee etc.
- 1.4. **Training and Awareness –**
Training for Employee: Every employee of the Bank shall have at least basic AML & CFT training that should cover all the aspects of AML & CFT measures in Bangladesh. To keep the employees updated about AML & CFT measures, Bank shall require imparting refreshment training programs of its employees on a regular basis.
- 1.5. **Awareness for Senior Management, Customer & Mass People:** For effective implementation of AML & CFT measures in the Bank, Bank shall arrange awareness program for Senior Management, Customer and for Mass people.
- 1.6. **Job Rotation:** Human Resources Division shall ensure that all branch officials including the branch managers must be transferred once in every 3 years.
- 1.7. **Leave Management:** Human Resources Division shall monitor leaves taken by employees to ensure that all branch officials including the branch managers have taken 10 continuous days leave at a time each year as mandatory leave as per HRD Circular No. 13/2021 dated March 14, 2021 and Bangladesh Bank BRPD Circular No. 15 dated October 25, 2018.

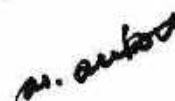


CHAPTER VIII: CUSTOMER DUE DILIGENCE**Introduction**

"Service First" is one of the main key issues for Premier Bank and as a result Premier Bank pays more attention to satisfy customer needs. As part of the process customer due diligence (CDD) plays an essential role. CDD is a vital and most effective defense against Money Laundering (ML) and Terrorist Financing (TF). As such, inadequacy in KYC standard can result in serious customer and counterparty risks, especially, reputational, operational, legal and compliance risks. As per section 25 of Money Laundering Prevention Act, 2012 (amendment 2015) and section 7 of Money Laundering Prevention Rules 2019, each bank requires to keep complete and accurate information of its customers. It is also the responsibility of each bank to identify suspicious transactions proactively and report the same to BFIU.

- 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 record keeping and require banks 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.
- 1.2. For the safety and soundness of financial institution the primary requirement is sound KYC procedures that help to protect financial institution's reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage. 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).
- 1.3. The inadequacy or absence of KYC standards can subject banks 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 loss to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, 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.
- 1.4. A sound Customer Due Diligence (CDD) program is one of the best ways to prevent money laundering and other financial crime. The more you know about its customers, the greater chance of preventing money-laundering abuses. Customer Due Diligence (CDD) combines the Know Your Customer (KYC) procedure, transaction monitoring based on the information and data or documents collected from reliable and independent sources.
- 1.5. The CDD obligations on banks under legislation and regulation are designed to make it more difficult to abuse the banking industry for money laundering or terrorist financing or proliferation financing. The CDD obligations compel banks to understand who their customers are to guard against the risk of committing



offences under MLP Act, 2012 (amendment 2015) including 'Predicate Offences' and the relevant offences under ATA, 2009 (amendment 2012 & 2013).

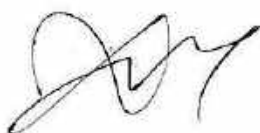
1.6. Therefore, Premier Bank implements adequate CDD measures considering the risks of ML, TF & PF. Such risk sensitive CDD measures should be based on-

- 1.6.1. Types of customers;
- 1.6.2. Business relationship with the customer;
- 1.6.3. Types of banking products; and
- 1.6.4. Transaction carried out by the customer.

Legal Obligation of CDD

1.1.1. Under the obligation of MLPA, 2012(amendment 2015), "The branch shall have to maintain **complete** and **accurate** information with regard to the identity of its customers during the operations of their accounts and provide with the information maintained under the clause to Bangladesh Bank". Under the MLP Act, 2012, SRO No. 357-Law/2013 dated 21.11.2013, Part -vi, section 17, (3) the bank shall identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data). The verification of identity of a customer or a beneficial owner should include a series of independent checks and inquiries and not rely only on documents provided by the customer or beneficial owner. The bank shall verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person.

- a) The bank shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the bank is satisfied that it knows who the beneficial owner is.
- b) The bank shall understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship. The bank shall also conduct ongoing due diligence on the business relationship.
- c) There are two things:
 - i) The bank shall scrutinize the transactions undertaken by a customer throughout the relationship with the customer to ensure that the transactions are consistent with the nature, business and risk profile of the customer, including where necessary, with the source of funds.
 - ii) The bank shall keep up to date documents, data, information and so on collected under CDD process and review the existing records, particularly for high





M. Ahsan

risk categories customers with utmost care and need to mitigate any sort of risk.

- 1.2. **Customer Due Diligence:** Considering the Risk Grading of Customer Due Diligence (CDD) should be done at different stages. Ongoing CDD has to be conducted to identify the nature of business, level of risk and incompatibility of income with the source of fund. Existing information of High-risk Customers should be evaluated, assessed or examined. Authenticity of the Customer or Beneficial Owner information has to be verified during establishing business relationship or before transaction occurred in the account. But at the time of Occasional Customers, these measurements have to be taken during conducting transaction. Verification of information should be done as soon as possible after establishing business relationship where risk about ML/TF low or where dissolution of business relationship is not necessary. Guidelines on Beneficial Ownership issued by BFIU should be followed to identify actual beneficiary of the account and what steps can be taken in this aspect. It is required for Premier Bank to be certain about the customer's identity and underlying purpose of establishing relationship with the bank, and must collect sufficient information up to its satisfaction. "Satisfaction of the bank" means satisfaction of the account opening approving officer that is necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

1.2.1. Timing of CDD – Officials involved with account opening/transaction must apply CDD measures when he/she does any of the following:

- a) Establishing a business relationship
- b) Carrying out an occasional transaction
- c) Suspecting money laundering or terrorist financing or
- d) Suspecting the veracity of documents, data or information previously obtained for the purpose of identification or verification.

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

a) Normal CDD Measures:

- i) Identifying the customer and verifying that customer identity using reliable, independent source documents, data of information.
- ii) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such as that the bank is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include banks understanding the ownership and control structure of the customer.
- iii) Understanding and as appropriate, obtaining information on the purpose and intended nature of the business relationship.





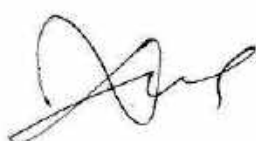

iv) Conducting on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transaction being conducted are consistent with the bank's knowledge of the customer, their business and risk profile, including where necessary the source of funds.

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

1.2.3. CDD Measures that could be applied for higher risk business relationship include:

- a) Obtaining additional information on the customer (occupation, volume of assets, information available through public data base and internet etc. and updating more the identification data of customer and beneficial owner.
- b) Obtaining additional information on the intended nature of the business relationship.
- c) Obtaining information on the source of wealth of the customer.
- d) Obtaining information on the reasons for intended or performed transaction
- e) Obtaining the approval of senior management to commence or continue the business relationship
- f) 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
- g) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

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





M. Anwar

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

Simplified CDD shall be done for low risk accounts like Student Accounts, Farmer's Accounts and other No-Frill accounts. Simplified Customer Due Diligence (SCDD) process can be followed as per Guidelines on e-KYC in this aspect⁵. However, Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher risk scenarios apply.

1.2.5. CDD related other issues:

- a) While opening an Account of Customer, the bank will preserve Customer's Identification and Documents with conducting CDD. In this regard, Sample FORMAT of 'Digital KYC Form' provided by BFIU in the Guidelines on e-KYC or KYC FORM Annexure - A may be applied where Digital KYC Form cannot be used.
- b) Bank may not consider KYC form/forms ANNEXURE - A provided by BFIU as a part of Account Opening Form (AOF) in any way, KYC form should not be filled in by the customers.
- c) Ensure to update the Account Opening Form as instructed by BRPD circular 23, dated 28 December 2021.
- d) For providing Privilege Banking service to the customers, Bank will take enhanced safety measure in addition to CDD related instructions.
- e) Enhanced safety measures have to be taken and Counter Measures is to be required from FATF (where necessary) to establish and continue business relationship and transaction with those countries, persons, entities who do not meet the international standard of ML/TF prevention measures or have the significant deficiency.
- f) Before establishing business relationship with any foreign bank, Bank has to consider ML/TF prevention system of that country.
- g) "Guidelines for Prevention of Trade Based Money Laundering" issued by BFIU has to be followed during opening of foreign trade account and transaction.

1.2.6. If CDD is not possible: After preserving related documents both account closure or declining to open an account, Branch will send



those documents to AML/CFT Division. AML/CFT Division will take initiatives to inform other branches about all this information, if necessary. BFIU will issue circular time to time regarding opening and operating of an account of under privileged people of the society.

Know Your Customer (KYC) Policies and Procedures

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

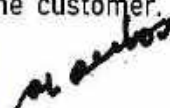
1.2.7. **Who is a Customer?** Customer identification and verification in terms of ML & TF risk management shall apply to both individuals and institutions where customer is defined as under:

- a) the person or entity that maintains an account with the bank/has business relationship with the bank;
- b) the person or entity on whose behalf an account is maintained (i.e. beneficial owners);
- c) professional intermediaries who is assigned to conduct transactions on behalf of the customer/trust/beneficial owner;
- d) any person or entity connected with occasional financial transaction who can pose a significant reputational or other risk to the bank;
- e) any person or entity defined as "customer" by BFIU from time to time.

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

1.2.9. **Identifying Real Person** - Bank must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any account, or transact business for the customer. Whenever



possible, the prospective customer should be interviewed personally. This will safeguard against opening of fictitious account.

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

1.2.11. Reliance on Third Party - Countries may permit financial institutions to rely on third parties to perform the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the bank relying on the third party. The criteria that should be met are as follows:

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

1.2.12. Customer Profiling

- a) Followings are required:
 - i) Obtaining and document the customer's basic background information.
 - ii) Try to use the information to evaluate the appropriateness of the customer's transaction activity.
 - iii) Determine the customer's source of fund.
- b) KYC Profile Should Disclose:
 - i) The customer expected transaction trend
 - ii) The source of wealth
 - iii) Net worth
- c) KYC Profile Should be Upgraded/Updated by:



- i) Regular review of transaction activity and balance fluctuation report
- ii) Newspaper and Magazine article, financial statement, brochure, industry activities relating to the customer.
- iii) Periodical discussion with the client relating to their business activities including future plan of the business for the next 12 months.

1.2.13. Customer Assessment

a) **Methodology of Assessing Customer** - In preparing the policy, following indicators/factors have been considered to assess customers:

- i) Customer's background
- ii) Country of origin and country where it operates
- iii) Geographic location of service or business
- iv) Purpose of establishing relationship with bank
- v) Information available for verifying the customer identity
- vi) Politically Exposed Person (PEP), Influential Person (IP) and chief/senior official of international organizations, their family members and close associates
- vii) Linked accounts
- viii) Customer profession or nature of business
- ix) Monthly income/Net worth/Turnover
- x) Presence of beneficial owner
- xi) Existence of customer details in sanction lists/banned list
- xii) Existence of customer's name in adverse media reports
- xiii) Presence of customer in branch during opening account and availing services
- xiv) Risk profile of customer based on risk register
- xv) Mode of marketing the products/services to the customer
- xvi) Type of product/service availed
- xvii) Source of fund to the account
- xviii) Transaction profile and pattern
- xix) On-boarding channel
- xx) Other risk indicators

1.2.14. **Know Your Customer Program** - Having sufficiently verified/corrected information about customers - "Knowing Your Customer" (KYC) - and making use of that information underpins all AML, CFT & CPF efforts, and is the most effective defense against being used to launder the proceeds of crime. Financial institutions with inadequate KYC program may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the financial institution's overall



safety and soundness, they also protect the integrity of its system by reducing AML, and CFT & CPF related offences.

1.2.15. Know Your Customer (KYC) Procedure - Money Laundering Prevention Act, 2012 (Amendment 2015) requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. FATF recommendation 10 states that where the financial institution is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner and unable to obtaining information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transaction report in relation to the customer.

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

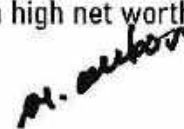
- a) Customer acceptance policy,
- b) Customer identification,
- c) On-going monitoring of high risk accounts, and
- d) Identification of suspicious transactions.

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

Customer Acceptance Policy

Premier Bank has developed its Customer Acceptance Policy laying down explicit criteria for acceptance of customers including a description of the types of customer that are likely to pose a higher than average risk to a financial institution. In preparing such policies, factors such as customers' background, country of origin, public or high-profile position, linked accounts, business activities or other risk indicators should be considered. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source



of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures (if considered high risk) or politically exposed persons should be taken exclusively at senior management level.

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

- a) No account can be opened in anonymous or fictitious name.
- b) Parameters of risk perception are clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grade.
- c) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.
- d) Bank should not open an account or close an account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non reliability of the data/information furnished to the bank. Decision by the bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
- e) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.
- f) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
- g) The status of a customer may change as relation with a customer progress. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.
- h) Bank should not open account in the name of listed in UN Sanction lists, OFAC Sanction lists and directed by Bangladesh Bank or any other sanction lists.
- i) No account should be opened through Online. In case of foreign resident account may be opened through Bangladesh Mission or own bank branch if available or legal representative obtaining KYC/e-KYC, ETP, source of income and risk grading.





- j) No account should be opened for those customers for whom reports of unusual or suspicious transaction are repeatedly submitted to the BFIU, if it is known, account of such person /entity should not be opened
- k) No account should be opened for that customer for whom the collection of information for assessing their overall profile is impossible.
- l) No account should be opened for that customer whose activities or transaction are not consistent with the information available to them, their professional activity, their risk profile and the origin of the fund.
- m) No account should be opened for that customer failing to provide all information required for the identification and verification of their identity.
- n) The status of a customer may change as relation with a customer progress. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.

Risk Perception

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

- 1.1.1. Customers' constitution: Individual, proprietorship, partnership, public or private ltd. etc.
- 1.1.2. Business segment: Retail, Corporate, SME etc.
- 1.1.3. Country of residence/ Nationality: Whether Bangladeshi or any overseas location.
- 1.1.4. Product subscription: Salary Account/NRB product etc.
- 1.1.5. Economic profile: High net worth individual, Public limited Co. etc.
- 1.1.6. Account status: Active, In-operative, dormant etc.
- 1.1.7. Account vintage: less than six months old etc. And as per BRPD circular 23 dated 28 December 2021.
- 1.1.8. Presence in regulatory negative/ PEP/Defaulter/Fraudster etc.
- 1.1.9. Suspicious Transaction Report (STR) filed for the customer, AML alerts.

Acceptance of Customer

- 1.1.1. **Individual** - Any citizen (male, female and third gender) of Bangladesh who is an adult individual of 18 years of age or more, and eligible to enter into a contract can open account individually or jointly.
- 1.1.2. **Existing Customer** - Branch must ensure that one customer has one unique customer identification code (UCIC) though he/she/it may



have more than one account with the bank.

1.1.3. The following entities can open account on completion of due diligence:

- a) Proprietorship concern;
- b) Partnership firm;
- c) Private Limited Companies;
- d) Public Limited Companies;
- e) One Person company;
- f) Government, semi-government and autonomous bodies;
- g) NGOs, NPOs, Clubs, Societies, Charities, Religious Organization, Social Organizations;
- h) Educational institute (School, College, Madrasah, University);
- i) Local Authorities;
- j) Executors/Administrators/Trustees;
- k) Liquidators;
- l) Foundations;
- m) Embassies;
- n) Other legally formed entities acceptable to bank

- 1.2. **Non-Resident Bangladeshi** - Non-Resident Bangladeshis can open account with Premier Bank while they are in Bangladesh and can also open account without being physically present in the country as per the process defined later in the document.
- 1.3. **Customers Who Want to Open Foreign Currency Account** - Resident Bangladeshis, Non-Resident Bangladeshis and Foreign Nationals can be allowed to open Foreign Currency (FC) Accounts with AD Branches observing formalities and existing laws, policies (including GFET) and instructions.
- 1.4. **Correspondent Institutions** - Other banks (local or foreign) can be allowed to establish Correspondent Relationships as well as SWIFT RMA (Relationship Management Application) with Premier Bank after completion of due diligence and KYC formalities subject to approval from the CAMLCO of the bank.
- 1.5. **Exchange Houses** - Exchange houses can establish relationship with Premier Bank after completion of due diligence and KYC formalities subject to approval from the CAMLCO of the bank.
- 1.6. **Politically Exposed Persons (PEPs)/ Influential Persons (IPs)/ Chief or Senior Officials of International Organizations and their Family Members and Close Associates:** PEPs/IPs/Chief or Senior Officials of international organizations can open accounts with the approval of CAMLCO of the bank. Enhanced due diligence is applicable for establishing and maintaining relationship with these accounts.
- 1.7. **Special Types of Customer(s)** - There are different types of people who cannot comply fully with the terms and conditions, laws, rules etc. to become customer, should be considered separately and they may be termed as special customers. Special care should be taken while opening and allowing operation of these accounts. All required documents should be obtained in order to follow





instructions of circulars and guidelines of Bangladesh Bank as well as the bank. Below are some examples of special customers:

- 1.7.1. **Minor** - A minor is a person who is below 18 years. In that case account may be opened and operated by his/her guardian (as defined by Bangladesh Financial Intelligence Unit) up to the date of their attaining majority.
- 1.7.2. **Illiterate Person**- Illiterate person(s) can open and operate accounts with his/her/their respective thumb impressions in presence of the branch manager/branch operations manager. For withdrawal of money the illiterate person/persons must come personally to the branch/office, where he/she/they opened the account and shall put thumb impression on the cheques in presence of the branch manager/branch operations manager. No debit card will be issued to such customers.
- 1.7.3. **Blind Person**- Blind person(s) can open account. Such accounts should be carefully handled by the bank. For withdrawal of money, the blind person(s) must come personally to the branch/office, where he/she/they opened the account and put their respective thumb impressions/signatures on the cheque in presence of the branch manager/branch operations manager.
- 1.7.4. **Under Privileged Person**- Special care needs to be taken for the people who are financially or socially disadvantaged people i.e. street children accounts, farmer's accounts etc.

