



COMPANY NAME
LOGODESIGN

AML

**REGULATORY
RISK**

**CUSTOMER
RISK**

**PRODUCT
&
SERVICE RISK**

**COUNTRY/
JURISDICTION
RISK**

**BUSINESS
PRACTICES/
DELIVERY
METHODS OR
CHANNELS RISK**

Updated: August

2023

**MONEY
LAUNDERING &
TERRORIST
FINANCING RISK
MANAGEMENT
GUIDELINE**

**AML
&
CFT
DIVISION**



Standard Bank Limited

Shari'ah Based Islami Bank

Preface

A bank should develop a thorough understanding of the inherent Money Laundering (ML) & Terrorist Financing (TF) risks present in its customer base, product/service, delivery channels and the jurisdictions within which it or its customers do business. This understanding should be based on specific operational and transaction data and other internal information collected by the bank as well as external sources of information such as national risk assessments and country reports from international organizations. Policies and procedure for customer acceptance, due diligence and ongoing monitoring should be designed and implemented to adequately control those identified inherent risks.

Risk management requires the identification and analysis of Money Laundering (ML) & Terrorist Financing (TF) risks present within the Bank and the design & effective implementation policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML & TF risks, Standard Bank Ltd consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied.

Bangladesh Bank (BB), as the major regulator of the financial system of the country plays a pivotal role to stabilize and enhance the efficiency of the financial system. Considering ML and TF as one of the major threats to the stability and the integrity of the financial system, Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank (BB) has taken several initiatives including issuance of circulars/circular letters/Guidance Notes under Money Laundering prevention Act (MLPA) and Anti-terrorism Act (ATA). To keep pace with international initiatives and promulgated MLPA, 2012 (Amendment 2015), ATA 2009 (amendment 2012 & 2013) and Money Laundering Prevention Rules 2019.

To comply with the international requirement as well as Bangladesh Financial Intelligence Unit (BFIU), Standard Bank Ltd has updated 'Money Laundering and Terrorist Financing Risk Management Guidelines'. Standard Bank Ltd instructs the Branches/Departments/Divisions/Agent Banking to follow ML & TF risk considering the customers, products, delivery channels and geographical locations and also follow the regulatory risk i.e. risk arises from non-compliance of AML & CFT measures.

The purpose of this guidance is to build the legal and regulatory framework for anti-money laundering and combating financing on terrorism (AML & CFT) requirements and systems. With a view to this, the document interprets the requirements of the relevant laws and regulations, and how they might be implemented in practice. It indicates good industry practices in AML and CFT procedures through a proportionate, risk-based approach; and assists the banks to design and implement the systems and controls necessary to mitigate the risks of the banks being used in connection with money laundering and the financing of terrorism.



Table of Contents

Particulars		Page No.
CHAPTER I: AN OVERVIEW OF ML & TF		
1.1	Preamble	1
1.2	Purpose	1
1.3	Definition Money Laundering	2
1.4	Stages of Money Laundering	3
1.5	Why Money Laundering is done	4
1.6	Penalties under Money Laundering Prevention Act 2012	5
1.7	Definition of Terrorist Financing	6
1.8	Penalties for Terrorist Financing	7
1.9	Duties of BFIU and Reporting Organizations	8
1.10	UNSCR Implementation Mechanism	8
1.11	The Link Between Money Laundering and Terrorist Financing	10
1.12	Why We Must Combat Money Laundering and Terrorist Financing	10
CHAPTER II: INTERNATIONAL INITIATIVES OF ML & TF		
2.1	International Initiatives	13
2.2	The United Nations	13
2.3	The Vienna Convention	13
2.4	The Palermo Convention	13
2.5	International Convention for the Suppression of the Financing of Terrorism	14
2.6	Security Council Resolution 1267 and Successors	14
2.7	Security Council Resolution 1373	14
2.8	Security Council Resolution 1540	15
2.9	The Counter-Terrorism Committee	15
2.10	The Counter-Terrorism implementation Task Force (CTITF)	15
2.11	Global Program against Money Laundering	16
2.12	The Financial Action Task Force	16
2.13	FATF 40+9 Recommendations	16
2.14	FATF New Standards	16
2.15	Monitoring Members Progress	17
2.16	The NCCT List	17
2.17	International Cooperation and Review Group (ICRG)	17
2.18	The Basel Committee on Banking Supervision	18
	2.18.1 Statement of Principles on Money Laundering	18
	2.18.2 Basel Core Principles for Banking	18
	2.18.3 Customer Due Diligence	19
2.19	International Organization of Securities Commissioners	19
2.20	The Egmont Group of Financial Intelligence Units	19
2.21	Asia Pacific Group on Money Laundering (APG)	20

STANDARD BANK LIMITED
 Approved in its...^{386th}...Board Meeting
 dated 26.12.2023 under agenda no. 22256
 Company Secretary

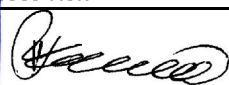
(Signature)

(i)

(Signature)

CHAPTER III: MAJOR NATIONAL AML & CFT INITIATIVES			
3.0		National Initiatives	21
3.1		Founding Member of APG	21
3.2		Legal Framework	21
3.3		Central and Regional Taskforces	22
3.4		Anti -Money Laundering Department	22
3.5		Bangladesh Financial Intelligence Unit	22
3.6		National ML & TF Risk Assessment (NRA)	22
3.7		National Strategy for Preventing ML, TF & PF	23
3.8		Chief Anti Money Laundering Compliance Officers (CAMLCOs) Conference	24
3.9		Egmont Group Memberships	24
3.10		Anti -Militants and De-Radicalization Committee	24
3.11		Memorandum of Understanding (MOU) between ACC AND BFIU	24
3.12		NGO/NPO Sector Review	24
3.13		Implementation of TFS	25
3.14		Coordinated Effort on the implementation of the UNSCR	25
3.15		Risk Based Approach	25
3.16		Memorandum of Understanding (MOU) BFIU AND other FIUs	26
CHAPTER IV: AML & CFT COMPLIANCE PROGRAM OF STANDARD BANK			
4.1		SBL AML, CFT & CPF Compliance Program	27
4.2		Roles and Responsibilities of Board of Directors	27
4.3		Senior Management Role & Responsibilities	28
4.4		Statement of Commitment of Managing Director (MD) & CEO	29
4.5		Customer Acceptance Policy	30
4.6		Policy for rejection of customer	30
4.7		ML & TF Risk Assessment	31
CHAPTER V: ML & TF RISK ASSESMENT OF STANDARD BANK			
5.1		Risk	32
5.2		Assessing Risk	32
5.3		Risk Identification	32
5.4		Risk Assessment process	32
	5.4.1	Methodology of Risk Assessment	33
	5.4.1.1	Likelihood Scale	33
	5.4.1.2	Impact of Scale	33
5.5		Risk matrix and risk score	34
5.6		Risk Assessment and Management Exercise	35
5.7		Risk Treatment	35
5.8		Monitoring and Review	36
CHAPTER VI: ML & TF RISK MANAGEMENT OF STANDARD BANK			
6.1		Risk Management	37
6.2		Risk management and mitigation	37
6.3		Which Risk do Banks Needs to Manage	37
	6.3.1	Business risk	37

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



(iii)



	6.3.2	Regulatory risk	38
6.4		Risk Management Process	38
	6.4.1	Risk Identification	38
	6.4.1.1	Business Risks	39
	6.4.1.2	Regulatory Risks	40
6.5		Risk Management Strategies	41
6.6		Ongoing Risk Monitoring	41
6.7		Higher Risk Scenario	42
	6.7.1	Specific High Risk Elements and Recommendations for EDD	43
6.8		Low Risk Scenario	44
6.9		Risk Variables	45
6.10		Counter Measures for Risks	45
CHAPTER VII: RISK REGISTER OF STANDARD BANK			
7.1		Risk Register	46
7.1.1		Business Risk	46
		a. ML & TF risk register for customer	46
		b. ML & TF Risk Register for Products & Services	58
		c. ML & TF Risk Register for Business practices/delivery methods or channels	64
		d. ML & TF Risk Register for Country/jurisdiction	67
7.1.2		Register for Regulatory Risk	70
CHAPTER VIII: COMPLIANCE STRUCTURE OF STANDARD BANK			
8.1		Central Compliance Committee	75
8.2		Formation of CCC, Head Office	76
8.3		Responsibilities and Authorities of the CCC	76
8.4		Separation of CCC from Internal Control & Compliance Department (ICCD)	78
8.5		Chief Anti Money Laundering Compliance Officer (CAMLCO)	78
8.6		Authorities and Responsibilities of CAMLCO	79
8.7		Branch Anti Money Laundering Compliance Officer (BAMLCO)	79
8.8		Responsibilities and Authorities of BAMLCO	79
8.9		Internal Control and Compliance	83
8.10		Employee Training and Awareness Program	85
8.11		External Auditor	89
CHAPTER IX: CUSTOMER DUE DILIGENCE			
9.1		Preamble	90
9.2		Legal Obligations of CDD	91
9.3		General Rule of CDD	92
9.4		Timing of CDD	94
9.5		Transaction Monitoring	94
9.6		Exception when opening a bank account	95
9.7		In case where conducting the CDD measure is not possible	95
9.8		Customer Identification	96
9.9		Verification of Source of Funds	96
9.10		Verification of Address	97

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



(iii)