Policy for Rejection of a Customer

- 1.1.1. **Accounts in fictitious names or numbered accounts-**
 - a) No account shall be opened in anonymous or fictitious name;
 - b) No account shall be opened without having name, address, signature etc.
- 1.1.2. **Lunatics, persons of unsound mind and bankrupts will not be allowed to open account.**
- 1.1.3. **Activities of Customer-** No account shall be opened for customers whose activities are not consistent with the information available about them, their professional activities, their risk profiles and the sources of the funds.
- 1.1.4. **Insolvent**-No individual account in the name of an insolvent shall be opened.
- 1.1.5. **Unlicensed Banks and/or NBFIs-** No account shall be opened for unlicensed banks and/or NBFIs and other entities that provide banking services to unlicensed banks and/or NBFIs.
- 1.1.6. **Section 311 of USA Patriot Act Designated Entities** - No account shall be opened for Section 311 designated entities.
- 1.1.7. **Other Entities** - No account will be opened or maintained for any unregulated charities, unlicensed/unregulated remittance agents, exchanges houses, casa de cambio, bureau de change or money transfer agents, red light business/adult entertainment





companies, gambling houses and individuals or entities with virtual currencies and illegal drugs.

1.1.8. **Shell Bank-** Bank shall not establish correspondent relationships with shell banks (a shell bank is defined as 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), and any other entity which maintains relationship with such shell bank(s).

1.1.9. **Existence in Sanction List -** No account shall be opened or operated in the name of any person or entity listed under sanction list (e.g. United Nations Security Council Resolutions) (UNSCRs), OFAC list etc.), adverse media list of their associates having suspicion of being involved in terrorist or terrorist financing activities and proscribed or enlisted by Bangladesh Government.

Bank shall not open an account where it is unable to apply appropriate customer due diligence measures i.e. when the bank is unable to verify the identity and/or obtain documents required as per risk categorization due to non cooperation of the customer. While undertaking due diligence procedures, bank must be careful to avoid harassment to the customer.

1.2. **Customer Identification -** Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for bank to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if the bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained.

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

1.3.1. the physical identity (e.g. Birth Certificate, TIN/VAT Registration, Registration Certificate, Certificate of Incorporation, Passport/National ID/ Smart ID etc.); and the activity undertaken. Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context to avoid breaches of UN or other



international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issuance should be recorded.

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

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

Customer Type Wise Account Opening and Operating Procedure:


Customer type wise account opening and operating procedure: special check points

Customer Type	Procedure
Individual	<ol style="list-style-type: none"> 1. In case, customer is involved in multiple profession/ business, bank shall consider nature of business with highest risk rating while assessing the risk. 2. Signature of nominee and beneficial owner not required 3. If a customer holds NID (which has been verified by bank with EC database), no introduction will be required. However, if the customer wants to establish relationship with identity document other than NID, he/she has to be introduced by an existing account holder or any person having NID, acceptable to the bank. Branch/office official checks whether the photograph of account holder is attested by introducer (in applicable cases) and the signature of the introducer matches with the one available in CBS/NID. 4. It is encouraged to have Nominee within immediate family members. However, if any






Customer Type	Procedure
	customer wants to assign a person as nominee, who is not an immediate family member, he/she has to state the reason behind assigning such person as nominee.
Joint Account Holder	Bank shall: <ol style="list-style-type: none"> 1. Ensure the purpose of opening joint account; 2. Identify the relationship between/among the applicants; 3. Complete due diligence for all the applicants; 4. Create separate CIF in CBS for each applicant (if there is no CIF earlier); 5. Complete separate KYC for all the applicants; 6. Highest risk grading of any of the joint applicants shall be the risk grading of the account.
Existing Customer	Bank shall: <ol style="list-style-type: none"> 1. Ensure the purpose of opening an additional account; 2. Make sure that the account is opened with UCIC already assigned to that customer; 3. Updated information of CIF supported by document(s), if there is any change/addition/deletion as per PBL Branch Network 4. Operations Manual and SOP on implementation of UCIC.
Self-employed individuals/ professionals	<ol style="list-style-type: none"> 1. Collect document(s) in support of profession. 2. If no document is available, obtain written declaration on self-employment acceptable to bank.
Proprietorship	Bank shall: <ol style="list-style-type: none"> 1. Complete KYC procedures for the entity as well as for the beneficial owner of the proprietorship firm (to be identified as per the SOP on identification & due diligence for BO). 2. Accounts opened in the name of proprietary concern shall be operated by the proprietor. Any person other than proprietor shall be allowed to operate the account if authorized to do so either by way of mandate or power of attorney. 3. Ensure having official seal of the proprietor affixed at appropriate places of the AOF and other documents, as applicable. 4. No introduction is required for proprietorship concern. 5. Assignment of nominee for proprietorship concern is not encouraged. However, if any customer wants to assign nominee then nominee may be allowed on completing due



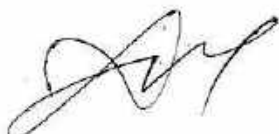
Customer Type	Procedure
	diligence i.e. have the nominee related information form filled in with photo and identity proof document.
Partnership Firm	Bank shall: <ol style="list-style-type: none"> 1. Study the clauses under partnership deed and prefer deed that is registered. 2. Complete KYC procedures for the firm as well as for the beneficial owners of the partnership firm (to be identified as per the SOP on identification & due diligence for BO). 3. Complete due diligence for the signatories and beneficial owners. 4. Ensure having official seal of the firm and of the partners/signatories (if and as applicable) affixed at appropriate places of the AOF and other documents, as applicable. 5. No introduction is required for partnership firm. 6. Do not accept nominee for partnership firm as per section 103 of Bank Company Act 1991 (Amendment 2013).
Limited Company	Bank shall: <ol style="list-style-type: none"> 1. Identify the beneficial owner(s) as per the SOP on identification & due diligence for BO; 2. Ascertain the power of the signatories with regard to the operation of the account as per Board Resolution/Articles of Association. 3. Complete due diligence for signatory (ies), top 5 directors in terms of shareholding (as per BRPD directives) and beneficial owner(s). 4. Complete KYC procedures for the limited company as well as for beneficial owner(s). 5. Ensure having official seal of the signatory (ies) (as applicable) affixed at appropriate places of the AOF and other documents, as applicable. 6. No introduction is required for Limited Company. 7. Do not accept nominee for limited company as per section 103 of Bank Company Act 1991 (Amendment 2013).
Executors, Administrators, Trustees	Bank shall: <ol style="list-style-type: none"> 1. Determine whether the customer is acting on behalf of another person as trustee/executor/administrator. If so, obtain satisfactory evidence of the identity of <ul style="list-style-type: none"> o the trustee/executor/administrator and o the persons on whose behalf they are acting



Customer Type	Procedure
	2. Ensure power/authority of signatories of the account as per the trust deed.
NGOs, Clubs, Charitable Organizations, Social Organizations, Societies, and Associations etc.	Bank shall: 1. Check the resolution from the board/governing body/executive committee and specify the persons authorized to operate the account 2. Complete due diligence for signatory(ies), 5 EC members and beneficial owner(s) 3. No introduction is required 4. Obtain an undertaking as well as fresh resolution from Governing Body/Board of Trustees/Executive Committee/sponsors to inform the bank about any change of control or ownership during operation of the account.
Foreign Nationals	Bank shall: 1. Ensure the purpose of opening account; 2. Check whether the individual has documents to support his/her/their stay in Bangladesh (applicable for those who are residing in Bangladesh); 3. Follow Foreign Exchange Regulation Act, 1947 and Guideline for Foreign Exchange Transaction meticulously; 4. Follow any other regulatory manuals, circulars, directives and instructions as applicable. 5. Any other instructions and guidelines that may be issued by PBL time to time.
Non-Resident Bangladeshi	Bank shall: 1. Ensure the purpose of opening account; 2. Check whether the individual has documents to support his/her/their stay outside Bangladesh; 3. Follow all relevant Acts, rules and regulatory guidelines, manuals, circulars, directives and instructions as applicable; 4. Follow any other instructions and guidelines that may be issued by PBL from time to time.
Politically Exposed Persons (PEPs), Influential Persons (IPs), Senior Officials or Chief of International Organizations (IOs), their family members and close associates	Bank shall: 1. Perform enhanced due diligence while establishing and maintaining relationship with PEPs/IPs/senior officials of international organization(s) and their family member(s)/close associate(s); 2. Follow SOP on PEP account management 3. Follow Foreign Exchange Regulation Act, 1947 and Guideline for Foreign Exchange Transaction meticulously for non- residents.
Minors	Bank shall: 1. Have the account opening form and document(s) (as applicable) signed by the guardian; 2. Ensure that the account is operated by the

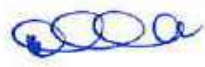


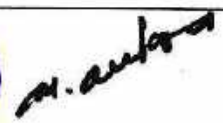
Customer Type	Procedure
	guardian until the minor becomes a major; 3. Ensure completing individual information form for both the minor and guardian and both the forms should be signed by the guardian; 4. Identify beneficial owner, if any as per the SOP on identification & due diligence for BO; 5. Complete KYC profiles for both the minor and the guardian. 6. Consider risk rating of the KYC profile with higher risk as the ultimate risk rating of the account.
Government Organizations	Bank shall: 1. Ensure purpose of opening the account; 2. Ensure completing individual information form by the signatory(ies); 3. Ensure that government accounts are not opened in the name of the government official; 4. Complete KYC profile for the government organization.
Walk-in Customers (non-account holder customers)	Bank shall obtain information of walk-in customers as per BFIU and AML & CFT directives.
Correspondent Banks/Institutions	Bank shall: 1. Obtain information as per instruction of BFIU circular No. 26 dated prescribed format provided by AML & CFT Division of Head Office. Annexure-; 2. Ascertain publicly available information whether the correspondent bank has been subject to any money laundering or terrorist financing investigation or regulatory action; 3. Be satisfied about the nature of the business; 4. Be sure about the effective supervision of that foreign institution by the relevant regulatory authority; 5. Should not establish or maintain any correspondent relationship with shell bank and those who maintain relationship with shell bank; 6. Ensure Enhanced Due Diligence while establishing and/or maintaining business relationship with entities of High Risk and Non-Cooperative Jurisdiction; 7. If any respondent bank allows direct transactions by their customers to transact business on their behalf (i.e. payable through account), the corresponding bank must be sure about the appropriate CDD of the customer has






Customer Type	Procedure
	<p>been completed by the respondent bank;</p> <ol style="list-style-type: none"> Obtain approval from CAMLCO before establishing and while continuing any relationship Perform enhanced monitoring on an ongoing basis and KYC to be reviewed regularly.
<p>Customers Who Want to Open Resident Foreign Currency Deposit (RFCD) Account:</p>	<ol style="list-style-type: none"> Eligible customers can open RFCD accounts with Authorized Dealer Branches of PBL; Any Bangladeshi citizen ordinarily resident in Bangladesh may open RFCD account with foreign exchange brought in at the time of their returns from travel abroad; Foreign Exchange Regulation Act, 1947 and Guideline for Foreign Exchange Transaction and circulars issued from respective department of Bangladesh Bank. PPG and circulars on RFCD account (if any) by relevant division of PBL to be followed.
<p>Customers Who Want to open Non-Resident Foreign Currency Deposit (NFCD) Account</p>	<p>a) Eligibility:</p> <p>Individual NFCD Account:</p> <ol style="list-style-type: none"> Bangladeshi nationals residing abroad such as: wage earners; Person having dual nationality and ordinarily residing abroad [any foreign Valid Passport holder of Bangladeshi origin (usually by birth) and Bangladesh mark]; Bangladeshi nationals serving at embassies/high commissions of Bangladesh in foreign countries; Bangladeshi nationals working with foreign/international organizations operating in Bangladesh, provided their salary is paid in foreign currency; Shore staff abroad of Bangladesh Shipping Corporation. <p>Non-Individual NFCD Account:</p> <ol style="list-style-type: none"> Foreign companies/firms registered and/or incorporated abroad; 100% foreign owned (A-Type) industrial units in the Export Processing Zones; <p>b) Bank shall follow:</p> <ol style="list-style-type: none"> Foreign Exchange Regulation Act, 1947 and Guideline for Foreign Exchange Transaction and circulars issued from respective department of Bangladesh Bank; PPG and circulars on NFCD account (if any) by relevant division of PBL to be followed.
<p>Customers Who Want to Open</p>	<p>a) Eligibility:</p>



Customer Type	Procedure
Export Retention Quota (ERQ) Account	1. Direct Exporters 2. Deemed Exporters 3. Service Exporters 4. Govt. approved recruiting agents for manpower export b) Bank shall follow PPG and circulars on ERQ account (if any) by relevant division of PBL to be followed.

Document or Strategy for Verification of Address

The address of the customer has to be verified following SOP on Risk Based CPV. **Indicative list of standard documents for opening account and verifying profession, nature of business and sources of funds** - Establishing the identity of customers is vital under Customer Due Diligence (CDD), for acceptance or rejection of customer. The customer identification means identifying the customer and verifying his/her identity by using reliable independent source, documents, data or information. Documents are to be obtained according to Acts, Rules, Manuals, Guidelines, and Circulars, Circular Letters issued by concerned authority and various divisions/departments of head office time to time.


Bank shall also perform enhanced due diligence as it deems required specially while dealing with Privilege Banking Customers.


In case of enhanced due diligence, bank shall follow ML & TF Risk Management Policy and thus shall obtain additional information on the identity of the customer from independent and reliable sources document in support of source of funds/asset in the account, preferable the one having financial figures on it, such as salary certificate, cash flow statement, bank loan document, other bank statement etc.

CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
Individuals/ Joint Account Holders	1. Document(s) in support of identity of the applicant(s), nominee(s) beneficial owner(s) and mandatee(if any): ➤ National ID Card; or Valid Passport; or ➤ Birth Registration Certificate; (with seal & signature) issued by competent authority such as, Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board. 2. Photograph of	➤ Salary Certificate (for the salaried person) ➤ Employment ID (for ascertaining level of employment) ➤ Self-declaration acceptable to the bank (commensurate with declared occupation); ➤ Documents in support of income of the beneficial owner (if any). ➤ Valid Trade License (if the customer is a businessperson);



CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<ul style="list-style-type: none"> ➤ Applicant(s) (attested by introducer, if applicable) ➤ Nominee(s) (attested by applicant) ➤ Beneficial Owner (attested by applicant) ➤ Mandatee (attested by applicant) 3. Document in support of the address of the individual 	<ul style="list-style-type: none"> ➤ E-TIN (if any); ➤ Documents of property sale (if applicable); ➤ Other bank statement (if any); Document of FDR encashment(if applicable); ➤ Document of foreign remittance (if any fund comes from outside the country); Document of retirement benefit (if applicable); ➤ Tax payment proof document issued by competent authority; ➤ Bank loan documents (if any), etc. ➤ Copy of share and debenture portfolio;
<p>Sole Proprietorship (Individuals Engaged in Business Activities)</p>	<ol style="list-style-type: none"> 1. Document(s) in support of identity of the Proprietor: <ul style="list-style-type: none"> ➤ National ID Card; or Valid ➤ Passport; or ➤ Birth Registration Certificate; (with seal & signature) issued by competent authority such as, Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board. 2. Photograph of <ul style="list-style-type: none"> ➤ Proprietor; ➤ Beneficial Owner (to be identified as per the SOP on identification & due diligence for BO ➤ Beneficial Owner (attested by applicant) ➤ Mandatee (attested by applicant) 3. Document in support of address of the <ul style="list-style-type: none"> ➤ Entity; ➤ Proprietor; 4. Document(s) in support of identity of the Proprietorship Concern; <ul style="list-style-type: none"> ➤ Valid Trade License; ➤ Rent receipt of the shop (if the shop is rental); ➤ Ownership documents of the shop (i.e. purchase documents of the shopper inheritance documents); ➤ Membership certificate of any 	<ul style="list-style-type: none"> ➤ Valid Trade License; ➤ E-TIN; ➤ Self-declaration acceptable to the bank; (commensurate with nature and volume of business); ➤ Documents of property sale. (if any fund is injected by selling personal property); ➤ Other bank statement (if any); ➤ Document of FDR endashment (if any fund is injected by en-cashing FDR); ➤ Document of foreign remittance (if any fund comes from outside the country); ➤ Bank loan documents (if any); Personal borrowing (if any), etc. ➤ Copy of Share & Debenture Portfolio; ➤ Tax payment proof document issued by competent authority; ➤ Financial statement of last year.



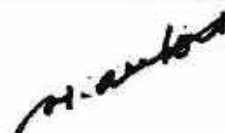
CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<p>association; (Chamber of commerce, market association, trade association i.e.; hardware association, cloth merchant association, hawkers association, etc.);</p> <ul style="list-style-type: none"> ➤ VAT registration number (optional); ➤ Any other documents that satisfy the bank. 	
<p>One Person Company (OPC)</p>	<p>1. Document(s) in support of identity and operation of the OPC:</p> <ul style="list-style-type: none"> ➤ Valid Trade License; ➤ Certificate of incorporation; ➤ Memorandum of Association (Registered); ➤ Articles of association (Registered); ➤ Power of attorney/mandate granted to the respective manager, officials or employees to transact business on its behalf; <p>2. Document(s) in support of identity of the</p> <ul style="list-style-type: none"> ➤ Owner ➤ Authorized Signatories ➤ Beneficial Owner; ➤ National ID Card; or ➤ Valid Passport; or ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board. <p>Photograph of</p> <ul style="list-style-type: none"> ➤ Owner; ➤ Each authorized signatories ➤ Beneficial Owner <p>Document in support of address of the</p> <ul style="list-style-type: none"> ➤ Entity ➤ Owner and authorized signatories 	<ul style="list-style-type: none"> ➤ Valid Trade License; ➤ E-TIN; ➤ Self-declaration acceptable to the bank. (commensurate with nature and volume of business); ➤ Documents of property sale. (if any fund is injected by selling personal property); ➤ Other bank statement (if any); ➤ Document of FDR encashment (if any fund is injected by en-cashing FDR); ➤ Other bank statement (if any); ➤ Document of FDR encashment (if any fund is injected by en-cashing FDR); ➤ Document of foreign remittance (if any fund comes from outside the country); ➤ Bank loan documents (if any); ➤ Personal borrowing (if any) etc.; ➤ Copy of Share & Debenture Portfolio; ➤ Tax payment proof document issued by competent authority;






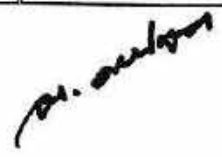

CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
		<ul style="list-style-type: none"> ➤ Financial statement of last year.
Partnership Firms	<p>Document(s) in support of identity and operation of the Partnership Firm:</p> <ul style="list-style-type: none"> ➤ Valid Trade License; ➤ Partnership deed (preferably registered). For loan account registration is mandatory. ➤ Resolution of the partners, specifying operational guidelines/instruction of the partnership account. ➤ Rent receipt of the office space/shop (if the space/shop is rental); ➤ Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents); ➤ Membership certificate of any association. (For example, chamber of commerce, market association, trade association i.e.; hard ware association, cloth merchant association, hawkers' association etc.); ➤ VAT registration number (optional); ➤ Any other documents that satisfy the bank. <p>Document(s) in support of identity of each of the partners</p> <ul style="list-style-type: none"> ➤ National ID Card; or ➤ Valid Passport; or ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board. <p>Photograph of</p> <ul style="list-style-type: none"> ➤ Each signatory; ➤ Beneficial Owner (to be identified as per the SOP on identification & due diligence for BO) <p>Document in support of address of the</p>	<ul style="list-style-type: none"> ➤ Valid Trade License; ➤ E-TIN; ➤ Document of property sale. (if any fund is injected by selling property of any partner); ➤ Other bank statement (if any); ➤ Document of FDR en-cashment; (if any partner injected capital by en-cashing personal FDR); ➤ Document of foreign remittance (if any fund comes from outside the country); ➤ Bank loan documents (if any); ➤ Personal borrowing (if any); ➤ Copy of portfolio; ➤ Tax payment proof document issued by competent authority; ➤ Financial statement of last year; ➤ VAT registration/BIN.



CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<ul style="list-style-type: none"> ➤ Entity ➤ Signatory 	
<p>Private Limited Company</p>	<p>1. Document(s) in support of identity and operation of the company:</p> <ul style="list-style-type: none"> ➤ Valid Trade License; ➤ Certificate of incorporation; ➤ Memorandum of Association (Registered); ➤ Updated list of directors with ownership structure (Form XII + Form X) ; ➤ Resolution of the board of directors to open an account of those who will operate the account; ➤ Power of attorney/mandate granted to its managers, officials or employees to transact business on its behalf; ➤ Permission from regulatory/competent authority to receive foreign remittance. <p>2. Document(s) in support of identity of each of the</p> <ul style="list-style-type: none"> ➤ Authorized signatories; ➤ Top 5(five) Directors in terms of shareholding; ➤ Beneficial Owners: <ul style="list-style-type: none"> a) National ID card; b) Valid Passport; or c) Birth Registration Certificate (with seal & signature) issued by competent authority, such as Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board etc. <p>3. Photograph(s) of:</p> <ul style="list-style-type: none"> ➤ Each authorized signatories; ➤ Top 5(five) directors in terms of share holding; ➤ Beneficial Owner (to be identified as per the SOP on identification and due diligence for BO). 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly authenticated by competent authority; ➤ Other bank statement; ➤ Valid Trade License; ➤ E-TIN; ➤ VAT registration/BIN; ➤ Bank loan documents (if any), etc. ➤ Tax payment proof document issued by competent authority; ➤ Any other legal document specifying source of fund.



CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<p>4. Document in support of address of the;</p> <ul style="list-style-type: none"> ➤ Entity; ➤ Authorized Signatories 	
<p>Public Limited Companies</p>	<p>1. Document(s) in support of identity and operation of the company:</p> <ul style="list-style-type: none"> ➤ Valid Trade License; ➤ Certificate of incorporation; ➤ Certificate of commencement of business; ➤ Memorandum of Association (Registered); ➤ Updated list of directors with ownership structure (Form XII + Form X) ; ➤ Resolution of the board of directors to open an account of those who will operate the account; ➤ Power of attorney granted to its managers, officials or employees to transact business on its behalf; ➤ Permission from regulatory/competent authority to receive foreign remittance. <p>2. Document(s) in support of identity of each of the</p> <ul style="list-style-type: none"> ➤ Authorized signatories; ➤ Top 5(five) Directors in terms of shareholding; ➤ Beneficial Owners: <ul style="list-style-type: none"> d) National ID card; e) Valid Passport; or f) Birth Registration Certificate (with seal & signature) issued by competent authority, such as Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board etc. <p>5. Photograph(s) of:</p> <ul style="list-style-type: none"> ➤ Each authorized signatory; ➤ Top 5(five) directors in terms of share holding; ➤ Beneficial Owner (to be identified 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certified by a professional accountant; ➤ Other bank statement (if any); ➤ Valid Trade License; ➤ E-TIN; ➤ Cash flow statement; VAT registration/BIN; ➤ Bank loan documents (if any); ➤ Tax payment proof document issued by competent authority; ➤ Any other documents of legal source, etc.





CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	as per the SOP on identification and due diligence for BO). 6. Document in support of address of the; ➤ Entity; ➤ Authorized Signatories	
Govern-ment- Owned Entities	➤ Government order/statute regarding formation of the entity/notification; ➤ Document related to opening and operation of account; ➤ ID documents of those who have authority to operate the account; Photograph of the ➤ operator(s); ➤ Document in support of address verification.	N/A
Semi Govt. / Corporation/ Statutory / Autonomous Body	➤ Government order/statute regarding formation of the entity/notification; ➤ Document related to opening and operating the account; ➤ Identification of those who have authority to operate the account; ➤ Photograph of the operator(s); Document in support of address verification.	➤ Donation/ Subscription/ Foreign or Local Aid (if any); ➤ Government/Other Specific Approved Fund (if any); ➤ Other bank statement (if any); ➤ Any other documents of legal source, etc.
NGO or NPO or Charities or Religious Organisations or Clubs or	1. Document(s) in support of identity and operation of the entity: ➤ Bye-laws (certified copy); ➤ Certificate of registration/permission document issued under relevant Acts or by competent authority (as applicable)- ➤ Societies Registration Act ➤ Cooperative Societies Act ➤ Ministry of Social Welfare ➤ Ministry of Religious Affairs ➤ Ministry of Commerce ➤ NGO Bureau ➤ Sub-registry Office ➤ Any other act/competent authority documents related to nature of the	➤ A copy of last available financial statements duly certified by a professional accountant; ➤ Other bank statement; ➤ E-TIN; ➤ Certificate of grant/aid; Subscription (if applicable); ➤ If unregistered, declaration of authorized person/body (if applicable); ➤ Bank loan documents (if any); ➤ Tax payment proof document issued by competent authority; ➤ Any other documents of legal



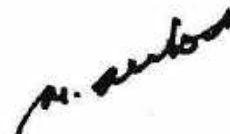
CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
Societies	<p>entity;</p> <ul style="list-style-type: none"> ➤ Permission from regulatory/competent authority to receive foreign remittance; ➤ List of executive committee/management committee/directors; ➤ Resolution of the executive committee/management committee/directors to open account, and identification of those who have authority to operate the account. <p>2. Document(s) in support of identity of each of the</p> <ul style="list-style-type: none"> ➤ Authorized signatories; ➤ 5 executive committee members; ➤ Beneficial owners; <ul style="list-style-type: none"> ○ National ID Card; or ○ Valid Passport; or ○ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/City Corporation/Union Parishad/Embassy/Cantonment Board. <p>3. Photograph of the</p> <ul style="list-style-type: none"> ➤ Each authorized signatories; ➤ 5 executive committee members; ➤ Beneficial Owner; <p>4. Document(s) in support of identity each of the</p> <ul style="list-style-type: none"> ➤ Entity; ➤ Authorized signatories; 	<p>source;</p>
Educational Institute (School/College/Madrasah/University)	<p>1. Document(s) in support of identity and operation of the entity:</p> <ul style="list-style-type: none"> ➤ Formation document ➤ Certificate of registration/permission document issued under relevant Acts or by competent authority (such as Ministry of Education/ UGC / Ministry of Religious Affairs / Relevant Govt. Authority). ➤ Serial number & date pertaining to 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certified by a professional accountant; ➤ Other bank statement (if any); Valid Trade License (as applicable); ➤ E-TIN; ➤ Cash flow statement;VAT






CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<p>certificate issued from local authority such as UNO, Union Parishad Chairman, Ward commissioner etc.)</p> <ul style="list-style-type: none"> ➤ Information of executive committee/management committee/governing body; ➤ Resolution of the executive committee/management committee/directors to open account, and ➤ Identification of those who have authority to operate the account; ➤ Educational Institution Identification Number (Optional) <p>2. Document(s) in support of identity of each of the</p> <ul style="list-style-type: none"> ➤ Authorized signatories; ➤ Governing body/EC member; ➤ Beneficial Owners; <ul style="list-style-type: none"> ○ National ID Card; or ○ Valid Passport; or ○ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/City Corporation/ Union Parishad/Embassy/ Cantonment Board. <p>3. Photograph of</p> <ul style="list-style-type: none"> ➤ Each authorized signatory; ➤ Governing body/EC member; ➤ Beneficial Owner; <p>4. Document in support of address of the</p> <ul style="list-style-type: none"> ➤ Entity; ➤ Authorized Signatories; 	<p>registration/BIN;</p> <ul style="list-style-type: none"> ➤ Bank loan documents (if any); Donation/ Subscription/ Foreignor Local Aid; ➤ Government/Other Specific approved Fund; ➤ Tax payment proof document issued by competent authority; Any other documents of legal source, etc.
<p>Trusts, Foundations or Similar Entities</p>	<p>1. Document(s) in support of identity and operation of the entity:</p> <ul style="list-style-type: none"> ➤ Bye-laws (certified copy); ➤ Certified true copy of the Trust Deed; ➤ Certificate of registration issued by competent authority (if any); ➤ Information of the executive committee/management committee/directors/ trustee board; 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certified by a professional (if registered); ➤ Other bank statement; Detail of donation (if any); <ul style="list-style-type: none"> ○ Form for foreign remittance (As & when remittance is received);



CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<ul style="list-style-type: none"> ➤ Power of attorney allowing transaction in the account; ➤ Registration Certificate from Regulatory/Competent Authority; ➤ Resolution to open account, and Identification of those who have authority to operate the account; ➤ Serial number & date pertaining to certificate issued from local authority such as UNO, Union Parishad Chairman etc. (Optional) <p>2. Document(s) in support of identity of each of the</p> <ul style="list-style-type: none"> ➤ Authorized signatories; ➤ Members of trustee board; ➤ Beneficial owners: <ul style="list-style-type: none"> a) National ID Card; or b) Valid Passport; or c) Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/ City Corporation/Union Parishad/ Embassy/ Cantonment Board (Please see note 2). <p>3. Photograph of</p> <ul style="list-style-type: none"> ➤ Each authorized signatory; ➤ Members of trustee board; ➤ Beneficial owner. <p>4. Document in support of address of the</p> <ul style="list-style-type: none"> ➤ Entity ➤ Authorized Signatories <p>5. In case of Turst Cum Settlement Account, follow "Guidelines for Trust Fund Management in payment and settlement service".</p>	<ul style="list-style-type: none"> ○ Certificate of grand/ Aid.
<p>Bank and Financial Institutions</p>	<p>1. Document(s) in support of identity and operation of the company:</p> <ul style="list-style-type: none"> ➤ Valid Trade License; ➤ Certificate of incorporation; ➤ Certificate of commencement of business; ➤ Memorandum and articles of association; 	<ul style="list-style-type: none"> ➤ A copy of last available financial statements duly certified by a professional accountant; ➤ Bank loan documents (if any); ➤ Valid Trade License; ➤ E-TIN; ➤ Other bank account; ➤ VAT registration/BIN;





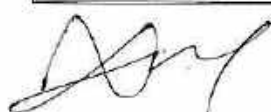

CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<ul style="list-style-type: none"> ➤ Updated list of directors with ownership structure (Form XII + Form X); ➤ Global Intermediary Identification Number (GIIN); ➤ Resolution of the board of directors To open account; ➤ Of those who will operate the account; ➤ Power of attorney/mandate granted to its managers, officials or employees to transact business on its behalf; ➤ E-TIN; ➤ VAT registration number. <p>2. Document(s) in support of identity of each of the</p> <ul style="list-style-type: none"> ➤ Authorized signatories; ➤ Top 5 Directors in terms of shareholding ➤ Beneficial owners: ➤ National ID Card; or ➤ Valid Passport; or ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/ City Corporation/Union Parishad/ Embassy/ Cantonment Board (Please see note 2). <p>3. Photograph of</p> <ul style="list-style-type: none"> ➤ Each authorized signatory ➤ Top 5 directors in terms of shareholding ➤ Beneficial owner (to be identified as per the SOP on identification & due diligence for BO) <p>4. Document in support of address of the -</p> <ul style="list-style-type: none"> ➤ Entity ➤ Authorized signatories 	<ul style="list-style-type: none"> ➤ Tax payment proof document issued by competent authority; ➤ Cash flow statement; ➤ Any other documents of legal source, etc.
<p>Embassies/ Missions/High</p>	<ul style="list-style-type: none"> ➤ Appointment letter/transfer order of the high commissioner/ambassador/expatriate employee; ➤ Copy of permit as diplomat/expatriate employee from foreign ministry of Bangladesh; ➤ Copy of Valid Passport with visa of the individual(s) who is/are the operator or 	<p>N/A</p>

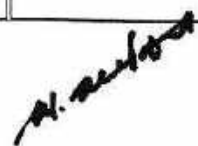


CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
Commissions (Private Foreign Currency Account, Convertible Taka Account)	<ul style="list-style-type: none"> signatory of account; ➤ Photographs of operator/signatory (duly attested); ➤ Approval/Authorization letter for opening FC account in official pad of the Embassy/Mission mentioning the name and designation of the signatory/operator of the account with his/her specimen signatures; ➤ Other relevant document(s) in support of opening account. 	
Expatriate employees of Embassy/Missions (Private Foreign Currency Account, Convertible Taka Account)	<ul style="list-style-type: none"> ➤ Copy of Valid Passport of individual with visa for staying in Bangladesh; ➤ Appointment letter/transfer order of high commissioner, ambassador/expatriate employee; ➤ Approval/authorization letter for opening FC account in official pad of the Embassy/Mission mentioning the name and designation of the signatory/ operator of the account with his/her specimen signature; ➤ Photographs of <ul style="list-style-type: none"> ○ Account holder (duly attested) ○ Nominee (duly attested) ➤ QA-22 Form (as per FEX guideline) Note: Expatriate employees of the Embassies/Missions/High Commissions may also open savings account for with drawing their money in local currency. 	N/A
Foreign National-Individual	<p>1. Document(s) in support of identity of the applicant(s), nominee(s), beneficial owner(s) and mandatee (if any):</p> <ul style="list-style-type: none"> ➤ National ID Card; or ➤ Valid Passport with visa page (as applicable); or ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/ City Corporation/Union Parishad/ Embassy/ Cantonment Board (Please see note 2). 	<ul style="list-style-type: none"> ➤ Work permit; ➤ Employment Certificate with salary from the employer; ➤ Self-declaration acceptable to the bank. (commensurate with declared occupation); ➤ Documents in support of (if any); ➤ Other bank statement (if any); Document of foreign remittance (if any fund comes from outside the country).