9.11		Persons without Standard Identification Documentation	97
9.12		Walk-in/one off Customers	98
9.13		Non Face to Face Customers	98
9.14		Customer Unique Identification Code	98
9.15		Corresponding Banking	98
9.16		Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top Level Officials of any International Organization	99
	9.16.1	Definition of PEPs	100
	9.16.2	CDD measures of PEPs	100
	9.16.3	Definition of Influential Persons	100
	9.16.4	CDD measures for influential persons	101
	9.16.5	Definition of Chief Executives or Top Level Officials of any International Organization	101
	9.16.6	CDD measures for Chief Executives or Top Level Officials of any International Organization	102
	9.16.7	Close Family Members and Close Associates of PEPs, Influential Persons and Chief Executives or Top Level Officials of any International Organization	102
	9.16.8	CDD measures for Close Family Members and Close Associates of PEPs, Influential Persons and Chief Executives or Top Level Officials of any International Organization	103
9.17		Wire Transfer	103
	9.17.1	Cross-Border Wire Transfers	103
	9.17.2	Domestic Wire Transfers	104
	9.17.3	Duties of Ordering, Intermediary and Beneficiary Bank in case of Wire Transfer	104
9.18		CDD for Beneficial Owner	105
9.19		Agent Banking	106
9.20		Mobile Banking	108
9.21		Management of Legacy Accounts	110
CHAPTER X: TRADE BASED MONEY LAUNDERING			
10.1		Definition of TBML	111
10.2		Basic Trade Based Money Laundering Techniques	111
	10.2.1	Over- and Under-Invoicing of goods and services	111
	10.2.2	Multiple Invoicing of goods and services	112
	10.2.3	Over- and Under-Shipments of goods and services	112
	10.2.4	Falsely described goods and services	112
10.3		Trade Based Money Laundering Risk	113
10.4		Instruments of Trade Finance and their vulnerabilities	113
10.5		Main Risks Associated with Trade Finance	119
10.6		Standard Bank Role	120
10.7		General CDD requirements in Trade Finance	120
	10.7.1	CDD Measures for Import Business	121
	10.7.1.1	KYC Policy & Procedures	121
	10.7.1.2	Collection & Verification of Import Related Documents	121
	10.7.2	CDD Measures for Export Business	126
	10.7.2.1	KYC Policy & Procedures	126
	10.7.2.2	Collection & Verification of Export Related Documents	126

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary

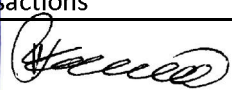
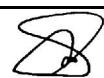


(iv)



CHAPTER XI: INVESTMENT/CREDIT/LOAN BACKED OR BASED MONEY LAUNDERING			
11.0		Definition & Process	131
11.1		Money Laundering through Real Estate Sector	131
	11.1.1	Complex Investments and Credit Finance	132
	11.1.2	Investment Back Scheme	132
	11.1.2.1	Indicators and methods identified in the scheme	133
	11.1.3	Back-to Back Investment Schemes	133
	11.1.3.1	Indicators and methods identified in the scheme	133
	11.1.4	The Role of Non -Financial Professionals	133
	11.1.4.1	Obtaining Access to Financial Institutions through Gatekeepers	134
	11.1.4.2	Indicators and methods identified in the scheme	134
	11.1.5	Assistance in the Purchase or Sale of Property	134
	11.1.5.1	Indicators and methods	135
	11.1.6	Trust Accounts	135
	11.1.6.1	Indicators and methods	135
	11.1.7	Management or Administration of Companies	135
	11.1.7.1	Indicators and methods	136
	11.1.8	Corporate Vehicles	136
	11.1.9	Offshore Companies	136
	11.1.9.1	Indicators and methods	136
	11.1.10	Legal Arrangements	137
	11.1.10.1	Indicators and methods	137
	11.1.11	Shell Companies	138
	11.1.12	Property Management Companies	138
	11.1.12.1	Indicators and methods	138
	11.1.13	Non –trading real estate investment companies	139
	11.1.13.1	Indicators and methods	139
	11.1.14	Manipulation of Appraisal or Valuation of a Property	139
	11.1.14.1	Over-valuation or Under- valuation	139
	11.1.15	Mortgage Schemes/ Murabaha or By Muazzel Schemes	140
	11.1.16	Illegal Funds in Mortgage Investments and Interest/profit/payments	140
	11.1.17	Investment Schemes and Financial Institutions	140
	11.1.18	Concealing Money Generated by Illegal Activities	141
	11.1.19	Investment in Hotel Complexes, Restaurants and Similar Developments	141
	11.1.19.1	Indicators and methods	141
	11.1.20	Personal Investment/Car Investment/Home Investment	141
	11.1.21	SME/Women Entrepreneur Investment	142
	11.1.22	Money Laundering through Credit Cards	142
11.2		The Role of Current technology in detecting ML techniques	144
CHAPTER XII: RECORD KEEPING			
12.1		Record Keeping Requirement	145
12.2		Legal Obligations	145
12.3		Obligations under Circulars	145
12.4		Records to be kept	146
12.5		Customer Information	146
		Transactions	147

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary

 (v) 

12.7		Internal and External Reports	147
12.8		Other Measures	147
12.9		Formats and Retrieval of Records	147
12.10		Training Records	148
CHAPTER XIII: REPORTING TO BFIU			
13.1		Legal Obligations	149
13.2		Suspicious Transaction Reporting	149
13.3		Identified of STR/SAR	150
13.4		Tipping Off	152
13.5		Cash Transaction Report	153
13.6		Self-Assessment Report	153
13.7		Independent Testing Procedure	154
13.8		ICCD's obligations regarding Self-Assessment or Independent Testing Procedure	154
13.9		CAMLCO's Office obligations regarding Self-Assessment or Independent Testing Procedure	154
CHAPTER XIV: RECRUITMENT, TRAINING AND AWARENESS			
14.1		Obligations under Circular	156
14.2		Employee Screening	156
14.3		Know Your Employee (KYE)	156
14.4		Training for Employee	157
14.5		Awareness of Senior Management	157
14.6		Customer Awareness	158
14.7		Awareness of Mass People	158
CHAPTER XV: TERRORIST FINANCING & PROLIFERATION FINANCING			
15.1		Terrorist Financing & Proliferation Financing	159
15.2		Legal Obligations	159
15.3		Obligations under Circular	159
15.4		Necessity of Funds by Terrorist	160
15.5		Source of Fund/Raising of Fund	160
15.6		Movement of Terrorist Fund	160
	15.6.1	Formal Financial Sector	160
	15.6.2	Trade Sector	161
	15.6.3	Cash Couriers	161
	15.6.4	Use of Alternative remittance systems (ARS)	161
	15.6.5	Use of Charities and Non Profit Organizations	161
15.7		Targeted Financial Sanctions	162
	15.7.1	TFS related to terrorism and terrorist financing	162
	15.7.2	TFS related to Proliferation	162
15.8		Automated Screening Mechanism of UNSCRs	163
15.9		Responsibilities of Bank Officials for detection and Prevention of Financing on Terrorism and Financing in proliferation	163
15.10		Role of Standard Bank in Preventing TF & PF	165

STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



(vi)



16		List of Abbreviations	167
17		Conventional Vs Islamic terms	169
		Annexure A: KYC Documentation	
		Annexure B: Red Flag of Risk Assessment	

STANDARD BANK LIMITED
 Approved in its...^{386th}...Board Meeting
 dated 26.12.2023 under agenda no. 22256
 Company Secretary



(vii)



CHAPTER I: AN OVERVIEW OF MONEY LAUNDERING & TERRORIST FINANCING AND PROLIFERATION FINANCING

1.1 Preamble:

Every Bank or FI should develop an integrated and institution-wide risk culture, based on a full understanding of the risks it faces and how they are managed, considering risk tolerance and appetite. Since the business of banks involves risk taking, it is fundamental that risks are appropriately managed. A sound and consistent risk culture throughout a financial institution is a key element of effective risk management. The core risks identified by Bangladesh Bank are credit or investment risk, market risk, liquidity risk, operational risk, compliance risk, strategic risk, reputation risk, environmental risk, and money laundering risk.

Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) have become very vital issue in recent years. Money laundering is employed by launderers worldwide to conceal the illicit money flow earned by unlawful activities. It may happen in almost every country in the world and the scheme typically involves transferring money through several countries in order to obscure its illicit origins. The rise of global financial markets makes money laundering easier than the imagination, making it possible to anonymously deposit "dirty" money in one country and then have it transferred to any other country for use.

It is widely recognized to be a crucial component of terrorist activity as terrorists are able to facilitate their activities only if they have the financial resources to do so. The consequences of terrorist activities are terrific and devastating. So, prevention of ML & TF are very much crucial for the economy and also for the security reason of the country. Recently another issue has come up and that is proliferation financing.

The process of ML, TF & PF is very much quicker and ever evolving. The money launderers and terrorist financiers are formulating more and more complicated and sophisticated procedures as well as using new technology for ML, TF and PF. To address these emerging challenges, the international community has taken numerous initiatives against ML, TF & PF. In accordance with international initiatives, Bangladesh has also acted on many fronts. All financial sectors today are investing more in technology and staff development to ensure a robust defense.

1.2 Purpose

The purpose of the Guidelines is:

- ✓ To identify ML, TF & PF risk;



- ✓ Assist banks, competent authorities as well as Country in the design and implementation of ML,TF & PF risk by providing general guidelines and examples of current industry best practice;
- ✓ Support the effective implementation and supervision of national AML & CFT measures, by focusing on risks and on mitigation measures ;
- ✓ To prevent the bank's product and services from being used as a channel for money laundering & terrorist financing;
- ✓ To construct awareness on the importance of AML, CFT & CPF among all employees, members of the Board of Directors, owners and customers of the Bank;
- ✓ To prevent the reputational loss by associating with money launderers/ terrorist financier/ proliferation financier;

1.3 Definition of Money Laundering

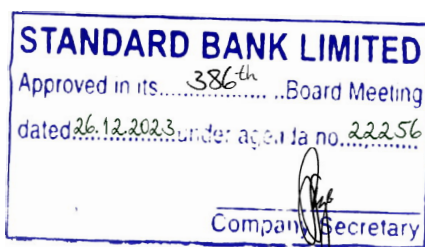
Briefly described, "money laundering" is the process by which proceeds from a criminal activity are disguised to disguise their illicit origin. More precisely, according to the Vienna Convention and the Palermo Convention provisions on money laundering, it may encompass three distinct: (i) the conversion or transfer, knowing that such property is the proceeds of crime (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; and (iii) the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime.