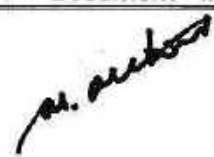
CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<p>2. Photograph of</p> <ul style="list-style-type: none"> ➤ Applicant(s) (attested by introducer) Nominee(s) (attested by applicant) Beneficial owner (attested by applicant) <p>3. Document in support of address</p> <p>4. Form QA-22</p> <p>5. Documents in support of stay in Bangladesh</p> <p>6. Any other document as in the PPG and circulars (if any) of the relevant division of PBL.</p>	
<p>Foreign National - Firm/ Company/ Joint Venture Contracting</p>	<p>1. Form QA-22;</p> <p>2. Documents in support of registration in Bangladesh issued by-</p> <ul style="list-style-type: none"> ➤ Registrar of Joint Stock Companies and Firms (RJSC); and following as applicable: <ul style="list-style-type: none"> ➤ Bangladesh Investment Development Authority (BIDA); or ➤ Bangladesh Economic Zones Authority (BEZA); or ➤ Bangladesh Export Processing Zones Authority (BEPZA); or ➤ Export Processing Zone (EPZ); or ➤ Any other competent authority (if any). <p>3. Document(s) in support of identity and operation of the entity (as applicable):</p> <ul style="list-style-type: none"> ➤ Joint venture contract Memorandum and Articles of Association/Deed of Partnership/ Bye-laws; ➤ Service Contract/Appointment Letter/Work Permit, if any, for operation of the account; ➤ Resolution: <ul style="list-style-type: none"> • To open account • Regarding authority to operate the account; ➤ List of authorized signatories and members of the governing bodies/management committee (as applicable); ➤ In case the signatory(ies)/ beneficial owner(s) is/are 	<ul style="list-style-type: none"> ➤ A copy of last available; financial statements duly certified by a professional accountant; ➤ Other bank statement; ➤ E-TIN; ➤ Certificate of grant / aid; ➤ FIRC (Foreign Inward Remittance Certificate); from BIDA/work permit; ➤ Declaration in "C" Form for foreign remittance (As & when remittance is received); ➤ Any other documents of legal source;



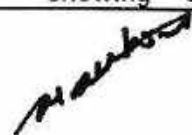
CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<p>foreigner, Valid Passport with visa page and work permit, as applicable;</p> <ul style="list-style-type: none"> ➤ In case, the signatory(ies)/beneficial owner(s) is/are Bangladeshi, document(s) in support of identity (NID/Valid Passport/Birth Registration + any other photo ID acceptable to the bank, if photo ID not available, then certificate from respectable person); ➤ Photographs of the signatory(ies) and beneficial owner(s); ➤ Permission number & date from Bangladesh Bank for foreign company/ firm Chamber of Commerce & Industry Certificate No. & Date 	
<p>Customers, Who Want to Open Non-Resident Bangladeshi (NRB) Account</p>	<p>1. Document(s) in support of identity of the applicant(s), nominee(s), beneficial owner(s) and mandate (if any):</p> <ul style="list-style-type: none"> ➤ National ID Card; or ➤ Valid Passport with arrival seal page (as applicable); or ➤ Valid Passport with visa; ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/ City Corporation/Union Parishad/ Embassy/ Cantonment Board. <p>2. Photograph of</p> <ul style="list-style-type: none"> ➤ Applicant(s) (attested by introducer, if applicable); ➤ Nominee(s) (attested by applicant); ➤ Beneficial owner, if any (attested by applicant). <p>3. Document in support of address</p> <p>Documents in support of staying abroad-</p> <ul style="list-style-type: none"> ➤ Work Permit ➤ Residence Permit ➤ Any other document in support of stay 	<ul style="list-style-type: none"> ➤ Employee ID (For ascertaining level of employment); ➤ Self-declaration acceptable to the bank. (commensurate with declared occupation); ➤ Documents in support of (if any); ➤ Documents of foreign remittance (if any)/FMJ form (as applicable); ➤ Overseas bank statement; ➤ Tax payment proof document issued by competent authority.
	<p>1. Document(s) in support of identity of</p>	<ul style="list-style-type: none"> ➤ Document in support of the



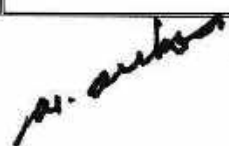
CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
Minor	<p>the minor(s), guardian(s), nominee(s) and beneficial owner(s) (if any):</p> <ul style="list-style-type: none"> ➤ National ID Card; or ➤ Valid Passport; or ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/ City Corporation/UnionParishad/ Embassy/ Cantonment Board <p>2. Photograph of</p> <ul style="list-style-type: none"> ➤ Minor(s) (attested by introducer); Guardian(s) (attested by introducer, if applicable); ➤ Nominee(s) (attested by guardian); Beneficial owner, if any (attested by guardian). <p>3. Guardianship certificate issued by competent court (if appointed by the court).</p>	<p>source of fund (as applicable); e.g. Income of parents Self-declaration acceptable to the bank. (commensurate with source of fund);</p> <ul style="list-style-type: none"> ➤ Documents in support of (if any).
Executors, Administrators, Correspondent Bank or Exchange House	<ul style="list-style-type: none"> ➤ Letter of administration or probate issued by competent court (as applicable); ➤ Details of A/C operator or signatories with document(s) in support of identity (NID/Valid Passport/Birth Registration Certificate + any other photo document acceptable to bank, if photo document is not available, certificate from respectable person); ➤ Photograph of the Executor/Administrator. ➤ Information to be obtained in the format provided by Bangladesh Financial Intelligence Unit (BFIU) and required documents. 	
Individual Customer, who wants to Open NITA	<p>1. Document(s) in support of identity of the applicant(s), nominee(s) beneficial owner(s) and mandatee(if any):</p> <ul style="list-style-type: none"> ➤ Valid Passport with arrival seal page (as applicable); or ➤ Valid Passport including the signature page with other relevant pages to be duly attested by the concerned authority(ies), i.e. Bangladesh Embassy/Bangladesh 	<ul style="list-style-type: none"> ➤ Copy of employer certificate/ work permit/ I-20 duly attested by the concerned authority(ies); ➤ Documents in support of income such as pay slip, bank statement etc.; ➤ In case the applicant is a businessman, documents showing existence of the



CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<p>High Commission/Notary Public of the concerned countries/Bank who have correspondent relationship with PBL;</p> <p>2. Photograph of</p> <ul style="list-style-type: none"> ➤ Applicant(s) (attested by introducer); ➤ Nominee(s) (attested by applicant); ➤ Beneficial owner, if any (attested by applicant). <p>3. Document in support of address.</p> <p>4. For NRBs, documents in support of staying abroad-</p> <ul style="list-style-type: none"> ➤ Work permit. ➤ Residence permit; ➤ Any other document in support of stay 	<p>business and business income;</p> <ul style="list-style-type: none"> ➤ Tax payer certificate by client's local authority; ➤ Documents in support of beneficial owner's income (as applicable).
<p>Non-individual Customers, Who Want to Open NITA</p>	<ul style="list-style-type: none"> ➤ Document(s) in support of identity and operation of the entity: ➤ Business license (as applicable) Certificate of incorporation; ➤ Memorandum and articles of association; ➤ List of directors; ➤ Resolution <ul style="list-style-type: none"> • To open account • Regarding authority to operate the account; ➤ Power of attorney granted to its managers, officials or employees to transact business on its behalf; ➤ Document(s) in support of identity of each of the <ul style="list-style-type: none"> ➤ Authorized signatories ➤ Beneficial owners; ➤ National ID Card; or ➤ Valid Passport with arrival seal page (as applicable); or ➤ Valid Passport including the signature page with other relevant pages to be duly attested by the concerned authority(ies), i.e. Bangladesh Embassy/ Bangladesh High Commission/ Notary Public of the concerned countries/ Bank who has correspondent relationship with PBL or 	<ul style="list-style-type: none"> ➤ Company tax certificate from local authority; ➤ A copy of last available financial statements duly certified by a professional accountant; ➤ Bank statement; ➤ Documents in support of beneficial (as applicable); ➤ Any other documents acceptable to the bank as proof of source of fund.

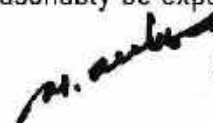


CustomerType	Indicative List of Standard Documents	Indicative List of Documents for Verification of Profession, Nature of Business and Sources of Funds
	<ul style="list-style-type: none"> ➤ Birth Registration Certificate (with seal & signature) issued by competent authority such as Municipality/ City Corporation/ Union Parishad/ Embassy/ Cantonment Board. ➤ Photograph of ➤ Each authorized signatories; ➤ Beneficial owner (to be identified as per the SOP on identification & due diligence for BO); ➤ Document in support of address of the ➤ Entity; ➤ Authorized Signatories 	

- 1.4. BAMLCO/GB In-Charge is the authorized official to verify/approve and update customer information during account opening and operation of the account. However, in absence of BAMLCO/GB In-Charge the Branch Manager will perform the role of BAMLCO/GB In-Charge.
- 1.5. Beneficial Owner's form has to be filled in for each beneficial owner (if and as applicable) and KYC of Beneficial Owner has to be completed.
- 1.6. If a customer wants to authorize another person to operate an account on his/her behalf, duly signed mandate form has to be obtained. In addition, complete and accurate information of mandate holder have to be obtained and preserved.
- 1.7. PSD Circular No 07 regarding distribution of cash received from the value declared products/parcels of the licensed Courier Services through banking channel has to be followed for any entity involved in courier service business that has a postal department license and is a member of the Courier Service Association.
- 1.8. Obtaining FATCA status declaration from each customer (including beneficial owner) is mandatory. If an individual customer is found to be the US person, obtain copy of passport/proof of being the US person, social security card and signed off form W9 from the customer in addition to the documents required to complete standard CDD. If non-individual customer or its beneficial owner is found to be the US person, communicate with the head of AML & CFT division or his/her designate. As per FATCA regulation, natural person having ownership of 10% or above in an entity will be considered as the beneficial owner of the entity.
- 1.9. **Persons without Standard Identification Documentation** - It is generally believed that financial inclusion is helpful in preventing money laundering and terrorist financing. Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do





so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous AML procedures is accepted. Internal procedures allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph. Bank shall not allow 'high value' transactions to this kind of customers.

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number. In these cases, it may be possible for the bank to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

- 1.10. **Companies Registered Abroad** - Specific measures should be taken when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, bank should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh's. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.
- 1.11. **Powers of Attorney/Mandates to Operate Accounts** - The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.
- 1.12. **Timing and Duration of Verification** - The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed. However, if it is necessary for sound business reasons to open an account or





carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority. This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is in itself suspicious.

- 1.13. **Risk Categorization- Based on Activity/KYC Profile** - When opening accounts, the concerned officer must assess the risk that the accounts could be used for "money laundering", and must classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form given in Annexure- 2 of BFIU circular No. 26 dated 16.06.2020 in which following six risk categories are scored using a scale of 1 to 5 where summation of Risk Score +15 denotes denotes High Risk, and less than 15 denotes Low Risk:

- 1.13.1. Product /Services type & channel Risk
- 1.13.2. Geographical Risk
- 1.13.3. Business or Occupational Risk
- 1.13.4. Relational Risk
- 1.13.5. Transactional Risk
- 1.13.6. Transparency related Risk

- 1.14. KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for "High Risk" accounts (as defined above). For "Low Risk" transactional accounts KYC Profiles and Transaction Profiles must be updated and re-approved in every five (5) years. These should, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern. Bank shall also update any account when deemed necessary.
- If a person deposits or withdraws money from an account which is maintained with other branch through online banking, the branch must obtain KYC of depositors/ withdrawer as per format provided & preserve record one copy in a file & another with the voucher.

Transaction Monitoring Process

- 1.15. **Transaction Monitoring Process**

- 1.15.1. Financial Institutions are expected to have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for Financial Institutions to be vigilant for any significant changes or inconsistencies in the pattern of




transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the customer. Possible areas to monitor could be: -

- a) transaction type
- b) frequency
- c) unusually large amounts
- d) geographical origin/destination
- e) changes in account signatories

- 1.15.2. It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions.
- 1.15.3. Monitoring of account transaction AML software was introduced and branch has to monitor the transaction by the system.
- 1.15.4. Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be declared in a Transaction Profile (TP) at the time of opening account from the customer. Ideally any deviation from the normally expected TP should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account.
- 1.15.5. It may not be feasible for some institutions or specific branches of institutions having very large number of customers to track every single account against the TP where a risk based approach should be taken for monitoring transactions based on use of "Customer Categories" and "Transaction Limits" (individual and aggregate) established within the branch. The Customer Category is assigned at account inception - and may be periodically revised - and is documented on the Transaction Profile. Transaction Limits are established by the business subject to agreement by BAMLCO. The Customer Categories and Transaction Limits are maintained in the manual ledgers or computer systems.
- 1.15.6. On a monthly basis Branch/ concerned unit of the financial institution must prepare an exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer based on Anti-Money Laundering risk assessment exercise.
- 1.15.7. Account Officers/Relationship Managers or other designated officer will review and sign-off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer. The concerned officer will document their review by initial on the report, and where necessary will prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the relevant Branch Manager and review with the BAMLCO. A copy of the transaction identified will be attached to the SARs.



CHAPTER IX: TRADE BASED MONEY LAUNDERING**Introduction**

In general, there are three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy.

- 1.1. The first involves the movement of value through the financial system using methods such as cheques and wire transfers;
- 1.2. The second involves the physical movement of bank notes using methods such as cash couriers and bulk cash smuggling; and
- 1.3. The third involves the movement of value using methods such as the false documentation and declaration of traded goods and services.

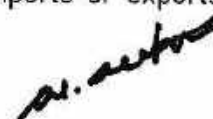
Each of these methods involves the movement of enormous volumes of funds and can operate at a domestic or international level. Research has shown that when governments take action against certain methods of money laundering or terrorist financing, criminal activities tend to migrate to other methods. In part, this reflects the fact that more aggressive policy actions and enforcement measures increase the risk of detection and therefore raise the economic cost of using these methods.

This suggests that the FATF's recent actions to revise the 40 Recommendations on money laundering and extend the 8 Special Recommendations on terrorist financing to cover cash couriers, as well as the ongoing efforts of countries to implement these stricter standards, may have the unintended effect of increasing the attractiveness of the international trade system for money laundering and terrorist financing activities.

Definition & Process

- 2 FATF defined trade-based money laundering (TBML) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover,



trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

Money launderers can move money out of one country by simply using their illicit funds to purchase high-value products, and then exporting them at very low prices to a colluding foreign partner, who then sells them in the open market at their true value. To give the transactions an air of legitimacy, the partners may use a financial institution for trade financing, which often entails letters of credit and other documentation.

The International Trade System

- 3 The international trade system is subject to a wide angle of risks and vulnerabilities, which provide criminal organizations with the opportunity to launder the proceeds of crime and provide funding to terrorist organisations, with a relatively low risk of detection. The relative attractiveness of the international trade system is associated with:
- 3.1. The enormous volume of trade flows, which obscures individual transactions and provides abundant opportunity for criminal organisations to transfer value across borders;
 - 3.2. The complexity associated with (often multiple) foreign exchange transactions and recourse to diverse financing arrangements;
 - 3.3. The additional complexity that can arise from the practice of commingling illicit funds with the cash flows of legitimate businesses;
 - 3.4. The limited recourse to verification procedures or programs to exchange customs data between countries; and
 - 3.5. The limited resources that most customs agencies have available to detect illegal trade transactions.

On this last point, research suggests that most customs agencies inspect less than 5 percent of all cargo shipments entering or leaving their jurisdictions. In addition, most custom agencies are able to direct relatively limited analytical resources to improve targeting and identification of suspicious trade transactions.

In recent decades, international trade has grown significantly. Much of this trade is associated with the financial system, as a significant amount of goods and services are financed by banks and other financial institutions.

In industrial countries the growth of trade has significantly exceeded the growth of gross domestic product, while in developing countries it has increased even faster. In addition, virtually all economies have become more open to trade. This has placed increasing pressure on the limited resources that most countries, especially developing countries, have available to scrutinise these activities.

Trade Based Money Laundering



- 4 Trade-based money laundering involves the proceeds of crime, which are more difficult to track. A number of authors and institutions, including Baker (2005), de Boyrie, Pak and Zdanowicz (2005), the Department of Homeland Security, US Immigration and Customs Enforcement (2005), have recently examined a range of other methods used to launder money through the international trade system as well as the scope that jurisdictions have to identify and limit these activities.

Basic Trade-Based Money Laundering Techniques

- 5 Trade-based money laundering is defined as the purpose of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin⁴. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include;

- 5.1. **Over- and under-invoicing of goods and services-** Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest methods of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

5.1.1 **Over-invoicing:** By invoicing the goods or service at a price above the fair market price, the seller is able to receive value from the buyer (i.e., the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market).

5.1.2 **Under-invoicing:** By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer (i.e., the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market).

5.1.3 The over- and under-invoicing of exports and imports can have significant tax implications. An exporter who over- invoices the value of the goods that he ships may be able to significantly increase the value of the export tax credit (or valued-added tax (VAT) rebate) that he receives. Similarly, an importer who is under-invoiced for the value of the goods that he receives may be able to significantly reduce the value of the import duties (or customs taxes) that he pays. Both of these cases illustrate the link between trade-based money laundering and abuse of the tax system.

- 5.2. **Multiple invoicing of goods and services -** Another technique used to launder funds involves issuing more than one invoice for the same international trade

⁴ FATF*GAFI, Financial Action Task Force.



transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions.

In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there are a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees. Unlike over- and under-invoicing, it should be noted that this is no need for the exporter or importer to misrepresent the price of the good or service on the commercial invoice.

- 5.3. **Over- and under-shipments of goods and services-** overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so-called "phantom shipment" are routinely processed.

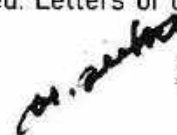
5.3.1 **Falsely described goods and services-** an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the tradeservices, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

5.3.2 **Ghost-shipping-** Fictitious traders where a buyer and seller collude to prepare all the documentation indicating goods were sold, shipped and payments were made, but no goods were actually shipped.

All of these techniques are not necessarily in use in every country.

- 5.4. **Shell Companies** - used to reduce the transparency of ownership in the transaction.
- 5.5. **Black Market Trades** - Commonly referred to as the Black Market Peso Exchange whereby a domestic transfer of funds is used to pay for goods by a foreign importer. Letters of credit are another vehicle for money laundering. Letters of credit are a credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met. Letters of credit are commonly used to finance export because exporters want assurance that the ultimate buyer of its goods will make payment and this is given by the buyer's purchase of a bank letter of credit. The letter of credit is then forwarded to a correspondent bank in the jurisdiction in which the payment is to be made. The letter of credit is drawn on when the goods are loaded for shipping, received at the importation point, clear customs and are delivered. Letters of credit can



be used to facilitate money laundering by transferring money from a country with lax exchange controls, thus assisting in creating the illusion that an import transaction is involved. Moreover, letters of credit can also serve as a façade when laundering money through the manipulation of import and export prices. Another method of using letters of credits illicitly is in conjunction with wire transfers to bolster the legitimate appearance of non- existent trade transactions.

Red Flag Indicators

5.6. Trade Based Money Laundering "Red flag" Indicators - Although Trade Based Money Laundering is extremely difficult to monitor, track and identify, there are common situational or behavioral indicators, or "Red Flags", that Banks should be aware of:

- 5.6.1 Customers→ Is the nature of each trade consistent with the customer's business?
- 5.6.2 Countries→ Is the buyer, seller, vessel or bank involved in the trade on a sanctions list?
- 5.6.3 Goods→ Is there potential for tax avoidance or money laundering?
- 5.6.4 Documentation and Products→ Is there complete, accurate and precise documentation for each trade?

Red flags may be present in every step of the Trade finance process and should be promptly examined. Although it is not necessarily an indicator of criminal activity, the presence of a Red flag requires thorough investigation, in order to properly determine if unlawful acts were committed.


Sl. No	Category	Red Flag Indicators
1.	Customer	<ul style="list-style-type: none"> • The transaction involves the receipt of cash (or by other payment methods) from third party entities that have no apparent connection with the transaction or which involve front or shell companies or wire instructions/ payment from parties which were not identified in the original letter of credit or other documentation. The transactions that involve payments for goods through cheques, bank drafts or money orders not drawn on the account of the entity that purchased the items also need further verification. • A client uses unusual or suspicious identification documents that cannot be readily verified. • A business is reluctant, when establishing a new trade relationship, to provide complete information about the nature and purpose of its business, anticipated trade activity, prior banking relationship, the names of its officers and directors or information on its business location. • A client's home or business telephone is disconnected. • The client's background differs from that which would be expected on the basis of his or her business activities. • A party to a transaction is a shell company. • Transacting businesses share the same address, provide only registered agent's address or have other address inconsistencies.

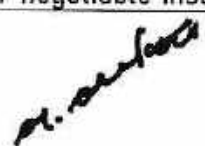





or auto

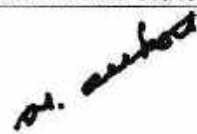
SL No	Category	Red Flag Indicators
		<ul style="list-style-type: none"> • Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets. • A client who significantly deviates from their historical pattern of trade activity (i.e. in terms of value, frequency or merchandise). • The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy (e.g. a steel company that starts dealing in paper products or an information technology company that starts dealing in bulk pharmaceuticals). • Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions(e.g. equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems or certain natural resources such as metals, ore and crude oil). • The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations. • The customer exhibits a lack of concern regarding risks, commissions or other transaction costs. • The customer has little experience in the product in which they are dealing or does not seem to appreciate the risks associated. • The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements. • Excessive insistence of the customer to complete the transaction quickly. • Transactions which are between parties controlled by the same business entity.
2	Countries	<ul style="list-style-type: none"> • Use of letter of credit to move money between those countries, where such trade would not normally occur and or is not consistent with customer's usual business activity. A letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts. • The method of payment requested by the client appears inconsistent with the risk characteristics of the transaction. For example receipt of an advance payment, for a shipment, from a new seller in a high- risk jurisdiction. • Shipment locations of the goods, shipping terms or descriptions of the goods are inconsistent with letter of credit. This may include changes in shipment locations to high risk countries or changes in the quality of the goods shipped. • Customers are conducting business in higher-risk jurisdictions or geographic locations, particularly when shipping items through higher- risk or non- cooperative countries as defined in the AML Risk Drivers. However, this attribute in isolation would not necessarily deem a transaction as high risk. • Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties also should prompt additional UN/OFAC/EU review.
3.	Transactions	<ul style="list-style-type: none"> • Unusual deposits i.e. use of cash or negotiable instruments (such as



Sl. No	Category	Red Flag Indicators
	and Goods	<p>traveller's cheques, cashier's cheques and money orders) in round denominations (to keep below reporting threshold limit) to fund bank accounts and pay for goods and services. The negotiable instruments may sequentially numbered or purchased at multiple locations and may frequently lack payee information. Further, cash payments for high -value orders are also indication of TBML activity.</p> <ul style="list-style-type: none"> • Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity are indicators for TBML. In this regard the study of foreign exchange remittances may help detect the offence. • In the case of merchant's trade, the trade finance mechanism should be in place for both export leg as well as import leg of transaction. If the trade finance mechanism, for example, Letters of Credit, have been provided for only the import leg of the transaction and not for export leg, it also indicates the possibility of TBML. • Goods or services purchased by the business do not match the customer's stated line of business. • The size of shipment appears inconsistent with the scale of the exporter or importer's regular business activities. • The goods are shipped through one or more jurisdictions or unconnected subsidiaries for no apparent economic reason. • The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with transaction. • Transport documents do not match letter of credit documents and evidence an over- shipment or under shipment not covered by the letter of credit agreement. • Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped. • Sudden and unexplained increases in a customer's normal trade transactions. • Obvious misrepresentation of quantity or type of goods imported or exported. • Obvious over or under pricing of goods and services (as per information received from our regulators, we are not expected to be pricing experts on the many products that could be involved in trade transactions. However, staff completing trade transactions should generally know that over or under pricing can be an indicator of money laundering and or fraud and any instances that come to their attention should be investigated and if suspicious reported). • Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction. • The method of payment appears inconsistent with the risk characteristics of the transaction. For example, the use of an advance payment for a shipment from a new supplier in a high risk country. • The shipment does not make economic sense. For example, the use of a forty foot container to transport a small amount of relatively low value goods. • Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the



Sl No	Category	Red Flag Indicators
		<p>organization and the other parties in the transaction.</p> <ul style="list-style-type: none"> • Additionally the shipment of any high value items (such as electronics, autos, auto parts, gems and precious metals) in conjunction with other indicators may be reason for further review. <p>Other inconsistencies to be considered;</p> <ul style="list-style-type: none"> • Routine installation, training or maintenance services are declined by the customer. • Delivery dates are vague or deliveries are planned for out of the way destinations. • A freight forwarding firm is listed as the product's final destination. • Packaging is inconsistent with the stated method of shipment or destination.
4.	Documentation and Products	<ul style="list-style-type: none"> • The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or that includes changes in regard to the beneficiary or location of payment without any apparent reason. • "Unnecessarily complex" and confusing transaction structures. These structures potentially aim to obscure a transaction's true purpose and nature. • A payment method that does not match the risk characteristics of the transaction. • Requests by exporters to take back and replace trade and shipping documents, notably if the new documents provided have been altered or issued by a different entity. • Abnormal markings on monetary instruments. • Modifications to third party documents, such as customs forms.

Preventive Measures to Combat Trade Based Money Laundering

1.1.1 Risk Assessment - The Bank shall conduct a comprehensive risk assessment of its trade finance business, taking into account the customer base, geographical locations, products offered and emerging risks if any, in determining the financial crime risks they are exposed to. The Bank shall also assess the adequacy of its risk management framework and internal controls to mitigate such risks.

The trade finance-specific risk assessment could be part of the broader risk assessment performed by the Bank at the enterprise-wide level. Such an assessment allows the bank to identify the risk areas in its trade finance activities and determine whether the controls in place are robust. The enterprise-wide risk assessment is intended to enable the bank to better understand its vulnerability to ML & TF risks, including the financial crime risks presented by its trade finance business and forms the basis for the bank's overall risk-based approach.

1.1.2 Due Diligence - The level of financial crime risks posed by customers and trade finance transactions varies based on their business, geographical locations and risk profiles. A typical trade finance transaction involves a number of different parties. The parties



n. autos

range from buyer and seller, to their respective agents, bankers and intermediaries. In general, the bank shall treat an instructing party in a trade finance transaction as their customer and conduct appropriate due diligence measures in accordance with a risk-based approach.

1.1.3 Additional Information to be obtained for Trade Finance Transactions - In addition to the customer due diligence requirements set out in the Bank, the Bank should ensure the followings:

- a) The Bank should obtain further information to assess the financial crime risks specific to a trade finance transaction.
- b) The Bank should obtain additional information on other relevant parties to a trade finance transaction, taking into account the bank's role in the transaction. The Bank should develop clear procedures on the additional information required under various circumstances for all the relevant parties, including beneficiaries of L/Cs and documentary collections, agents and third parties identified.
- c) The type and timing of the additional information obtained depend on the bank's role in the transaction and should be in line with a risk-based approach. This also applies to cases where the bank provides credit lines for, or facilities open account trades (e.g. invoice financing, pre-shipment financing, inventory financing) of its customers. Examples of such additional information are -
 - i) trading partners or counterparties of the customer (including buyers, sellers, shippers, consignees, notifying parties, shipping agents etc.)
 - ii) nature of the goods traded;
 - iii) country or countries of origin of the goods (including whether the goods originate from any sanctioned country);
 - iv) trade cycle;
 - v) flag of vessel, flag history and name history (to check whether it is related to any country in the list of sanctioned countries);
 - vi) name and unique identification number (e.g. International Maritime Organization (IMO) number) of any vessel proposed to be used (e.g. to better identify if it is ultimately owned by a sanctioned party);
 - vii) beneficial owner, commercial operator and registered owner of the vessel involve in the transaction to trace the history of former ship owners with focus on country of residence;
 - viii) port of loading, port-of-call and port of discharge (including whether the goods originate from or are sold to any sanctioned country) and the trade routes proposed to be used; and
 - ix) market prices of goods such as commodities to assess if further information should be obtained where the contract price differs significantly from the market price to mitigate financial crime risk.



The Bank should verify information obtained on a trade finance transaction (e.g. against commercial documents, transport documents and on a risk-sensitive basis, from independent or public sources) to authenticate the details of the transaction. This should also apply to cases where the bank provides credit lines for or otherwise facilitate, open account trades (e.g. invoice financing, pre-shipment financing, inventory financing) of its customers.

1.2. Additional Information to be obtained for Trade Finance Transactions that present higher financial crime risks:

If, at the initial stage or during the course of any trade finance transaction, the bank becomes aware that the transaction presents higher financial crime risks, the bank is expected to obtain information, to assess-

- 1.2.1 the transaction structure;
- 1.2.2 the ports of call, including the route of the shipment, ensuring that it appears to be logical with regard to transshipment points and the final destination;
- 1.2.3 the legitimacy of the payment flows;
- 1.2.4 the transaction against public sources of specialized data, documents or information (e.g. the International Maritime Bureau) in relation to sea transportation to verify the authenticity of the bills of lading and to confirm that the shipment has taken place; and
- 1.2.5 Whether they are dual-use goods.
- 1.2.6 In addition, the bank should conduct site visits and meetings with the instructing party, where appropriate.

Sanction Control

- 1.1. Sanction screening is a major component of transactional due diligence to ensure that the Bank is not Dealing with sanctioned individuals or entities. The Bank should perform name screening on key parties to each transaction. Besides, screening the parties to the transaction, such as the seller of the goods, bank should also screen the vessel used to transport the underlying goods, the shipping company, any agents or third parties present in the transaction and know the ports of call of the vessel for the particular transaction flow (origin port, destination port) where possible.
- 1.2. The Bank should be aware of any adverse developments pertaining to some parties (e.g. addition to list of designated individuals/entities) present in the trade finance transaction, between the inception of the trade finance transaction and submission of trade documents since there could be significant time difference during this period. Furthermore, the Bank is expected to perform sanctions screening both at the inception of the trade finance transaction and at the point of submission of the trade finance documents as some of the transactional details e.g. vessel used to transport the cargo, ports of call, may not be known at trade inception and hence would not have been screened at that



stage.