The Financial Action Task Force (FATF), the international standard setter for anti money laundering (AML) and combating financing of terrorism (CFT) efforts, recommends that money laundering should criminalized in line with the Vienna Convention and Palermo Convention. Like other countries of the world, Bangladesh has criminalized money laundering in line with those conventions. Moreover, Bangladesh also considers some domestic concerns like 'smuggling of money or property from Bangladesh' in criminalizing money laundering.

As per Money Laundering Prevention Act 2012 (amendment 2015), Section 2 (v), Money Laundering is defined as under:

"Money Laundering" means -

- i) knowingly move, convert, or transfer proceeds of crime or property involved in an offence for the following purposes:-
 - 1) concealing or disguising the illicit origin/nature, source, location, ownership or control of the proceeds of crime; or
 - 2) assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
- ii) smuggling money or property earned through legal or illegal means to a foreign country;



- iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
- iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
- v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
- vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
- vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
- viii) participating in, associating with conspiring, attempting, abetting, instigating or counseling to commit any offence(s) mentioned above;

1.4 Stages of Money Laundering

Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages which are as follows:

❖ • **Placement** – The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international. Examples of placement transactions include:

- ❖ Blending of funds: Comingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurant.
- ❖ Foreign exchange: Purchasing of foreign exchange with illegal funds.
- ❖ Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements.
- ❖ Currency smuggling: Cross-border physical movement of cash or monetary instruments.
- ❖ Investments: Repayment of legitimate investments using laundered cash.
- ❖ Purchasing monetary instruments i.e. travelers' checks, payment orders.
- ❖ Using cash to purchase expensive items that can be resold.

Smurfing – a form of Placement where the launderer makes many small cash deposits instead of a large one to evade local regulatory reporting requirements applicable to cash



transactions. Launderers intend to avoid the threshold of Cash Transaction for dodging the reporting to Regulatory or competent authority.

- ❖ **Layering** – The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds. This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds. Examples of layering transactions include:
 - ❖ Electronically moving funds from one country to another and dividing them into advanced financial options and or markets.
 - ❖ Moving funds from one financial institution to another or within accounts at the same institution.
 - ❖ Converting the cash placed into monetary instruments.
 - ❖ Reselling high value goods and prepaid access/stored value products.
 - ❖ Investing in real estate and other legitimate businesses.
 - ❖ Placing money in stocks, bonds or life insurance products.
 - ❖ Using shell companies to obscure the ultimate beneficial owner and assets.
 - ❖ Early surrender of an annuity without regard to penalties.
 - ❖ L/Cs with false invoices/bills of lading etc.

- ❖ **Integration:** Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions. This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth.

This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets. Examples of integration transactions include:

- ❖ Purchasing luxury assets like property, artwork, jewelry or high end automobiles.
- ❖ Getting into financial arrangements or other ventures where investments can be made in business Enterprises.

1.5 Why Money Laundering is Done

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



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

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

1.6 Penalties under Money Laundering Prevention Act, 2012 (Amendment, 2015)

i) Offence of Money Laundering and Punishment (Section 4):

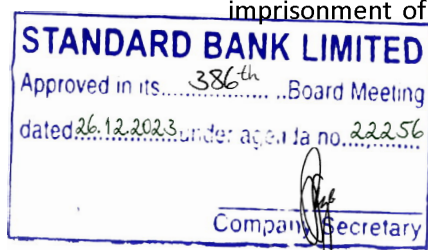
1. According to section 4(1), Money laundering is an offence.
2. According to section 4(2), Any person who commits or abets or conspires to commit the offence of money laundering, shall be punished with imprisonment for a term of at least 4(four) years but not exceeding 12(twelve) years and, in addition to that, a fine equivalent to the twice of the value of the property involved in the offence or taka 10 (ten) lac, whichever is greater. However, in case of failure of the payment of the fine in due time, the court may issue an order of extra imprisonment considering the amount of the unpaid fine.
3. According to 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.
4. According to section 4(4), Any entity which commits or abets, assists or conspires to commit the offence of money laundering under this section, subject to the provisions of section 27, measures shall be taken as per sub-section (2) and punished with a fine of not less than twice the value of the property related to the money laundering or taka 20(twenty) lacks, whichever is higher and in addition to this the registration of the said entity shall be liable to be cancelled. However, in case of failure in payment of the fine by the entity in due time, the court may, considering the amount of unpaid fine, issue an order of imprisonment to the entity's owner, chairman or director or by whatever name he is regarded.

ii) Punishment for violation of a freezing or attachment order (Section 5):

Any person who violates a freeze order or order of attachment issued pursuant to this Act shall be punishable with an imprisonment for a maximum period of 3 (three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or both.

iii) Punishment for divulging information (Section 6):

Whoever contravenes the provisions contained of this act shall be punishable by imprisonment of maximum period of 2 (two) years or a fine, not exceeding Tk. 50 (fifty)



thousand or both.

iv) Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information (Section 7):

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

v) Punishment for providing false information (Section 8):

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

1.7 Definition of Terrorist Financing

Terrorist financing provides funds for terrorist activities. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Financing of Terrorism is also includes:

- providing or collecting property for carrying out an act of terrorism;
- providing services for terrorism purposes;
- arranging for retention or control of terrorist property; or
- dealing with terrorist property.

The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

- 'If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
 - a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or
 - b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.



- 2) For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

According to the article 7 of the Anti-Terrorism Act 2009, (Amendment) 2013 of Bangladesh, Offence of terrorist financing: Sub-section (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

(a) it will be used to carry out terrorist activity;

(b) it will be used for any purposes by terrorist person or entity or in the knowledge that they are to be used by terrorist person or entity;

the said person or entity shall commit the offence of terrorist financing.

Sub-section 2) Conviction for terrorist financing shall not depend on any requirement that the fund, services or any other property mentioned in sub-section (1) were actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.

1.8 Penalties for Terrorist Financing

According to the Section 7 of the Anti-Terrorism Act 2009, (Amendment) 2013 of Bangladesh,

Section 7(3) If any person is found guilty of any of the offences mentioned in sub-sections (1), the person shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (four) years, and in addition to that, a fine may be imposed equal to twice the value of the property involved with the offence or taka 10(ten) lac, whichever is greater.

Section 7(4) If any entity is found guilty of any of the offences mentioned in the sub-sections (1)- (a) steps may be taken in accordance with section 18 and in addition to that a fine may be imposed equal to thrice the value of the property involved with the offence or taka 50 (fifty) lacs, whichever is greater; and

(b) The head of such entity, whether he is designated as Chairman, Managing Director, Chief Executive or any other name, shall be punished with an imprisonment for a term not exceeding 20 (twenty) years but not less than 4 (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.



1.9 Duties of BFIU and Reporting Organizations:

Adequate powers have been assigned to BFIU through section 15 of the Anti -Terrorism Act 2009 to take all necessary actions that the Unit deems fit to combat TF. Duties of the Reporting agency have been delineated in section 16 of the Act.

1.10 UNSCR Implementation Mechanism:

A) Measures to implement United Nations Security Council Resolutions as mentioned in section 20(A) of Anti -Terrorism Act, 2009:

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, the Government of Bangladesh shall, in addition to the power mentioned in other sections of this Act or in any other law for the time being in force, have power of taking measures-

- (a) to freeze, seize or attach, without delay and without issuing any prior notice, the property, funds or other financial assets or economic resources held by, including funds derived or generated from property owned or controlled directly or indirectly by the listed person or entity or by any undertaking owned or controlled by the listed person or entity, or on behalf of a natural person or an entity, if the name of the person or entity is included in the lists, maintained by the committee established under Resolution NO. 1267 of the United Nations Security Council;
- (b) to freeze, seize or attach, without delay and without issuing any prior notice, the funds or other financial assets or economic resources of the person who commits, or attempts to commit terrorist acts or participates in or facilitates the commission of terrorist acts; or of entities owned or controlled directly or indirectly by such person; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such person and associated persons and entities listed by the United Nations Security Council or proscribed or listed under Resolution No. 1373 of the United Nations Security Council;
- (c) to prohibit any willful provision or collection, directly or indirectly, of funds by any person or entity, whether in or outside Bangladesh, with the intention to use such funds or having the knowledge that they shall be used to carry out any

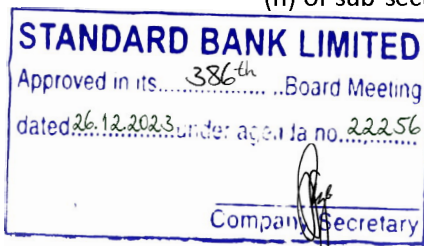


terrorist act;

- (d) to prohibit any person or entity from making any funds, financial assets or economic resources of financial or other related services available, directly or indirectly, for the benefit of the persons or entities listed by the United Nations Security Council or proscribed or listed under Resolution No. 1373 or of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons;
- (e) to prevent the entry into or the transit through Bangladesh of the persons listed by the United Nations Security Council through effective border control and immigration measures;
- (f) to prevent any direct or indirect supply, sale and transfer, in or outside Bangladesh, of arms and ammunition and other related items, materials, equipment, goods and technologies to the persons or entities listed by the United Nations Security Council;
- (g) to deny permission for any aircraft to take off or land in their territory if it is owned, leased or operated by or on behalf of the persons or entities listed by the United Nations Security Council;
- (h) to prevent illicit trafficking in nuclear, chemical or biological weapons, their means of delivery and related materials, including through inspection of cargo to and from the persons or entities listed by the United Nations Security Council;
- (i) to prohibit and prevent any activity mentioned in the said Resolutions and related with the persons and entities listed by the United Nations Security Council;
- (j) to issue directions, from time to time, to the reporting agencies by Bangladesh Financial Intelligence Unit for proper implementation of this section;
- (k) to determine, by issuing order or notification, the appropriate authority to take required actions as per the power stated in clauses (a) to (i).