Trade Based Money Laundering Controls

1.1. Prices:

- 1.1.1 Checks on the reasonableness of invoice prices of goods/commodities against prevailing market prices (referred to as "price checks") are not only useful to mitigate credit risks; they also serve to identify potential fraud and ML & TF activities arising from over invoicing or under invoicing of transactions.
- 1.1.2 Bank should perform price checks, particularly where market prices are available, minimally on a sampling basis. Policies and procedures should be clearly set up to guide staff in performing such checks, including establishing the level of acceptable price variance and escalation procedures when significant differences in prices are identified.
- 1.1.3 Bank could consider setting different thresholds for different types of underlying goods/commodities. There should also be periodic assessments of whether the thresholds continue to be reasonable based on prevailing market prices for the goods/commodities.
- 1.1.4 Price checks should be performed by functions independent of front office so as to enhance the effectiveness of the checks and minimize conflicts of interest.
- 1.1.5 There should be guidelines in place for the selection of reference prices for the purpose of performing price checks.

1.2. Related Party Transactions:

- 1.2.1 There are inherently higher risks of fraud and financial crime associated with the financing of transactions between a customer and its related parties.
- 1.2.2 The Bank could consider implementing additional safeguards to mitigate the risks arising from related party transactions e.g. requiring documentary evidence to verify the authenticity of these related party transactions.
- 1.2.3 Bank's front office would obtain information about a customer's business and its present and future trading profile, including information on the customer's related parties and where applicable, the typical related party transactions that occur in the course of the customer's business. However, such information may not be made available to the middle or back offices for additional due diligence, such as checks on the rationale for the trade flows and pricing, to be performed on the individual transactions.
- 1.2.4 The middle office or back office staff processing the trade finance transactions would be better informed when identifying related party transactions if there is effective sharing of information between the front office, which would have collected information



on their customer's related entities as part of the customer on-boarding and regular review process and the control or operations units processing the trade transactions.

1.3. Underlying Goods Financed

- 1.3.1 Bank should formalize process to identify unusual transaction patterns that are inconsistent with the customers' profiles for further reviews and investigations. In addition to checking for inconsistencies in customers' trading patterns, bank is encouraged to check the descriptions of goods stated in the trade documents, particularly for descriptions which are unclear or worded in a foreign language. Bank should, on a best effort basis, determine whether the underlying goods financed are embargoed goods and there should be special attention paid to dual use goods.
- 1.3.2 Bank should ensure that there are effective channels for information obtained by the front office during the customer on-boarding and ongoing review processes, which should include information on typical goods the customer deals in, to be shared with the middle and back office staff. This is to facilitate checks on the underlying goods by the middle and back office staff in their day-to-day processing of transactions.
- 1.3.3 The front office should also regularly review customer transactions to check if there are any inconsistencies with the customers' profiles.

1.4. Controls over Multiple Financing of Invoices

- 1.4.1 When invoice financing facilities are granted, banks should ensure that there are proper processes and controls in place to detect if customers have submitted the same invoice for financing more than once.

1.5. Transaction Monitoring & Filing of Suspicious Transaction Reports:

- 1.5.1 Bank should ensure its transaction monitoring processes and systems are robust to enable suspicious transactions to be fluffed, investigated and escalated. Regular compliance checks, especially on transactions that were not escalated, should be performed for quality assurance purposes.
- 1.5.2 Bank should ensure that transactions suspected of being used for ML purposes are duly investigated and promptly escalated to the compliance function or senior management. If there are grounds to suspect that a customer is using trade finance to launder money, finance terrorism or facilitate proliferation financing (PF), STRs must be promptly filed. The bank should also minimally subject the customer account to enhance monitoring and consider rejecting the transaction.

1.6. Internal Escalation Procedures - Trade controls should provide clear guidance on






a good transaction review process. For example, a sample review process is outlined as follows:

- 1.6.1 "Level 1" review by trade processors with a good knowledge of international trade, customers' expected activity and a sound understanding of trade-based money laundering risks, who are responsible for assessing ML or TF or PF risks in each transaction and escalating potentially suspicious transactions. "Level 1" should be reviewed by the foreign trade in-charge of AD branch, PBL.
- 1.6.2 "Level 2" review by official with expertise able to further assess the merits of an escalation from a "Level 1" processor and the relevant suspicion itself. This official is likely to require extensive knowledge of trade-based money laundering risk and make appropriate use of third party data sources to verify key information. "Level 2" should be reviewed by foreign trade specialized official in International Division, PBL.
- 1.6.3 A "Level 3" compliance or investigation takes referrals from "Level 2" processors. This stage may conduct a further investigation to determine additional measures which may be required to mitigate a risk and whether the obligation to make a suspicious transaction report arises. Where these are unacceptable ML or TF or PF risks, Bank should not process the transaction. "Level 3" should be reviewed by the Head of International Division of Premier Bank.
- 1.6.4 Bank should tailor their own review process to their particular needs. Smaller operations are likely to require fewer stages of review due to the volumes of transactions involved and the nature of their businesses.

Policies and Procedures & Training

The Bank should regularly review the need to allocate more resources toward training to raise the awareness of officials to the financial crime risks associated with trade finance and the measures to mitigate such risks. Case Studies and relevant industry publications could be included in the training to highlight high risk areas that require more attention from officials or common typologies. Premier Bank is well-aware of trade based money laundering. Continuous training courses are arranged on "Trade Based Money Laundering" for the concerned officers working in the Foreign Exchange Desks.

Branches and Subsidiaries Situated/Located in Foreign Jurisdiction

- 1.1. Bank would confirm the implementation of Money Laundering Prevention Act-2012(amendment 2015) and Anti-Terrorism Act -2009 (Amendment 2012 & 2013) on subsidiaries and foreign branches of the bank.
 - 1.1.1 If branch or a subsidiary located abroad, for any reason fails to comply with the instructions of Money Laundering Prevention Act-2012 (amendment 2015) and Anti-Terrorism Act-2009 (Amendment- 2012 & 2013) it shall without any delay report to



such cases to AML & CFT Division mentioning the reason of the failure.

- 1.1.2 In Premier Bank, AML & CFT Division/Central Compliance Committee shall supervise the subsidiaries for proper implementation of Money Laundering Prevention Act-2012 (amendment 2015) and Anti-Terrorism Act-2009 (Amendment- 2012 & 2013). AML & CFT Division shall conduct audit & inspection of subsidiaries and foreign branches of the bank in order to comply under the BFIU circular # 26 dated 16.06.2020 & Money Laundering Prevention Act 2012 (Amendment 2015) and Anti Terrorism Act 2009 (Amendment 2012 & 2013).

CHAPTER X: RECORD KEEPING

Record keeping is an essential component of the audit trail that the Laws and Regulations seek to establish in order to assist in any financial investigation and to ensure that criminal funds which are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Branch must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

Statutory Requirement

- 1.1. The requirement contained in Section 25 (1) of Money Laundering Prevention Act, 2012, to retain complete and accurate information of customers' identification and transactions while operating an account of a customer, and to retain the records of customers' identification and transactions at least for five years after closing of relationships with the customers are essential constituents of the audit trail that the law seeks to establish.
- 1.2. According to the BFIU, Bank will have to preserve the following necessary documents at least 5 (five) years after closure of account : Domestic and foreign transaction related information and documents, collected Documents and information in the process of CDD with KYC, customer related any report or any account review related information or any banking report of overall compliance scenario⁵.
- 1.3. FATF recommendation 11 states that financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual





transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

1.3.1 The records prepared and maintained by the bank on its customer relationships and transactions should be such that:

- a) requirements of legislation and Bangladesh Bank directives are fully met;
- b) competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
- c) any transactions effected via the institution can be reconstructed;
- d) any customer can be properly identified and located;
- e) all suspicious reports received internally and those made to Bangladesh Bank can be identified; and
- f) the institution can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.
- g) 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.
- h) Records relating to transactions will generally comprise:
 - i) details of personal identity, including the names and addresses, etc. pertaining to:
 - the customer;
 - the beneficial owner of the account or product;
 - the non-account holder conducting any significant one-off transaction;
 - any counter-party;
 - ii) details of transaction including:
 - nature of such transactions;
 - volume of transactions customer's instruction(s) and authority(ies);
 - source(s) of funds;
 - destination(s) of funds;
 - book entries;
 - custody of documentation;



- date of the transaction;
- form in which funds are offered and paid out.
- parties to the transaction
- identity of the person who conducted the transaction on behalf of the customer

i) 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:

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

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

Retrieval of Records

1.1. 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 the bank, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduce and recollected without undue delay.

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

However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the



transactions relating to different customers and of identifying where the transaction took place and in what form.

1.2. Obligations Under Circulars - Under the obligations of BFIU Circular No. 26 dated June 16, 2020 -

1.2.1 All necessary information/ documents of customer's domestic and foreign transactions has to be preserved for at least 5(five) years after closing the account.

1.2.2 All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved for at least 5(five) years after closing the account.

1.2.3 All necessary information/documents of a walk-in Customer's transactions has to be preserved for at least 5 (five) years from the date of transaction.

1.2.4 Preserved information has to be sufficient for presenting as a documentary proof for the judiciary process of the offence.

1.2.5 Bank should provide all information and documents collected during CDD along with KYC procedure and information and documents of transactions as per the instruction or demand by BFIU.

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

1.3.1 The date of submission and reference of the STR;

1.3.2 The date and nature of the enquiry;

1.3.3 The authority who made the enquiry, investigation and reference; and

1.3.4 Details of the account(s) involved.

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

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

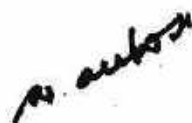
1.4.1 Details of the content of the training programs provided;

1.4.2 The names of staff who have received the training;

1.4.3 The date on which the training was delivered;

1.4.4 The results of any testing carried out to measure staffs understanding of the requirements;



1.4.5 An on-going training plan.

- 1.5. **Branch Level Record Keeping** - To ensure the effective monitoring and demonstrate their compliance with the concerned regulations, bank will ensure the keeping or availability of the following records at the branch level either in hard form or electronic form:
- 1.5.1 Information regarding Identification of the customer,
 - 1.5.2 KYC information of a customer,
 - 1.5.3 Transaction report,
 - 1.5.4 Suspicious Transaction Report generated from the branch,
 - 1.5.5 Exception report,
 - 1.5.6 Training record,
 - 1.5.7 Return submitted or information provided to the Head Office or competent authority,
 - 1.5.8 BAMLCC Meeting Minutes.
- 1.6. **Sharing of Record/Information of /To a Customer** - Under the provisions of MLPA 2012, Bank shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having approval from the court and prior approval from Bangladesh Bank.

Wire Transfer Transactions

- 1.1. Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of telegraphic transfers (TT) and electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction.
- 1.2. Following the recent focus on terrorist financing, relevant financial businesses are required to include accurate and meaningful information of originator (name, account number, and where possible address) and beneficiary (account name and/or account number) on all outgoing funds transfers and related messages that are sent, and this information should remain with the transfer or related message throughout the payment chain. Bank should conduct enhanced scrutiny of and monitor for suspicious incoming funds transfers which do not contain meaningful originator information.
- 1.3. The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a minimum of five years.

Cross Border Wire Transfer

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



- 1.2. Proper Information of applicant should be collected and preserved during Cross Border Wire Transfer of US dollar not minimum 1000 or above or equivalent any other foreign currency and send the information to the intermediary or Beneficiary Bank. Applicant account number or (Unique Transaction Reference Number) should be included in the information so that transaction can be identified in future. Moreover, Beneficiary Account Number or Unique Transaction Reference Number should be included in the beneficiary related information so that transaction can be identified in future⁶.
- 1.3. The information related to applicant and beneficiary (which is not required for verification) such as name, address etc. and account number is not present in the transaction less than the amount prescribed in Article
- 1.4. Unique Transaction Reference Number should be included so that the transaction can be identified in future⁷.
- 1.5. Where several individual transfer from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (1.11.2) above.

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

- 1.6. **STR/SAR and Investigation:** Where a FI 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 the financial institutions should maintain a register or tabular records of all investigations and inspection made by the investigating authority and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:
 - 1.6.1 the date of submission and reference of the STR/SAR;
 - 1.6.2 the date and nature of the enquiry;
 - 1.6.3 the authority who made the enquiry, investigation and reference; and
 - 1.6.4 details of the account(s) involved.

- 1.7. **Internal and External Reports - A branch should make and retain:**

- 1.7.1 records of actions taken under the internal and external reporting requirements; and
- 1.7.2 when the nominated officer has considered information or other material concerning possible money laundering but has not made a report to BFIU, a record of the other material that was considered.

⁶ Ref: Section 9.1 (1) (a) of BFIU Circular No.-26/2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)

⁷ Ref: Section 9.1 (1) (b) of BFIU Circular No.-26/2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)



1.7.3 In addition, copies of any STRs made to the BFIU should be retained for 05 (five) years. Records of all internal and external reports should be retained for five years from the date the report was made.

CHAPTER XI: TRANSACTION MONITORING & REPORTING

Reporting requirements

Reporting agencies are required by the AML/CFT legislation in Bangladesh to report to the Bangladesh Financial Intelligence Unit (BFIU). Most of such reports are derived from transaction monitoring. Such as:

Cash Transaction Report (CTR)

1.1.1. All banks are required to submit CTR to the BFIU 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/equivalent any foreign currency or more, there is no scope of treating it as suspicious only for this. However, the bank will have to report CTR to BFIU for information only.

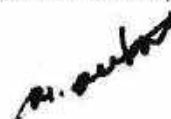
1.1.2. In the case of cash deposit (regardless of amount) of the Govt. accounts or of accounts of the Govt. owned entities need not to be reported. CTR must be submitted in soft copy. So every branch of PBL is required to submit CTR to the CCC by the 1st week of every month. After receiving such reports from every branch, Head office (CCC) will compile all the CTRs and send it to the BFIU before 21st day of every month.

Suspicious Transaction Report (STR)

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk for financial institutions. So it is necessary/essential for the safety and soundness of the institution. Generally, STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual manner. Such report is to be submitted by financial institutions to the competent authorities. In the section (2)(z) of MLP Act 2012 (amendment 2015) "suspicious transaction" means such transactions which deviates from usual transactions; of which there is ground to suspect that,

- 1.1. the property is the proceeds of an offence,
- 1.2. it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- 1.3. which is, for the purposes of this Act, any other transaction or attempt of transaction



delineated in the instructions issued by BFIU from time to time.

In Anti Terrorism Act, 2009 (amendment 2012 & 2013), STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. One important thing is that financial institutions need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion.

2. The Branches 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 PBL 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 i.e. the declared Transaction Profile (TP) of the Customer. Possible areas to monitor could be:

- 2.1. Transaction type
- 2.2. Frequency
- 2.3. Unusually large amounts
- 2.4. Geographical origin/destination
- 2.5. Changes in account signatories

3. It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. PBL 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.
4. PBL is looking for a computer system specifically designed to assist the detection of fraud and money laundering. Until the latest software is installed, PBL will continue detecting fraud and money laundering from the available information in the system.
5. Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be inputted in the Transaction Profile (TP) at the time of opening of account by the account opening officer. 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.
6. It may not be feasible for some specific branches of PBL having very large number of customers to track every single account against the TP where a risk based approach should be taken for monitoring transactions. The Customer Category is assigned at account inception - and may be periodically revised - and is documented on the Transaction Profile. Transaction Limits are established by the business subject to agreement by BAMLCO. The Customer Categories and Transaction Limits are maintained in the manual ledgers or computer systems.
7. On a periodical basis the Branch shall prepare an exception report of customers whose accounts show one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer based on Anti-Money Laundering risk assessment exercise.
8. Account Opening Officers/Relationship Managers or other designated staff will review and sign-off on such exception report of customers whose account 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 with initial on the report, and where necessary he will prepare internal Suspicious Activity Reports (SARs) with action plans approved by the Branch Manager and reviewed by the BAMLCO. A copy to of the transaction identified will be attached to the SARs.

9. BAMLCO will review the Suspicious Activity Reports (SARs) and responses from the Account opening Officers/Relationship Managers or other concerned staff. If the explanation for the exception does not appear reasonable then the Branch Manager should review the transactions prior to considering submitting them to the CAMLCO.
10. If the Branch Manager and / or BAMLCO that believes the transaction should be reported, then BAMLCO will supply the relevant details to the CAMLCO.
11. The 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 further notification has been received.
12. If, after confirming with the client, the transaction trend is to continue, the Account Opening Officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly. Attach all necessary documents with the KYC profile as the proof of the change of TP.
13. As per the Money Laundering Prevention Act 2012 (amendment 2015) FIs are obligated to submit STR/SAR to BFIU. Such obligation also prevails for the FIs in the Anti Terrorism Act, 2009 (amendment 2012 & 2013). Other than the legislation, BFIU has also instructed the FIs to submit STR/SAR through AML/BFIU Circulars issued by AMLD, Bangladesh Bank and BFIU time to time.

Reasons for Reporting of STR/SAR

14. As discussed above, STR/SAR is very crucial for the safety and soundness of the financial institutions. The Bank should submit STR/SAR considering the followings:
 - 14.1. It is a legal requirement in Bangladesh;
 - 14.2. It helps to protect the reputation of Bank(s);
 - 14.3. It helps to protect Bank(s) from unfounded allegations of assisting criminals, including terrorists;
 - 14.4. It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

Identification and Evaluation STR/SAR

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

Identification of STR/SAR

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



unusual transactions/activities may something be sourced as follows:

- 16.1. Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation.
- 16.2. By monitoring customer transactions.
- 16.3. By using red flag indicators.

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

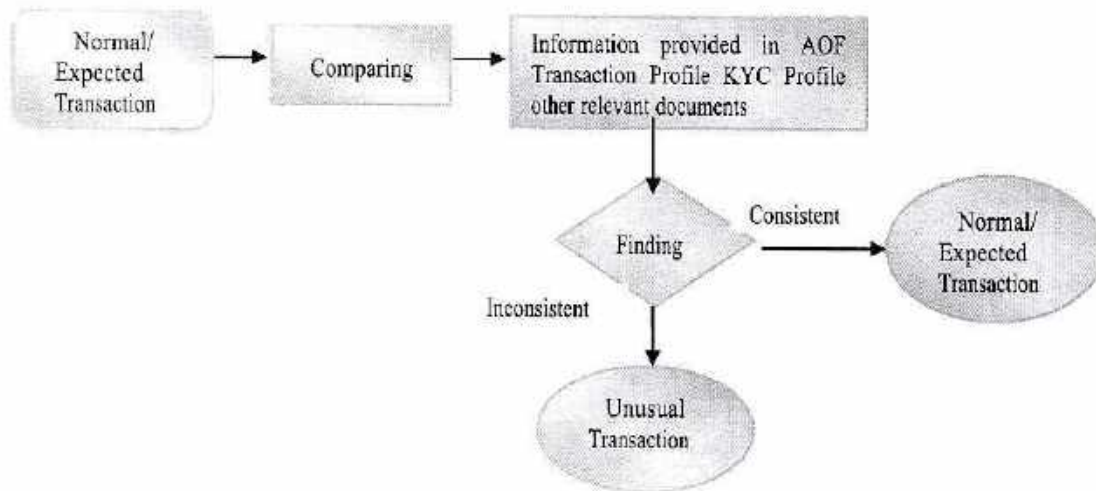


Figure: Identification of STR/SAR

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

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

16.4.2. **Evaluation** - These problems must be in place at Branch level and AML &



CFT Division. After identification of STR/SAR, at Branch level BAMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage, concerned BAMLCO must be tactful considering the tipping off provision of the acts. If BAMLCO is not satisfied, he should forward the report to AML & CFT Division. After receiving report from Branch, AML & CFT Division should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stages of evaluation (whether reported to BFIU or not) bank should keep records with proper manner.

16.4.3. Disclosure - This is the final stage and Bank(s) should submit STR/SAR to BFIU if it is still suspicious. For simplification the flow chart given below shows STR/SAR identification and reporting procedures:

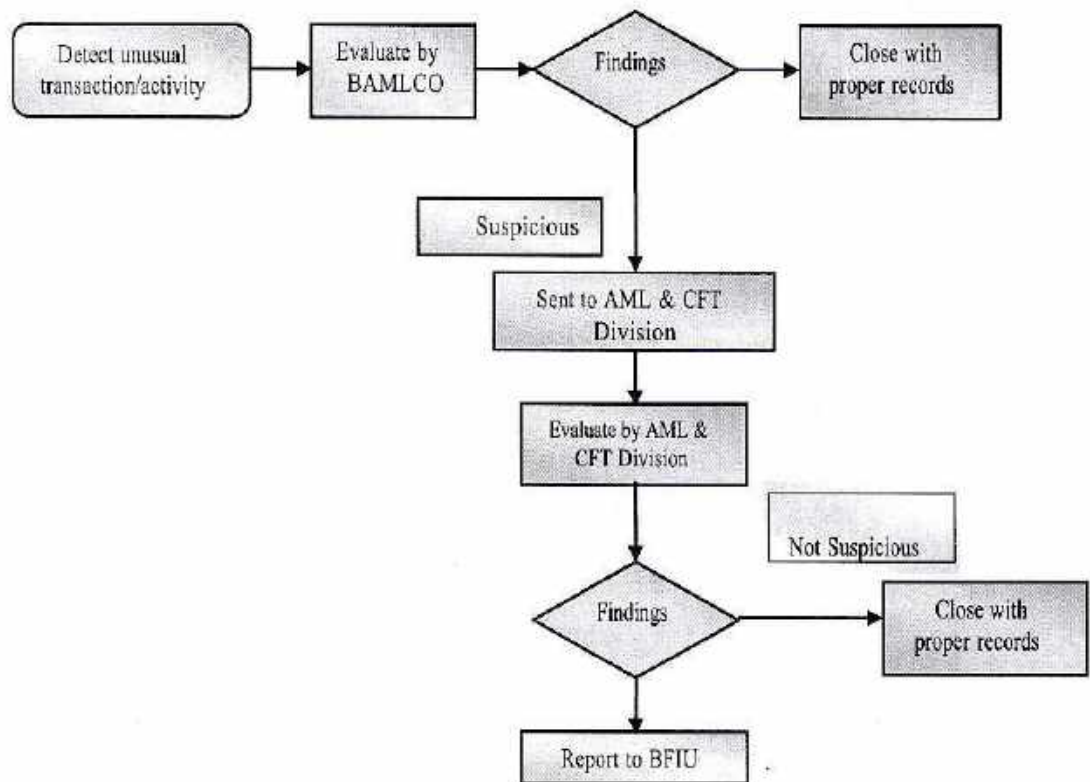


Figure: STR/SAR identification and reporting procedures

Recognition of Suspicious Transactions

17. 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

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

enough about the customer's business to recognize that a transaction, or series of transactions, is/are unusual.

- 17.1. Questions that a Branch must consider when determining whether an established customer's transaction must be suspicious are:
- 17.1.1. Is the size of the transaction consistent with the normal activities of the customer?
- 17.1.2. Is the transaction rational in the context of the customer's business or personal activities?
- 17.1.3. Has the pattern of transactions conducted by the customer changed?
- 17.1.4. Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Reporting of STR/SAR

18. Institutions enlisted as per MLP Act, 2012 (amendment 2015) and ATA, 2009 (as amended in 2012 & 2013) are obligated to submit STR/SAR to BFIU. Such report must come to the BFIU from AML & CFT Division of the respective institutions by using specified format/instruction given by the BFIU.

Suspicious Activity Reporting Process

19. Branches must establish written internal procedures so that, in the event of a suspicious activity being discovered, all staff are aware of the reporting chain and the procedures to follow. Such procedures should be periodically updated by Head Office to reflect any regulatory changes.
- 19.1. **Branch Managers** 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 BAMLCO, 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 suspicion.
- 19.2. **Where staff continues** to encounter suspicious activities on an account, which they have previously reported to the BAMLCO, they should continue to make reports to the BAMLCO 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 may be used.
- 19.3. **All reports of suspicious activities** must reach to the CAMLCO and only the CAMLCO should have the authority to determine whether a disclosure in accordance with the regulation is appropriate. However, the Branch Manager or BAMLCO can be permitted to add his comments to the suspicion report indicating any evidence as to why he/she believes the suspicion is not justified.

Transaction Monitoring Mechanism

20. As the reporting of suspicious transaction is the best tools to mitigate ML/TF risks. PBL adopt the following mechanism to indentify the suspicious transaction. BAMLCO is responsible to inplace this mechanism. The mechanisms are as follows:






- 20.1. Daily CTR (country/own limit)
 - 20.2. Report below CTR threshold.
 - 20.3. Cash activity report over a period.
 - 20.4. Threshold based transaction report.
 - 20.5. Wire transfer report (threshold/location)
 - 20.6. New a/c act. Report (periodic)
 - 20.7. Change report (periodic)
21. **Reporting Suspicious Transactions** - There is a statutory obligation for all staff to report suspicions of money laundering. The actual reporting should be made using goAML and an internal reporting will be made using the prescribed format.
22. Such unusual or suspicious transactions will be drawn initially to the attention of immediate Supervisory Officer or Branch Manager to ensure that there are no known facts that will negate the suspicion before further reporting to the CAMLCO.
23. Each Branch must have a clear instruction for the Officers and Employees to ensure:
- 23.1. That each relevant employee knows to which person they should report suspicions, and
 - 23.2. 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).
24. 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.
25. PBL Branches must refrain from carrying out transactions, which they know or suspect to be related to money laundering until they have apprised the Bangladesh Financial Intelligence Unit (BFIU). Where it is impossible in the circumstances to refrain from executing a suspicious transaction before reporting to the BFIU 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 BFIU 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.
26. 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), and will provide the liaison between the Bank and the BFIU.
27. 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.
28. He/She must take steps to validate the suspicion in order to judge whether or not a report should be submitted to BFIU. 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



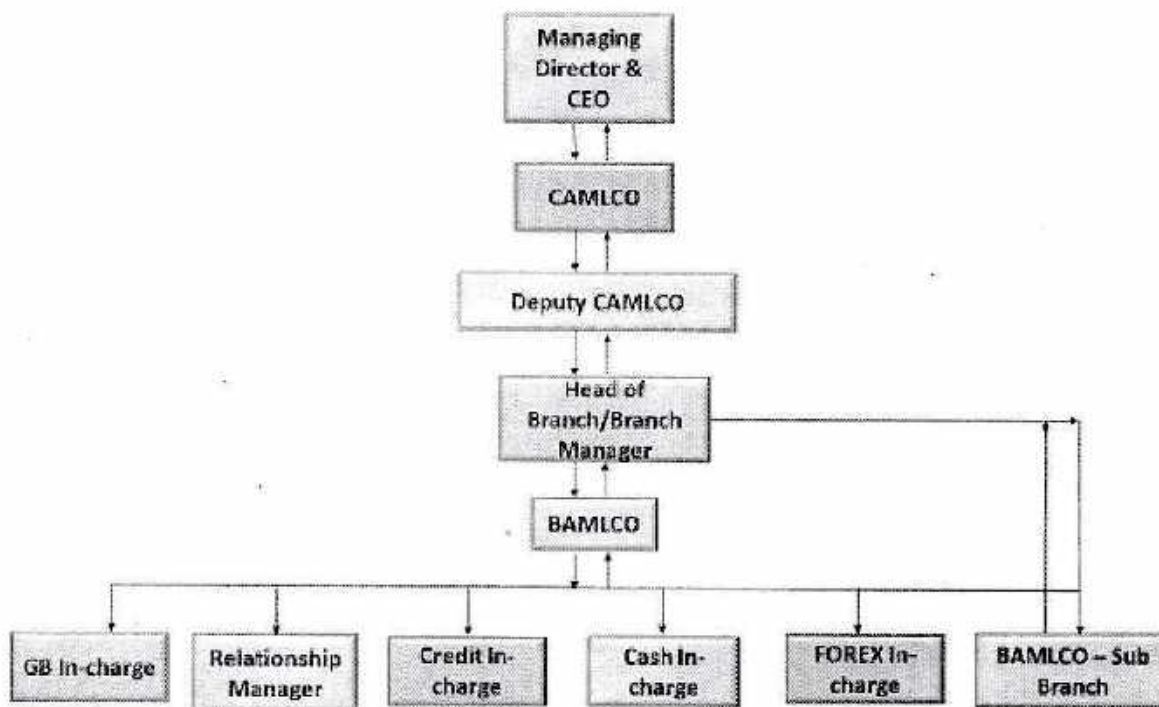
CAMLCO decides that there are no facts that would negate the suspicion, then he must disclose the information to Bangladesh Bank.

29. 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 BFIU.
30. It is therefore imperative that the CAMLCO has reasonable access to information that will enable him/her to undertake his/her responsibility. It is also important that the CAMLCO should keep a written record of every matter reported to him, whether or not the suggestion was negated or reported for his decision.
31. 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.
 Care should be taken to guard against a report being submitted as a matter of routine to BFIU without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

32. Internal Reporting Procedures and Records

Reporting Lines

33. The AML reporting line is shown as under:



34. Supervisors should also be aware of their own legal obligations. An additional fact, which the



supervisor supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the supervisor. The supervisor then has a legal obligation to report to the BAMLCO.

35. All suspicions reported to the BAMLCO should be documented (in urgent cases this may follow an initial discussion). The report should include as full details of the customer and full statement as possible as the information giving rise to the suspicion.
36. The BAMLCO 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.
37. On-going communication between the BAMLCO and the reporting person/department is important. The Bank may wish to consider advising the reporting person, department or the BAMLCO'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 BAMLCO is informed of all communication between the investigating officer and the Branch concerned at all stages of the investigation.
38. Reporting Destination - The national reception point for reporting of suspicions by the CAMLCO is:

The Director
Bangladesh Financial Intelligence Unit (BFIU)
Bangladesh Bank
Head Office Dhaka- 1000.

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

Telephone: (02) 7120659
Fax: (02) 7120371
Email: gm.bfiu@bb.org.bd

39. Sufficient information should be disclosed on the suspicious transaction, including the reason for the suspicion, to enable the investigating officer to conduct appropriate enquiries. If a particular offence is suspected, this should be stated so that the report may be passed to the appropriate investigation team with the minimum of delay. However, it is not necessary to complete all sections of the suspicious activity report form and its submission should not be delayed if particular details are not available.
40. Where additional relevant evidence is held which could be made available to the investigating officer, this should be noted on the Form.
41. Following the submission of a suspicious activity report, The Branch is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a "tipping-off" offence.
42. Self-Assessment Process - Every branch has to conduct self-assessment program aiming to identify the implementation of AML & CFT policy, rules and laws and instructions issued by BFIU. 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:

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

43. Such report should be prepared as per the checklist provided by BFIU. As per instruction, all branch of PBL will take necessary initiatives to overcome the shortcomings immediately, where necessary, Branches will seek for the help of PBL Head Office.

- 43.1. 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;
- 43.2. A sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- 43.3. A test of the validity and reasonableness of any exemptions granted by the financial institution; and
- 43.4. A test of the record keeping system according to the provisions of the Act.

44. 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.

45. **Assessment Procedure** - The procedure is based on a set of questionnaire, as attached to the BFIU circular 26, dated 16 June 2020 Annexure-Kha.

46. **Records of suspicions**, which were raised internally with the CAMLCO but not disclosed to BFIU, should be retained for five years from the date of the transaction. Records of suspicions, which the BFIU has advised are of no interest should be retained for a similar period. Records of suspicions that assist with investigations should be retained until the Bank is informed by the BFIU that they are no longer needed.

Grading of the scores

47. The following is the grade matrix based on the total score obtained through questionnaire:

Score	Grade	Number
(90+)-100	Strong	1
(70+)-90	Satisfactory	2
(55+)-70	Fair	3
(40+)-55	Marginal	4
40 & Below	Unsatisfactory	5

48. **Tipping Off** - Section 6 of MLP Act, 2012 (amendment 2015) and FATF Recommendation 21 prohibits financial institution, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the bank is seeking to perform its CDD obligation in those circumstances. The customer's awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.



- 49. Penalties of Tipping Off** - Under section 6 of MLP Act, 2012(amendment 2015) if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.
- 50. "Safe Harbor" Provisions for Reporting** - Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting financial institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLP Act, 2012(amendment 2015) provides the safe harbor for reporting.