B) Punishment for the offence of violating United Nations Security Council Resolutions as mentioned in Anti- Terrorism Act 2009-

- a) If any person or entity violates a freezing or attachment order issued under this section, the person or the concerned person of the entity shall be punished with imprisonment for a term not exceeding 04(four) years or with a fine equivalent to twice the value of the property subject to freeze or attachment, or with both.
- b) If any person or entity does any act or fails to do an act in contravention of clauses (c) and (d) of sub-section (1) of 20(A), the said person or entity shall be deemed to have committed an offence of financing of terrorist activities and shall be punished according to the provisions of sub-section (3), (4)(a) or, as the case may be,(4)(b) of section 7.
- c) If any person or entity does any act or fails to do an act in contravention of clauses (e) to (h) of sub-section (i), the person or entity shall be deemed to have committed an offence



- of terrorist activity and shall be punished according to the provisions of sub-section (2),(3)(a) or, as the case may be, (3)(b) of section 6.
- d) If any reporting agency fails to comply with the directions issued by Bangladesh Financial Intelligence Unit under this section, or fails to take immediate freezing action required under this section, the said reporting agency shall be liable to pay a fine, determined and directed by Bangladesh Financial Intelligence Unit, not exceeding taka 25 (twenty five) lac but not less than 05 (five) lac or twice the value of the suspected fund, whichever is greater, and Bangladesh Bank may also 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.
- e) If any charge of negligence in implementing the provisions of this section is proved against any public servant, administrative actions shall follow in accordance with his respective service rules.

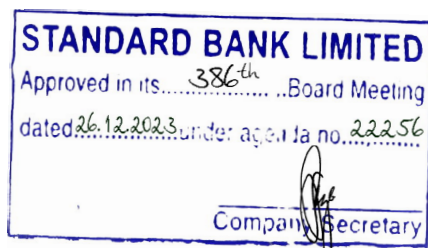
1.11 The Link between Money Laundering and Terrorist Financing

Money laundering is the process of concealing the illicit origin of proceeds of crimes. Terrorist financing is the collection or the provision of funds for terrorist purposes. In the case of money laundering, the funds are always of illicit origin, whereas in the case of terrorist financing, funds can stem from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the funding activity and the nature of the funded activity.

Similar methods are used for both money laundering and the financing of terrorism. In both cases, the actor makes an illegitimate use of the financial sector. The techniques used to launder money and to finance terrorist activities/terrorism are very similar and in many instances identical. An effective anti money laundering/counter financing of terrorism framework must therefore address both risk issues: it must prevent, detect and punish illegal funds entering the financial system and the funding of terrorist individuals, organizations and/or activities. Also, AML and CFT strategies converge; they aim at attacking the criminal or terrorist organization through its financial activities, and use the financial trail to identify the various components of the criminal or terrorist network. This implies to put in place mechanisms to read all financial transactions, and to detect suspicious financial transfers.

1.12 Why We Must Combat Money Laundering and Terrorist Financing

According to Mr. Min Zhu, Deputy Managing Director of the IMF --



“Effective anti money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse.”

Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a vital process to making crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (example: treatment of drug addicted person) to combat the serious consequences that result.

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

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

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

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

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

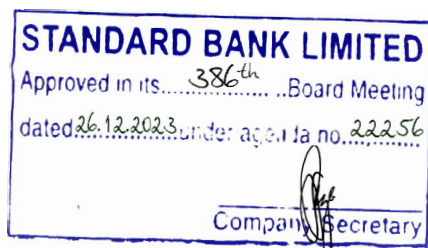
STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



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

Besides its effect on macro level, ML & TF also affects individual financial institution. If a money launderer uses a financial institution for making his/her money legitimate, the business of that financial institution may hamper. If the money launderer withdraws his/her deposited money from an FI before maturity, the FI will face liquidity crisis if the amount is big enough. Moreover, if it 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.

It is generally recognized that effective efforts to combat ML, TF & PF cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies.



CHAPTER II: INTERNATIONAL INITIATIVES ON ML AND TF

2.1 International Initiatives:

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

2.2 The United Nations:

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

First, it is the international organization with the broadest range of membership. The UN, founded in 1945, has 193 members from all across the world.

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

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

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

2.3 The Vienna Convention:

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

2.4 The Palermo Convention:

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

- Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;



- Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;
- Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyze and disseminate information; and
- Promote international cooperation.

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

2.5 International Convention for the Suppression of the Financing of Terrorism:

The financing of terrorism was an international concern prior to the attacks on the United States on 11 September, 2001. In response to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002, with 132 countries signing the convention and 112 countries ratifying it.

The convention requires ratifying states to criminalize terrorism, terrorist organizations and terrorist acts. Under the convention, it is unlawful for any person to provide or collect funds with the (1) intent that the funds be used for, or (2) knowledge that the funds be used to, carry out any of the acts of terrorism defined in the other specified conventions that are annexed to this convention.

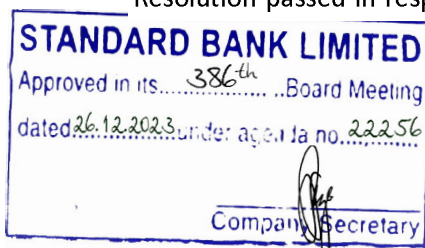
2.6 Security Council Resolution 1267 and Successors:

The UN Security Council has also acted under Chapter VII of the UN Charter to require member States to freeze the assets of the Taliban, Osama Bin Laden and Al-Qaeda and entities owned or controlled by them, as designated by the "Sanctions Committee" (now called the 1267 Committee). The initial Resolution 1267 of October 15, 1999, dealt with the Taliban and was followed by 1333 of December 19, 2000, on Osama Bin Laden and Al-Qaeda. Later Resolutions established monitoring arrangements (1363 of July 30, 2001), merged the earlier lists (1390 of January 16, 2002), provided some exclusions (1452 of December 20, 2002), and measures to improve implementation (1455 of January 17, 2003).

The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee.

2.7 Security Council Resolution 1373:

Unlike an international convention, which requires signing, ratification, and recognition in local law by the UN member country to have the effect of law within that country, a Security Council Resolution passed in response to a threat to international peace and security under Chapter VII of



the UN Charter, is binding upon all UN member countries. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to:

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

2.8 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 (weapons of mass destructions) and the importance for all States to implement them fully; it reiterates that 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 Organization for the Prohibition of Chemical Weapons (OPCW).

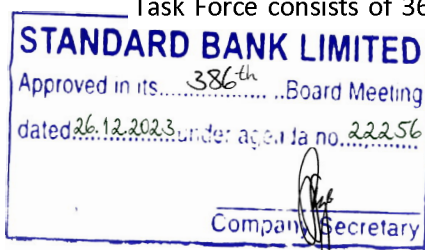
2.9 The Counter-Terrorism Committee:

As noted above, on September 28, 2001, the UN Security Council adopted a resolution (Resolution 1373) in direct response to the events of September 11, 2001. That resolution obligated all member countries to take specific actions to combat terrorism. The resolution, which is binding upon all member countries, also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism.

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

2.10 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.

2.11 Global Program against Money Laundering:

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

2.12 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 37 countries and territories and two regional organizations. There are also 31 associate members or observers of FATF (mostly international and regional organizations) that participate in its work.

2.13 FATF 40+9 Recommendations:

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

2.14 FATF New Standards:

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

STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary



Table 1: Summary of new FATF 40 Standards

Group	Topic	Recommendations
1	Policies and Coordination	1-2
2	Money Laundering and Confiscation	3-4
3	Terrorist Financing and Financing of Proliferation	5-8
4	Preventive Measures	9-23
5	Transparency and Beneficial Ownership of Legal Persons and	24-25
6	Power and Responsibilities of Competent Authorities and Other Institutional Measures.	26-35
7	International Co-operation	36-40

2.15 Monitoring Members Progress:

Monitoring the progress of members to comply with the requirements of 40+9 recommendations is facilitated by a two-stage process: self-assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of 40+9 recommendations. In the mutual evaluation stage, each member is examined and assessed by experts from other member countries in every five years. The first Mutual Evaluation (ME) of Bangladesh was conducted by a joint team of World Bank and International Monetary Fund in October, 2002 and the report thereof was adopted by the APG in September, 2003. The 2nd Mutual Evaluation of Bangladesh was conducted by an APG team in August, 2008 and 3rd round ME was conducted by APG team in October, 2015.

2.16 The NCCT List:

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

2.17 ICRG:

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

focused on specific threats and specific risk in specific countries. If needed, these jurisdictions may be publicly identified by the FATF Plenary.

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

2.18 The Basel Committee on Banking Supervision:

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

2.18.1 Statement of Principles on Money Laundering:

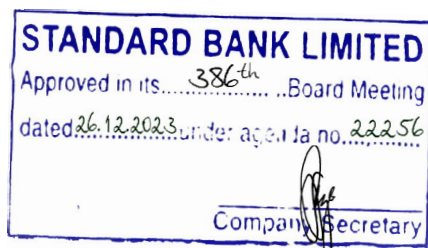
In 1988, the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention). The Statement on Prevention outlines basic policies and procedures that Managements of Banks/FIs should undertake to assist in suppressing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

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

2.18.2 Basel Core Principles for Banking:

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

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



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

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

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

2.18.3 Customer Due Diligence:

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

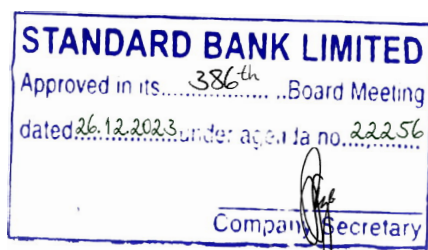
2.19 International Organization of Securities Commissioners:

The International Organization of Securities Commissioners (IOSCO) is an organization of securities commissioners and administrators that have day-to-day responsibilities for securities regulation and the administration of securities laws in their respective countries. The current membership of IOSCO is comprised of regulatory bodies from 105 countries. With regard to money laundering, IOSCO passed a “Resolution on Money Laundering” in 1992. Like other international organizations of this type, IOSCO does not have law-making authority. Similar to the Basel Committee and International Association of Insurance Supervisors (IAIS), it relies on its members to implement its recommendations within their respective countries.

2.20 The Egmont Group of Financial Intelligence Units:

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

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



terrorism, or (ii) required by national regulation, in order to counter money laundering and terrorist financing.”

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

2.21 Asia Pacific Group on Money Laundering (APG):

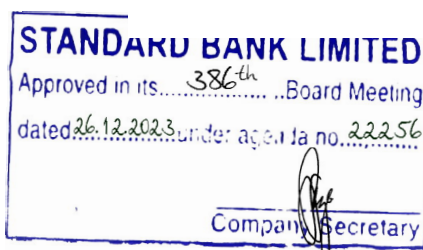
The Asia Pacific Group on Money Laundering (APG), founded in 1997 in Bangkok, Thailand, is an autonomous and collaborative international organization consisting of 40 members and a number of international and regional observers. Some of the key international organizations who participate with, and support, the efforts of the APG in the region include the Financial Action Task Force, International Monetary Fund, World Bank, OECD (Organization for Economic Cooperation and Development), United Nations Office on Drugs and Crime, Asian Development Bank and the Egmont Group of Financial Intelligence Units.

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

The APG has five key roles:

- To assess compliance by APG members with the global standards through a robust mutual evaluation program;
- To coordinate bi-lateral and donor-agency technical assistance and training in the Asia Pacific region in order to improve compliance by APG members with the global standards;
- To participate in, and co-operate with, the international anti money laundering network - primarily with the FATF and with other regional Anti Money Laundering groups;
- To conduct research and analysis into money laundering and terrorist financing trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities; and
- To contribute to the global policy development of Anti Money Laundering(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 of terrorism offences.



CHAPTER III: MAJOR NATIONAL AML & CFT INITIATIVES

3.0 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.

3.1 Founding Member of APG:

Bangladesh is a founding member of Asia Pacific Group on Money Laundering (APG) and has been participating annual plenary meeting since 1997. APG is a FATF style regional body that enforces international standards in Asia Pacific region. As a member of APG, Bangladesh is committed to implement FATF's 40 recommendations. 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.

3.2 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.

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, Money Laundering Prevention Rules 2019 has also been promulgated to make the role and responsibilities of related agencies clear specially to provide specific guidance on the implementation procedure of the provisions of the UNSCRs.

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.



3.3 Central and Regional Taskforces:

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.

3.4 Anti Money Laundering Department:

Anti-Money Laundering Department (AML/D) 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).

3.5 Bangladesh Financial Intelligence Unit:

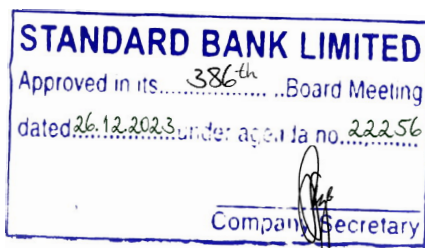
As per the provision of MLPA, 2012 Bangladesh Financial Intelligence Unit (BFIU) has been established abolishing AML/D as a national central agency to receive, analyze and disseminate STRs/SARs, CTRs and complaints. BFIU has been entrusted with the responsibility of exchanging information related to 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.

3.6 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 decades



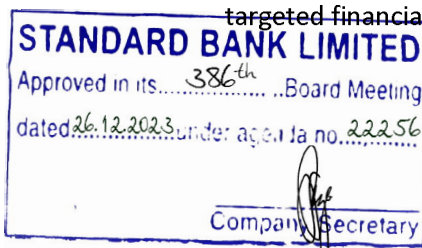
statistics from relevant agencies and identified the vulnerabilities of sectors, limitations of legal framework and weaknesses of the institutions on ML & TF.

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 consider 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.

3.7 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:

- Updating National ML & TF Risk Assessment Report regularly and introducing Risk Based Approach of monitoring and supervision of all reporting organizations.
- Deterring corruption induced money laundering considering corruption as a high risk.
- 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.
- 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.
- Discouraging illicit fund transfer by increasing pace of stolen assets recovery initiatives and or recovering the evaded tax.
- Enhancing the capacity of BFIU in identifying and analyzing emerging ML & TF cases including ML & TF risks arising from the use of new technologies.
- Enhancing compliance of all reporting agencies with special focus on new reporting agencies like NGOs/NPOs and DNFBPs.
- Expanding investigative capacity and improving the quality of investigation and prosecution of ML & TF cases to deter the criminals.
- Establishing identification and tracing out mechanism of TF& PF and fully implementation of targeted financial sanctions related to TF & PF effectively.



- Boosting national and international coordination both at policy and operational levels.
- Developing a transparent, accountable and inclusive financial system in Bangladesh.

3.8 Chief Anti Money Laundering Compliance Officers (CAMLCO) Conference:

Separate annual conferences for the Chief Anti Money Laundering Compliance Officers (CAMLCO) 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.

3.9 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.

3.10 Anti Militants and De- Radicalization Committee:

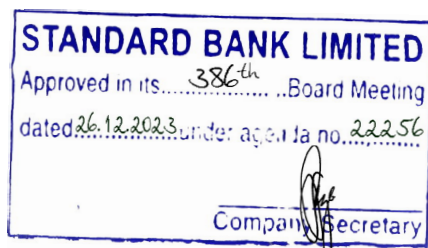
The Government of Bangladesh is very much vigilant against terrorism and violent extremism. An inter-ministerial committee headed by Minister of Home is working actively to prevent and redress of terrorism, to fight against terrorist and the terrorist organizations in a more coordinated way. The committee comprised of high officials from different ministries, law enforcement and intelligence 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.

3.11 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.

3.12 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.

3.13 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.

3.14 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.

3.15 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 every Reporting Organization-Financial Institution (RO-FI) shall conduct periodic risk assessment and forward the same to the Bangladesh Financial Intelligence Unit (BFIU) for vetting. **Rule 10** also states that RO-FI shall utilize this risk assessment report after having vetted by BFIU. 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

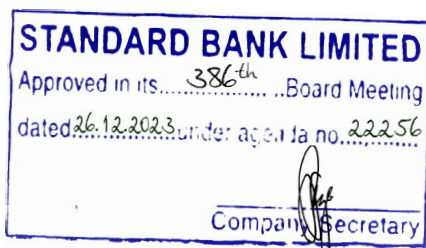
STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



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.

3.16 Memorandum of Understanding (MOU) BFIU and Other FIUs:

Money laundering and the financing of terrorism offenses are global in nature. So, it's imperative for the Financial Intelligence Units (FIUs) to extend cooperation and exchange information relating to ML, TF and related offences with authorities in other jurisdictions for effective case investigations. To enhance the cooperation with foreign counterparts, BFIU signed Memorandum of Understanding (MoU) with other FIUs. Being a member of the Egmont Group, BFIU is authorized to exchange information with 164 member FIUs through Egmont Secure Web (ESW). Going beyond its requirements as an Egmont member, BFIU has taken initiative to sign MoUs with the other FIUs, Egmont members and non-members alike, to facilitate the information exchange process and strengthen relationships with them. Until June 2020, BFIU has signed (79) seventy-nine MoUs with its counterparts.



CHAPTER IV: AML & CFT COMPLIANCE PROGRAM OF STANDARD BANK

Banking sector is one of the most vulnerable sectors for the ML, TF & PF among the financial sectors due to its indigenous nature of business, customer base, product type, delivery channel, external linkage and ownership. 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 implementation of required provisions of Acts, Rules and directives of BFIU, Standard Bank Ltd 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.

4.1 SBL AML, CFT & CPF Compliance Program:

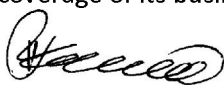
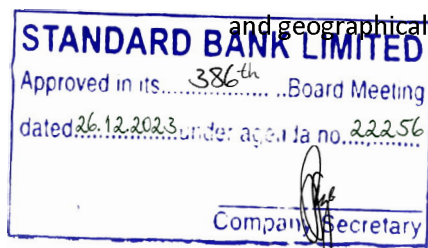
In the process of developing the compliance program, Standard Bank Ltd has paid special attention to size and range of activities, complexity of operations, and the nature and the degree of ML, TF & PF risk facing by Standard Bank Ltd. The program includes-

1. Senior Management role including their commitment to prevent ML, TF & PF;
2. Internal policies, procedure and controls- it shall include Bank's AML, CFT & CPF policy, customer acceptance policy, customer due diligence (CDD), transaction monitoring, self-assessment, independent testing procedure, employee screening, record keeping and reporting to BFIU;
3. Compliance structure includes establishment of central compliance committee (CCC), appointment of Chief Anti Money Laundering Compliance Officer (CAMLCO), Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO), Branch Anti Money Laundering Compliance Officer (BAMLCO), Deputy BAMLCO;
4. Independent audit function-it includes the role and responsibilities of internal audit on AML, CFT and CPF compliance and external audit function;
5. Awareness building program includes training, workshop, seminar for bank employees, member of the Board of Directors, owners and above all for the customers on AML, CFT and CPF issues.

4.2 Roles and Responsibilities of Board of Directors:

The Board of Directors (Board) have the following roles and responsibilities:

- shall understand their roles and responsibilities in managing ML, TF & PF risks faced by the bank as reporting institution;
- must be aware of the ML, TF & PF risks associated with business strategies, delivery channels and geographical coverage of its business products and services;



- understand the AML, CFT & CPF measures required by the laws including the MLPA, 2012 (amendment 2015) & ATA, 2009 (amendment 2012 & 2013) and the industry's standards and best practices as well as the importance of implementing AML, CFT & CPF measures to prevent the bank from being abused by money launderers and financiers of terrorism;
- 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;
- assess the implementation of the approved AML, CFT & CPF policies through regular reporting and updates by the Senior Management and Audit Committee; and
- define the lines of authority and responsibility for implementing the AML, CFT & CPF measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;
- maintain accountability and oversight for establishing AML, CFT & CPF policies and minimum standards;
- 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;
- 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;
- ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML, TF & PF;
- 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.