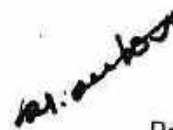
Red Flags or Indicators of STR

51. Red Flags or Indicators of STR

- 51.1. Moving Customers** - A customer who moves every month, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal, could be suspicious.
- 51.2. Out of Market Windfalls** If customer service officer think a customer who just appeared at our institution sounds too good to be true, he/she might be right. Pay attention to one whose address is far from your institution, especially if there is no special reason why he/she was given the business. Aren't there institutions closer to home that could provide the service? If the customer is a business, the distance to its operations may be an attempt to prevent from verifying there is no business after all. Do not be bullied by your sales personnel who follow the - "no questions asked" philosophy of taking in new business.
- 51.3. Suspicious Customer Behavior**
- 51.3.1. Customer has an unusual or excessively nervous demeanor.
- 51.3.2. Customer discusses the institution's record-keeping or reporting duties with the apparent intention of avoiding them.
- 51.3.3. Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- 51.3.4. Customer is reluctant to proceed with a transaction after being told it must be recorded.
- 51.3.5. Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- 51.3.6. Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- 51.3.7. Customer who is a student uncharacteristically transacts large sums of money.
- 51.3.8. Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

51.4. Suspicious Customer Identification Circumstances



- 51.4.1. Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- 51.4.2. Customer is unwilling to provide personal background information when opening an account.
- 51.4.3. Customer's Business address is outside the bank's service area.
- 51.4.4. Customer asks many questions about how the financial institution disseminates information about the identification of a customer.
- 51.4.5. A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

51.5. Suspicious Cash Transactions

- 51.5.1. Customer opens several accounts in or more names, then makes several cash deposits under the reporting threshold.
- 51.5.2. Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.
- 51.5.3. Corporate account has deposits and withdrawal primarily in cash than cheques.

51.6. Suspicious Non-Cash Deposits

- 51.6.1. Customer deposits large numbers of consecutively numbered money orders or round figure amounts.
- 51.6.2. Customer deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business.
- 51.6.3. Funds out of the accounts are not consistent with normal business or personal items of the account holder.
- 51.6.4. Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

51.7. Suspicious Activity in Credit Transactions

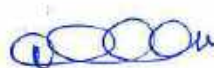
- 51.7.1. A customer's financial statement makes representations that do not conform to accounting principles.
- 51.7.2. Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- 51.7.3. Customer purchases certificates of deposit and uses them as collateral for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

51.8. Suspicious Commercial Account Activity

- 51.8.1. Business customer presents financial statements noticeably different from those of similar businesses.
- 51.8.2. Large business presents financial statements that are not prepared by an account.

51.9. Suspicious Employee Activity

- 51.9.1. Employee exaggerates the credentials, background or financial ability and



resources of a customer in written reports the bank requires.

- 51.9.2. Employee frequently is involved in unresolved exceptions or recurring exceptions on exception reports.
- 51.9.3. Employee lives a lavish lifestyle that could not be supported by his/her salary.
- 51.9.4. Employee frequently overrides internal controls or establishes approval authority or circumvents policy.

51.10. Suspicious Activity in an FI Setting

- 51.10.1. Request of early encashment
- 51.10.2. A DPS (or whatever) calling for the periodic payments in large amounts.
- 51.10.3. Lack of concern for significant tax or other penalties assessed when cancelling a deposit.



CHAPTER XII: EDUCATION, TRAINING, & AWARENESS**Statutory Controls****FATF recommendation for Employee Awareness & Training**

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 the bank's policy, procedures, and controls affect them in their day to day activities. BFIU ensures that employees of all financial institutions and other institutions engaged in financial activities have adequate training in order to combat money laundering. Therefore, as per BFIU circular, Banks have to arrange training sessions for their respective employees to ensure proper education on prevention of Money laundering and Terrorist Financing⁸ including Refresher Training Programme on AML & CFT covering all Executives/Officers and the process will be continuing.
- 1.1 **The need for Employees Awareness:** The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the serious nature of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to cooperate fully and to provide a prompt report of any suspicious transactions/activities. It is, therefore, important that bank introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.
- 1.2 **Education and Training Program:** 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

Ref.: Section 11.2.1 of BFIU Circular No.-25//2020 dated 16-05-2020 of Bangladesh Financial Intelligence Unit (BFIU)



the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the bank itself. Some sorts of high-level general awareness raising training are, therefore, also suggested by the Central Bank.

- 1.3 **General Training:** A general training program of the bank should include the following:
- 1.3.1 General information on the risks of money laundering schemes, methodologies, and typologies;
 - 1.3.2 Legal framework, how AML related laws apply to the bank and its employees;
 - 1.3.3 Bank's policies and systems with regard to customer identification and verification, due diligence, monitoring;
 - 1.3.4 How to react when faced with a suspicious client or transaction;
 - 1.3.5 How to respond to customers who want to circumvent reporting requirements;
 - 1.3.6 Stressing the importance of not tipping off clients;
 - 1.3.7 Suspicious transaction reporting requirements and process;
 - 1.3.8 Duties and accountabilities of employees;

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

Training

2. Training

- 2.1 **Job Specific Training** - The nature of responsibilities/activities performed by the staff of the bank is different from one another. So their training on AML issues should also be different for each category. Job specific AML trainings are discussed below:
- 2.1.1 **New Employees** -A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the bank, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.
 - 2.1.2 **Customer Service/Relationship Managers** - Members of staff who are dealing directly with the public are the first point of contact with



or. auto

potential money launderers and their efforts are vital to the organization's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that 'front-line' staffs are made aware of the bank's policy for dealing with non-regular (walk in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

- 2.1.3 **Processing (Back Office) Staff** - The staffs, who receive completed Account Opening, FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the bank's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.
- 2.1.4 **Credit Officers** - Training should reflect an understanding of the credit function. Judgments about collateral and credit all require awareness and vigilance toward possible money laundering activities. Indirect lending programs and lease financing also call for KYC efforts and sensitivity to laundering risks.
- 2.1.5 **Audit and Compliance Staff** - These are the people charged with overseeing, monitoring and testing AML controls, and they should be trained about changes in regulation, money laundering methods and enforcement, and their impact on the bank.
- 2.1.6 **Senior Management/Operations Supervisors and Managers** - A higher level of instruction covering all aspects of money laundering prevention procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and terrorist financiers; internal reporting procedures and the requirements for verification of identity and the retention of records.



2.1.7 **Senior Management and Board of Directors** - Money Laundering issues and dangers should be regularly and thoroughly communicated to the board. It is important that the compliance department has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering poses to the bank.

2.1.8 **The AML Compliance Officer** - should receive in depth training on all aspects of the Money Laundering Prevention Legislation, Bangladesh Bank directives and internal policies. In addition, the AML Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity. Also to improve the efficiency of the CAMLCO & D-CAMLCO or any other concerned official, Bank shall arrange proper training and/or professional certification program for the same.

Training Procedures

3. Training Procedures - The trainers or the facilitators (internal/external) will take the following steps to develop an effective training/workshop program.

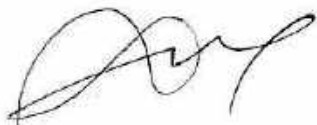


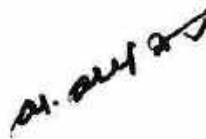
- 3.1 Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- 3.2 Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.
- 3.3 Determine the needs that are being addressed; e.g. uncovered issues by audits or exams, created by changes to systems, products or regulations.
- 3.4 Determine who can best develop and present the training program.
- 3.5 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.
- 3.6 To ensure all employees have adequate experience and/or training in order to carry out job duties effectively Learning and Talent Development Center will design/develop different program/course/module with the help of AML & CFT Division and the CAMLCO will have to approve it.
- 3.7 Establish a training calendar that identifies the topics and frequency of each course.
- 3.8 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.





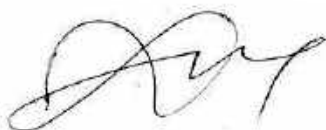

- 3.9 Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee personal file.
4. **Refresher Training** - In addition to the above relatively standard requirements, training may have to be tailored to the needs of specialized areas of the bank's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least once in every two years to ensure that staff does not forget their responsibilities. Bank will provide such training once in every two years; sometimes may choose a shorter or longer period or take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.
- Training should be ongoing, incorporating trends and developments in the bank's business risk profile, as well as changes in the legislation. Training on new money laundering schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.
5. **In-house Discussion** - Branch will arrange in house discussion on regular basis to update the employees of the branch on AML laws and regulation and circulars issued from Bangladesh Bank and Head Office from time to time.
6. **Education and Training of Customer** - As instructed by Bangladesh Bank vide BFIU circular 26 issued dated 16 June 2020, Bank shall respond to customers on different matters including KYC and TP attached to the account opening form with proper rational. Bank shall time to time distribute leaflets among the customers to make them aware about money laundering and terrorist financing and also to arrange to stick poster in every branch at a visible place. Every Bank has to arrange public awareness programs like advertisements through Billboard, poster, leaflet etc.

The Bank will continue to devote considerable resource to establish and maintain employee's awareness of the risk of money laundering and their competence to identify and report relevant suspicions in this area. The Bank is dedicated to a continuous program of increasing awareness and training of employees at all appropriate levels in relation to their knowledge and understanding of AML issue, their respective responsibilities and the various control and procedures introduced by the bank to deter money laundering and terrorist financing.

CHAPTER XIII: BANKING RELATIONSHIPCorrespondent Banking Relationship

1. Correspondent banking relationship sometimes creates a risk that the other Bank's customer may be using that Bank to launder funds. It is not necessary possible to conduct due diligence on that Bank's customer base and as such. These relationships require care and attention to guard against becoming unwilling participants in these activities. The following control should be implemented for establishing corresponding banking relationship.
 - 1.1. Before providing correspondent banking service CAMLCO's approval must be obtained on being satisfied about the nature of the business of the respondent bank through collection of information (KYC on AML Questionnaire) as per Annexure-Kha of BFIU Circular No. 26 dated 16/06/2020 - Bank should establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority. (Annexure-Kha)
 - 1.2. Bank should not establish or continue a correspondent banking relationship with **SHELL BANK or Banks maintain relationship with SHELL Bank** (here Shell Bank refers to such banks as are incorporated in a jurisdiction where it has no branches / physical presence in the country in which it is incorporated and licensed and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within the country. The existence simply of a local agent or low level staff does not constitute physical presence).
 - 1.3. Correspondent Banking relationship shall not be established or continued with those responded bank that established correspondent banking relationship or maintain account with a shell bank. Bank has to ensure that Respondent Bank is not serving or continuing any relationship with any Shell Bank⁹.
 - 1.4. Bank should pay particular attention when maintaining a correspondent banking relationship with bank incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries & territories enlisted in FATF's non cooperative countries and Territories list). Enhanced due diligence shall be required in such case. Detail information on the beneficial ownership of such banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.
 - 1.5. Enhanced due diligence shall have to be exercised in case of the respondent banks that allow direct use of the correspondent account by their customer to transact business on their behalf (i.e. payable through account)
 - 1.6. The Bank will review correspondent banking relationship as and when required.
 - 1.7. Before establishing relation Bank will be satisfied with the respondent institution's Anti money laundering and Anti-Terrorism control.
 - 1.8. CDD measures are almost same but such measures also apply for securities transaction or fund transfer, whether for the cross border financial institution as principal or for its customer.






Non-Profit Organizations (NPO) and NGO

2. Account of Charities, NGO & NPO to be treated as high risk account. No account shall open without the registration from the appropriate authorities i.e. Bureau of NGO, Directorate of Co-operative Society, and Directors of social welfare where applicable. Enhance Due Diligence (EDD) will be performed for opening and operating such account to prevent money laundering. As per foreign donation regulations (voluntary Activities) ordinance, 1978 and the foreign contribution (Regulation), 1982 no person or organization can accept or expense the foreign fund/donation for voluntary activities without the prior permission of the Govt. It is punishable offence. The Bank shall release the fund to ensure the approval of the Bureau of NGO. Periodical monitoring of transaction is a must to observe the nature of transaction. Account of such organization should be treated as high risk account and should be monitored the transaction regularly.

KYC requirement for High Net Worth Customer

3. Complete the form for high net worth customer falling under the following criterion:
- 3.1. New customer whose initial deposit is more than Tk.50.00 lac (initial means within one month of account opening)
 - 3.2. Existing customer whose total asset under management grow to > Tk. 50.00 lac for 3 consecutive months

Source of Wealth

4. Source of Wealth

- 4.1. Types of source of wealth
- 4.1.1. Business ownership profession
 - 4.1.2. Top executive investment
 - 4.1.3. Inheritance others

Officials will have to ask questions referred to be used when obtaining source of wealth. He/she may need to choose more than one category for a business owner with inherited wealth.

5. Notes of face to face meeting with customers

The customer evaluation process may involve understanding the circumstances and profile of the customer, such as: The source of their funds and source of wealth. The nature of their circumstances. The reasons why they have chosen the bank to establish a relationship with, the anticipated and expected level of activity etc. for which officials should take notes while obtaining information regarding related issues.

Annual Review of Customer Profile

6. Annual review of customer profile
- 6.1. Profession – e.g. Physician, Lawyer, Engineer, Accountant and Sports professional etc.



- 6.2. Investment – customer who buys and sells assets of any type: real estate, securities, companies, royalties and patents etc.
- 6.3. Should be prepared by Account Officer/Relationship Manager with name and date.
- 6.4. And reviewed by Branch Manager/Operations Manager & BAMLCO with name and date.

Model questions to be asked when obtaining source of wealth

7. Model questions to be asked when obtaining source of wealth.

7.1. Wealth Generated from Business Ownership

- 7.1.1. Description & nature of business and its operation
- 7.1.2. Ownership type: private or public
- 7.1.3. What kind of economy
- 7.1.4. Percent of ownership?
- 7.1.5. Estimated sales volume?
- 7.1.6. Estimated net income?
- 7.1.7. Estimated net worth?
- 7.1.8. How long in Business?
- 7.1.9. How was the business established?
- 7.1.10. Other owners or partners: Yes/ No
- 7.1.11. Names of other owners or Partners?
- 7.1.12. Percent owned by other owners or partners?
- 7.1.13. Number of employees?
- 7.1.14. Number of Locations?
- 7.1.15. Geographic trade areas of business?
- 7.1.16. Other family members in business?
- 7.1.17. Significant revenue from govt. contact or license?

7.2. Wealth derived from a Top executive

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

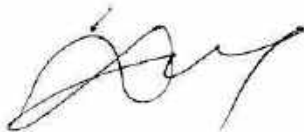
7.3. Primary sources of wealth

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






- 7.4. Wealth generated from a profession (Physician, Doctor, Lawyer, Engineer, Entertainer etc.)
 - 7.4.1. What is the profession, including area of specialty (example: Arts, singer, construction – engineer etc.)?
 - 7.4.2. Source of wealth
 - 7.4.3. Estimate of income
- 7.5. Wealth generated from investment
 - 7.5.1. Where did the source of wealth come from?
 - 7.5.2. What do the currently invest in (ex. Invested in share, bonds)?
 - 7.5.3. What is the size of investment?
 - 7.5.4. Cite notable public transactions if any
 - 7.5.5. What is the client's role in transaction?
 - 7.5.6. Estimated annual income/ capital appreciation?
 - 7.5.7. How long has the client been an investor?



References

- ¹ International Convention for the Suppression of the Financing of Terrorism (1999), Article 2, <http://www.un.org/law/cod/finterr.htm>.
- ² <https://www.hSDL.org/?view&did=3549>
<https://documents.worldbank.org/curated/en/982541468340180508/pdf/634980WP0Refer00Box0361517B0PUBLIC0.pdf>
- ³ Ref.: Section 1.3.1 Chha of BFIU Circular No.-26//2020 dated 16-09-2017 of Bangladesh Financial Intelligence Unit (BFIU).
- ⁴ Ref.: Section 1.3.1 (Kha) of BFIU Circular No.-26//2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)
- ⁵ FATF*GAFI, Financial Action Task Force, FATF Special Recommendation IX pertains to cash couriers.
- ⁶ FATF*GAFI, Financial Action Task Force, The International Trade System.
- ⁷ FATF*GAFI, Financial Action Task Force.
- ⁸ Ref.: Section 12(1) (a) of BFIU Circular No.-26//2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)
- ⁹ Ref.: Section 9.1 (1) (a) of BFIU Circular No.-26//2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)
- ¹⁰ Ref.: Section 9.1 (1) (b) of BFIU Circular No.-26//2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)
- ¹¹ Ref.: Section 11.2.1 of BFIU Circular No.-26//2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)
- ¹² Ref.: Section 11.2.1 of BFIU Circular No.-26//2020 dated 16-06-2020 of Bangladesh Financial Intelligence Unit (BFIU)