4.3 Senior Management Role & Responsibilities:

The Senior Management have the following roles and responsibilities:

- be aware of and understand the ML, TF & PF risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;
- 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;
- formulate AML, CFT & CPF policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by the bank and its geographical coverage;

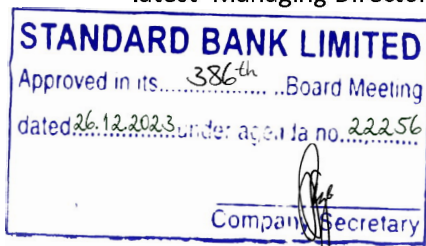


- provide periodic reporting on time to the Board on the level of ML, TF & PF risks facing the bank, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML, CFT & CPF which may have an impact on the bank;
- convey a clear signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service;
- communicate clearly to all employees on an annual basis by a statement from the CEO or Managing Director that clearly sets forth its policy against ML, TF & PF and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the bank to comply with all laws and regulations designed to combat money laundering, terrorist financing and proliferation financing;
- assign adequate resources to effectively implement and administer AML, CFT & CPF compliance programs that are reflective of the size and complexity of the bank's operations and risk profiles;
- appoint a Chief Anti-Money Laundering Compliance Officer (CAMLCO) at management level at Head Office and designate a Compliance officer at Management level at each Branch or subsidiary or Division/Department of Head Office ;
- provide appropriate level of AML, CFT & CPF training for employees at all levels throughout the Bank;
- Senior Management of Standard Bank Ltd shall advise Human Resource Division (HRD) for inclusion of AML, CFT & CPF compliance in their manual so that it helps to adopt HR policy for ensuring the compliance of AML, CFT & CPF measures by the employees of the bank. Senior Management shall also instruct HRD to develop following issues for proper implementation of AML, CFT & CPF measures:-
 - ❖ Proper administrative sanction (proportionate and dissuasive) for non-compliance of AML, CFT & CPF measures;
 - ❖ Proper weight in the annual performance evaluation of employees for extra ordinary preventive action vis a vis for non-compliance;
 - ❖ Written procedure to recover the fined amount from the concerned branch if the fine imposed by the BFIU on Bank for the performance of the Branch ;

Senior management of Standard Bank shall be responsive of the level of Money Laundering, Terrorist Financing and Proliferation Financing Risk when the bank is exposed to and take a view whether the bank is equipped to mitigate that risk effectively.

4.4 Statement of Commitment of Managing Director (MD) & CEO:

Standard Bank communicates to all employees at the beginning of every year by the message from the Managing Director & CEO that clearly sets forth Standard Bank's policy against ML, TF & PF and any activity which facilitates Money Laundering or the funding of terrorist or criminal activities. The latest Managing Director CEO's message already communicated to all the employees of SBL through



Instruction Circular No. 01/2022 dated January 02, 2022 which covers the following issues:-

- ❖ Bank's policy or strategy to prevent ML, TF & PF;
- ❖ Emphasize on effective implementation of bank's AML, CFT & CPF compliance program;
- ❖ Clear indication of balance between business and compliance, risk and mitigating measures;
- ❖ Compliance is the responsibility of each employee during their normal course of assignment and ignorance shall not be considered as the excuse for non-compliance;
- ❖ Point of contact for clarification in case of any ambiguity arise;
- ❖ Consequences of non-compliance as per human resources (HR) policy of the bank.
- ❖ Special attention to COVID-19 related Money Laundering and Terrorist Financing Risks and risk mitigation policy response.

As per BFIU circular 26 dated 16.06.2020, "the account of PEPs/Influential Person/Chief Executives or Top Level Officials of any international organization and their close family members or close associates account must take approval from CAMLCO before opening". This instruction has conveyed to all the Branches vide AML & CFT Division Instruction Circular no: SBL/HO/AML & CFT/ Instruction Circular/2020/1159 dated June 30, 2020.

4.5 Customer Acceptance Policy:

Standard Bank has developed a clear Customer Acceptance Policy which was approved at the 255th Board meeting dated March 03, 2022 vide memo no 20111 with effect from 3rd March,2022. This customer acceptance policies and procedures have to be implemented to identify the types of customer that are likely to pose a higher risk of ML and TF pursuant to the Bank's risk assessment. When assessing risk, Branch should consider the factors relevant to the situation, such as a 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 basis 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.

4.6 Policy for rejection of customer:

- a) No account shall be opened in anonymous or fictitious name.
- b) Standard Bank will not establish any kind of correspondence relationship with shell Bank.



- c) 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.

4.7 ML & TF Risk Assessment:

Assessing AML, CFT & CPF risk is, therefore one of the most important steps in creating a good AML, CFT & CPF 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. Standard Bank develops systems and procedures to detect, monitoring and report the riskier customers and transactions. Considering the issues, Branch can assess their risk level and the action taken against mitigation of risk. Standard Bank has developed ML & TF risk assessment procedure including the risk register in this guideline.



CHAPTER V: ML & TF RISK ASSESMENT OF STANDARD BANK

The regulatory framework for combating money laundering and terrorist financing is applicable in the form of AML & CFT Regulations as amended from time to time. Keeping in view of growing sensitivities on domestic and international front, there is need to focus on the areas where related risks are relatively high in order to allocate resources in the most effective way. Accordingly, following guidelines are aimed at providing enabling environment for effective implementation of risk based approach considering banks' internal policies, procedures and risk parameters etc.

5.1 Risk

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

5.2 Assessing Risk

Banks should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks for customers, countries or geographic areas, products, services and transactions or delivery channels. They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities.

5.3 Risk Identification

Risk identification is the process of documenting any risks that could keep an organization or program from reaching its objective. It is the first step in the risk management process, which is designed to help companies understand and plan for potential risks.

Risk identification allows businesses to prepare for potential harmful events and minimize their impact before they occur. It involves not just determining the possible risks, but also documenting and sharing them with stakeholders. This documentation serves as evidence of the company's risk management strategy.

5.4 Risk Assessment process

Having identified the risks involved, they need to be assessed or measured in terms of the chance (likelihood) they will occur and the severity or amount of loss or damage (impact) which may result if they do occur. The risk associated with an event is a combination of the chance (likelihood) that the event will occur and the seriousness of the damage (impact) it may do.



5.4.1 Methodology of Risk Assessment

Money Laundering and Terrorist Financing Risk Assessment Committee of Standard Bank Ltd. has rated each risk element by-

- the chance of the risk happening – **'likelihood'**
- the amount of loss or damage if the risk happened – **'impact' (consequence)**.

5.4.1.1 Likelihood Scale

A likelihood scale refers to the potential of an ML & TF risk occurring in the business for the particular risk being assessed. Three levels of risk are shown in the following Table, but the Bank can have as many as they believe are necessary:

Frequency	Likelihood of an ML & TF risk
Very likely	Almost certain: it will probably occur several times a year
Likely	High probability it will happen once a year
Unlikely	Unlikely, but not impossible

Table: Likelihood Scale

5.4.1.2 Impact of Scale

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. It does not cover everything and it is not prescriptive. Impact of an ML & TF risk could, depending on individual business circumstances, be rated or looked at from the point of view of:

- how it may affect the business (if through not dealing with risks properly the entity suffer a financial loss from either a crime or through fines from the regulator)
- the risk that a particular transaction may result in the loss of life or property through a terrorist act.
- the risk that a particular transaction may result in funds being used for any of the following: corruption, bribery, smuggling of goods/workers/immigrants, banking offences, narcotics offences, psychotropic substance offences, illegal arms trading, kidnapping, terrorism, theft, embezzlement, or fraud, forgery, extortion, smuggling of domestic and foreign currency, black marketing.
- the risk that a particular transaction may cause suffering due to the financing of illegal

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




drugs

- reputational risk – how it may affect the business if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being shunned by the community of customers
- how it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.

Three levels of Impact are shown in the following table, but the branch/department can have as many as they believe are necessary:

Consequence	Impact – of an ML & TF risk
Major	Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.
Moderate	Moderate level of money laundering or terrorism financing impact.
Minor	Minor or negligible consequences or effects.

Table: Impact of Scale

5.5 Risk matrix and risk score

A risk matrix has been developed combining of LIKELIHOOD and IMPACT in order to obtain risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the risk matrix and risk score table shown below. Four levels of risk or score are shown in the following figure and table, but the bank can have as many as they believe are necessary.



 Very Likely Likely Unlikely What is the chance it will happen	Medium 2	High 3	Extreme 4
	Low 1	Medium 2	High 3
	Low 1	Low 1	Medium 2
	Minor	Moderate	Major
	 Impact		

Table: Risk Matrix and Score

Four levels of score have been shown in the matrix. The implication of each score is as follows:

Rating/Score	Impact – of an ML & TF risk
Extreme 4	Risk almost sure to happen and/or to have very serious consequences. Response: Do not allow transaction to occur or reduce the risk to acceptable level.
High 3	Risk likely to happen and/or to have serious consequences. Response: Do not allow transaction until risk reduced.
Medium 2	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk.
Low 1	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

5.6 Risk Assessment and Management Exercise

From the above discussion, the banks will have an idea to calculate risk score by blending likelihood and impact, the risk matrix and risk score and can assess the risks of individual customer, product/service, delivery channel and risks related to geographic region by using the simplified risk management worksheet. It can also fix up its necessary actions against the particulars outcomes of risks. All the exercises done by the banks would be called together "Risk Register" (Discussed in the chapter VII of this guidelines).

5.7 Risk Treatment

Manage the business risks by -

- ◆ minimizing and managing the risks; and
- ◆ applying strategies, policies and procedures

Manage the regulatory risks by -

- ◆ putting in place systems and controls; and
- ◆ carrying out the risk plan and AML & CFT program

This stage is about identifying and testing methods to manage the risks the bank may have identified and assessed in the previous process. In doing this they will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk. Examples of a risk reduction or treatment steps are:

- setting transaction limits for high-risk products;
- having a management approval process for higher-risk products;



(Handwritten signature)

(Handwritten signature)

- process to place customers in different risk categories and apply different identification and verification methods;
- not accepting customers who wish to transact with a high-risk country

5.8 Monitoring and Review

Keeping records and regular evaluation of the risk plan and AML & CFT program is essential. The risk management plan and AML & CFT program cannot remain static as risks change over time; for example, changes to customer base, products and services, business practices and the law.

Once documented, the entity should develop a method to check regularly on whether AML & CFT program is working correctly and well. If not, the entity needs to work out what needs to be improved and put changes in place. This will help keep the program effective and also meet the requirements of the AML & CFT Acts and respective Rules.



CHAPTER VI: ML & TF RISK MANAGEMENT OF STANDARD BANK

6.1 Risk Management

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

6.2 Risk management and mitigation

Banks should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified. They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures must be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities.

Higher risk - Where higher risks are identified banks should be required to take enhanced measures to manage and mitigate the risks.

Lower risk - Where lower risks are identified, countries may allow banks to take simplified measures to manage and mitigate those risks.

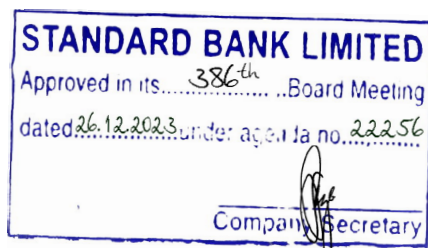
6.3 Which Risk do Banks Needs to Manage?

For the ML & TF aspects, BFIU expects a risk management practice to address two main risks: business risk and regulatory risk.

6.3.1 Business risk

Business risk is the risk that your business may be used for ML&TF. The banks must assess the following risks in particular:

- **customer risks** - Identifying risk determinants while establishing relationships with customer;
- **products or services risks** - Predicting risk attributes resulting from customer's need for financial services and appropriate controls;
- **business practices and/or delivery method risks**- Identifying risks associated with delivery channels which may vary from customer to customer depending on their needs;



- **country or jurisdictional risks** - Risks resulting from customer geographic presence and jurisdiction in which the customer is operating.

6.3.2 Regulatory risk

Regulatory risk is associated with not meeting all obligations of banks under the Money Laundering Prevention Act, 2012(amendment 2015), Anti Terrorism Act, 2009 (amendment 2012 & 2013) (including all amendments), the respective Rules issued under these two acts and instructions issued by BFIU. Examples of regulatory obligations are failure to report STR/SAR, unable or inappropriately verification of customers and lacking of AML & CFT program (how a business identifies and manages the ML & TF risk it may face) etc.

It is unrealistic that a bank would operate in a completely ML & TF risk-free environment. Therefore, it is suggested that a bank shall identifies the ML&TF risk it faces, and then works out the best ways to reduce and manage that risk.

6.4 Risk Management Process

In assessing and mitigating ML & TF risk, the bank should consider a wide range of financial products and services, which are associated with different ML & TF risks.

6.4.1 Risk Identification

The first step is to identify what ML & TF risks exist in a bank when providing designated services. Some examples of ML & TF risks associated with different banking activities:

Retail banking: provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.

Corporate banking: where banks provide corporate finance and corporate banking products and investment services to corporations, governments and institutions

Wealth management: culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.

Investment banking: layering and integration transfer of assets between parties in exchange for cash or other assets, global nature of markets.

Correspondent banking: high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not



comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved regarding the ownership of a bank.

6.4.1.1 Business Risks

A bank must consider the risk posed by any element or any combination of the elements listed below:

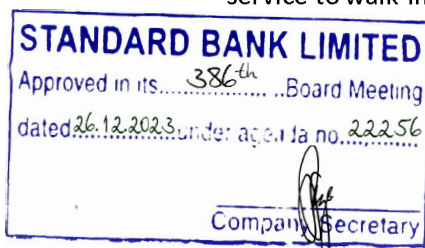
Customers

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

- a new customer;
- a new customer who wants to carry out a large transaction;
- a customer or a group of customers making lots of transactions to the same individual or group;
- a customer who has a business which involves large amounts of cash;
- a customer whose identification is difficult to check;
- a customer who brings in large amounts of used notes and/or small denominations;
- customers conducting their business relationship or transactions in unusual circumstances, such as:
 - significant and unexplained geographic distance between the institution and the location of the customer,
 - frequent and unexplained movement of accounts to different institutions,
 - frequent and unexplained movement of funds between institutions in various geographic locations;
- a non- resident customer;
- a corporate customer whose ownership structure is unusual and excessively complex;
- customers that are Politically Exposed Persons (PEPs) or Influential Persons (IPs) or Head of international organizations and their family members and close associates;
- customers submits account documentation showing an unclear ownership structure;
- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income.

Products and services

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



- mobile banking.

Business practices/delivery methods

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

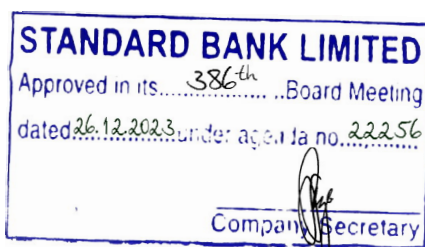
Channels Countries it does business in/with (jurisdictions)

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

6.4.1.2 Regulatory Risks

This risk is associated with not meeting the requirements of the Money laundering Prevention Act, 2012 (amendment 2015), Anti-Terrorism Act, 2009 (amendment 2012 & 2013) (including all amendments) and instructions issued by BFIU. Examples of some of these risks are:

- customer/beneficial owner identification and verification not done properly;
- failure to keep record properly;
- failure to scrutinize staffs properly;
- failure to train staff adequately;
- not having an AML & CFT program;
- failure to report suspicious transactions or activities;
- not submitting required report to BFIU regularly;
- not having an AML & CFT Compliance Officer;
- failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs);
- not complying with any order for freezing or suspension of transaction issued by BFIU, BB;
- not submitting accurate information or statement requested by BFIU, BB.



6.5 Risk Management Strategies

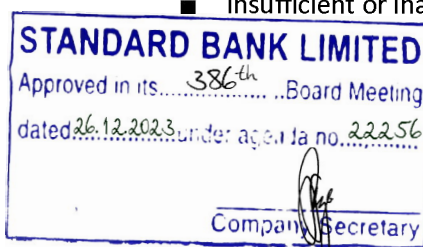
The banks may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:

- reviews at senior management level of the bank's progress towards implementing stated ML & TF risk management objectives;
- clearly defined management responsibilities and accountabilities regarding ML & TF risk management;
- adequate staff resources to undertake functions associated with ML & TF risk management
- specified staff reporting lines from ML & TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system;
- procedural controls relevant to particular designated services;
- documentation of all ML & TF risk management policies;
- a system, whether technology based or manual, for monitoring the bank's compliance with relevant controls;
- policies to resolve identified non-compliance;
- appropriate training program(s) for staff to develop expertise in the identification of ML & TF risk(s) across the bank's designated services;
- an effective information management system which should:
 - produce detailed and accurate financial, operational and compliance data relevant to ML & TF risk management;
 - incorporate market information relevant to the global AML & CFT environment which may assist the banks to make decisions regarding its risk management strategy;
 - enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML & CFT Compliance Officer) within the banks;
 - allow the banks to identify, quantify, assess and monitor business activities relevant to ML & TF risk(s);
 - allow the banks to monitor the effectiveness of and compliance with its internal AML & CFT systems and procedures;
 - allow the banks to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.

6.6 Ongoing Risk Monitoring

A bank's ongoing monitoring of its risk management procedures and controls may also alert the bank to any potential failures including (but not limited to):

- failure to include all mandatory legislative components;
- failure to gain board and/or executive approval of the AML & CFT program;
- insufficient or inappropriate employee due diligence;



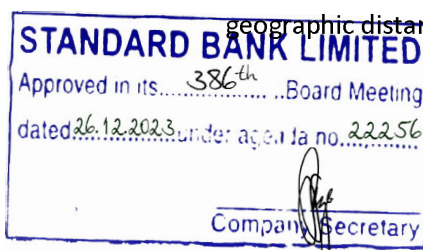
- frequency and level of risk awareness training not aligned with potential exposure to ML & TF risk(s);
- changes in business functions which are not reflected in the AML & CFT program (for example, the introduction of a new product or distribution channel);
- failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML & CFT program;
- legislation incorrectly interpreted and applied in relation to a customer identification procedure;
- customer identification and monitoring systems, policies and procedures that fail to:
 - prompt, if appropriate, for further identification and/or verification when the ML & TF risk posed by a customer increases;
 - detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;
 - take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;
 - take appropriate action where the identification document provided is neither an original nor a certified copy;
 - recognize foreign identification documentation issued by a high risk jurisdiction
 - record comprehensive details of identification documents, for example, the date of issue;
 - consult appropriate resources in order to identify high-risk customers;
 - identify when an expired or old identification document (for example, a driver's license) has been used;
 - collect any other name(s) by which the customer is known;
- lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers;
- lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
 - customer identification policies, procedures and systems;
 - identifying potential ML & TF risks
- acceptance of documentation that may not be readily verifiable.

6.7 Higher Risk Scenario

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations include the following:

a. Customer risk factors

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer);



(Handwritten signature)

(Handwritten signature)

- Non-resident customers;
- Legal persons or arrangements that are personal asset-holding vehicles;
- Companies that have nominee shareholders or shares in bearer form;
- Business that are cash-intensive;
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

b. Country or geographic risk factors

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML & CFT systems;
- Countries subject to sanctions, embargos or similar measures;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity;
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

c. Product, service, transaction or delivery channel risk factors

- Private banking;
- Anonymous transactions (which may include cash);
- Non-face-to-face business relationships or transactions;
- Payment received from unknown or un-associated third parties.

6.7.1 Specific High Risk Elements and Recommendations for EDD

Some of the relatively high risk elements identified by AMLD and recommended actions for EDD may be as under:

Sl. No.	Customers	Recommendations for EDD
01	NPOs/NGOs/Charities, Trusts, Clubs, Societies, and Associations etc.	In relation to these customers, branches may: <ul style="list-style-type: none"> i. obtain a declaration from Governing Body / Board of Trustees / Executive Committee / sponsors on ultimate control, purpose and source of funds etc; ii. obtain an undertaking 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; and iii. obtain a fresh Resolution of the Governing Body/Executive Committee of the entity in case of change in person(s) authorized to operate the account.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




Sl. No.	Customers	Recommendations for EDD
02.	Housewife accounts	In relation to housewife accounts, branches may- i. obtain a self-declaration for source of fund. Besides this branch may obtain beneficial ownership information; ii. Update details of funds providers, if any along with customer's profile; and iii. Identify and verify funds providers if monthly credit turnover exceeds an appropriate threshold to be decided by banks.
03.	Landlords	In relation to such customers, branches may apply any recommend methods for assessment of source of funds/income e.g. collecting rent agreement copy etc.
04.	PEPs/IPs	In relation to such customers, branches may apply CDD as well as EDD process as this is a High Risk Account.
05.	Student Account	In relation to such customers, branches should- i) Obtain purpose of opening account; ii) Source of fund; iii) Beneficial owner information, if needed. iv) Regular monitoring of transaction.
	Products & Services	Recommendations for EDD
01.	Online transactions	In relation to online transactions, Branches should pay special attention to geographical factors / locations for movement funds.
	Delivery Channels	Recommendations for EDD
01.	Wire transfers	In relation to wire transfers, branches may: i. monitor such transactions on enhanced basis by applying relatively stringent thresholds, as deemed appropriate; and ii. Ensure that funds transfers which are out of character/ inconsistent with the history, iii. pattern, source of earnings and purpose, shall be viewed with suspicion and properly investigated for appropriate action, as per law.

6.8 Low Risk Scenario

There are circumstances where the risk of money laundering or terrorist financing may be lower. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following :

a. Customer risk factors

- ◆ Banks – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those



requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements;

- ◆ Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- ◆ Public administrations or enterprises.

b. Product, service, transaction or delivery channel risk factors

- ◆ Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

c. Country risk factors

- ◆ Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML & CFT systems;
- ◆ Countries identified by credible sources as having a low level of corruption or other criminal activity. In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

Note that having a lower money laundering and terrorist financing risk for identification and verification purposes does not necessarily mean that the same customer poses lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

6.9 Risk Variables

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

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

6.10 Counter Measures for Risks

- a. Enhanced due diligence measures
- b. Simplified CDD measures
- c. Ongoing Due Diligence

(The above mentioned points are specified in the paragraph 9.3 of Chapter IX of this guidelines)



A handwritten signature in blue ink.



A handwritten signature in blue ink.

CHAPTER VII: RISK REGISTER OF STANDARD BANK

7.1 Risk Register

In line with the above methodology, the Money Laundering and Terrorist Financing risk register of Standard Bank Ltd. is as follows:

7.1.1 Business Risk

Business risk is the risk that business may be used for Money Laundering and Terrorist Financing. Following are some examples of ML & TF risk the Bank faces and the possible ways to reduce and manage those risks.

a. ML & TF risk register for customer

Standard Bank will need to assess the customer-base. Depending on the number and types of customers, the inherent ML & TF risk will differ. Certain types of customers can increase the ML & TF risk, especially when there are large numbers of these customers. Examples are large corporations that do international business, corporations with complex structures, non-resident customers, or customers from high-risk countries. On the other hand, when the customer-base consists mainly of domestic retail customers or small enterprises, the risk can be lower.

For the purpose of the ML & TF risk assessment, the Branch should define type of customer who carries an increased ML & TF risk. Based on its own criteria, Branch will determine whether a customer poses a higher risk. These are some example of ML & TF risk that Bank may face and the possible ways to reduce and manage those risks:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer	Very Likely	Minor	Medium 2	a) Sanction list must be checked before opening account. b) Comply CDD. c) Complete KYC perfectly. d) Input TP as per authentication of the source of fund of the client. e) Physical verification is required.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
A new customer who wants to carry out a large transaction (i.e. transaction above CTR threshold or below the threshold)	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Sanction list must be checked before opening account. a) Confirm the source of fund. b) Identify beneficial owner, if any. c) Input TP as per nature of business and source of fund. d) Obtain supporting document against the large transaction. e) Complete CDD accurately.
Walk-in customer (beneficiary is government/ semi government/ autonomous body/ bank & NBF) in case of issuing PO,DD, etc.	Very Likely	Minor	Medium 2	<ul style="list-style-type: none"> a) Check Sanction list. b) Ensure the purpose of transaction and source of fund of the applicant. c) Complete the KYC of the applicant perfectly.
Walk-in customer (beneficiary is other than government/ semi government/ autonomous body/ bank & NBF) in case of issuing PO,DD, etc.	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Check Sanction list. b) Identify the reason of transaction. c) Complete and accurate information of the applicant and beneficiary.
Non-resident customer (Bangladeshi)	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Sanction list must be checked before opening account. b) Maintain proper documentation as per Foreign Exchange guideline and circulars issued by regulatory authority. c) Complete KYC accurately.
A customer making series of transactions to the same individual or entity	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Monitoring the TP of the client. b) Justify the source of fund. c) Generate the statement and review the transactions. d) Monitoring the online transactions exceeding the limits declared in their TPs. e) Justify the link between the two parties.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Customer				
Customer involved in outsourcing business	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Monitoring the inward remittance in favor of the client. b) Confirm the work area of outsourcing income. c) Monitoring the transaction on regular basis. d) Comply the CDD. e) Collect the information of KYCC. f) Monitoring the countries/jurisdiction from which the fund comes/receives.
Customer appears to do structuring to avoid reporting threshold	Likely	Major	High 3	<ul style="list-style-type: none"> a) Monitoring the cash transaction on regular basis. b) Obtain justification of transaction. c) If found any suspicious then report as STR.
Customer appears to have accounts with several banks in the same area	Likely	Major	High 3	<ul style="list-style-type: none"> a) Confirm the source of fund of the client. b) Monitoring transaction pattern. c) Obtain justification from the customer regarding maintains of several accounts. d) Complete CDD and EDD perfectly.
Customer who shows curiosity about internal systems, controls and policies on internal and regulatory reporting	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Monitoring the nature of business of the client. b) Monitoring the nature of transaction. c) If found any suspicious then report as SAR.
Customer is the subject of a Money Laundering or Financing of Terrorism investigation by the order of the court.	Likely	Major	High 3	<ul style="list-style-type: none"> a) Update the KYC. b) Regular monitoring of the client transaction. c) Take necessary steps as per court order against the client (if any).


Risk	Likelihood	Impact	Risk Score	Treatment/Action
Negative news about the customers' activities/business in media or from other reliable sources.	Likely	Major	High 3	a) Inform AML & CFT Division/CAMLCO's Office immediately. b) Update KYC. c) Regular monitor transaction. d) If seems to be suspicious submit STR to CCC/AML & CFT Division/ CAMLCO's Office for onward submission to BFIU.
Customer is secretive and reluctant to meet in person	Unlikely	Major	Medium 2	a) Visit customer address and try to communicate. b) Regular monitoring of transaction. c) If found suspicious then submit STR.
Customer is a mandate who is operating account on behalf of another person/ company.	Likely	Moderate	Medium 2	a) Proper CDD of the mandatee. b) Relationship between the account holder and mandate. c) Proper KYC of the mandate. d) Find out the reason for providing mandate. e) Duration of mandate. f) Monitoring of transaction.
Large deposits in the account of customer with low income	Likely	Major	High 2	a) Request to client for submitting supporting document regarding the large transaction. b) If failed to submit the document take necessary steps for STR.
Customers about whom BFIU seeks information (individual)	Very Likely	Moderate	High 3	a) Regular monitor of the client. b) Update KYC. c) Check whether there is any negative information about the customer in media. d) If suspicious found then submit STR.
A customer whose identification is difficult to check	Likely	Major	High 3	a) Verify the identity of the customer through bank officials. b) For new account if identification not possible then do not open account. c) If existing account then close the account prior notice to customer.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Significant and unexplained geographic distance between the bank and the location of the customer.	Likely	Major	High 3	a) Purpose of account opening. b) Complete the CDD. c) Keep transaction especially online transaction under monitoring.
Customer is a foreigner	Likely	Major	High 3	a) Check the Sanction list before opening the account. b) Purpose of opening account in Bangladesh. c) Apply EDD. d) Follow the instruction of Foreign Exchange guideline and circulars of FEPD.
Customer is a minor	Very Likely	Minor	Medium 2	a) Obtain birth certificate. b) Complete the CDD of guardian and the minor. c) Reason for opening minor account. d) Identify the beneficial ownership.
Customer is Housewife doing small transaction	Very Likely	Minor	Medium 2	a) Confirm source of fund. b) Reason for opening account. c) TP will be low. d) Monitoring of transaction on regular basis.
Customer is Housewife doing large transaction	Likely	Major	High 3	a) Confirm source of fund. b) Obtain supporting document against the large transaction. c) Identify the beneficial owner. d) Obtain KYC of beneficial owner. e) Monitoring of transaction on regular basis.
Customers that are politically exposed persons (PEPs) or influential persons (IPs) or chief / senior officials of international organizations and their family members and close associates	Likely	Major	High 3	a) Take the Senior Management permission before opening the account. b) Check whether the source of fund commensurate with the designation. c) Complete the EDD. d) Follow the instruction of Foreign Exchange guideline and FEPD circulars.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer opens account in the name of his/her family member who intends to credit large amount of deposits.	Likely	Major	High 3	<ul style="list-style-type: none"> a) Confirm of the source of fund. b) Monitor the transactions. c) Find out the beneficial owner. d) Complete KYC of customer and beneficial owner. e) Perform CDD of customer and beneficial owner.
Customers doing significant volume of transactions with higher-risk geographic locations.	Likely	Major	High 3	<ul style="list-style-type: none"> a) Reason for opening account. b) Regular monitoring of online transaction. c) Install TP as per source of fund of the client. d) Find out the Reason by supporting documents.
A customer who brings in large amounts of used notes and/or small denominations.	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Justification of nature of business. b) Whether the nature of business consistence with this condition or not.
Customer dealing in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain source of fund with supporting documents. b) Obtain customer's customer (KYCC). c) Regular monitoring of transaction on regular basis. d) Obtain the membership certificate issued from relevant trade body i.e. membership of jewelry Association in case of jewelry business.
Customer is a money changer/ courier service agent / travel agent	Likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain correct and complete information regarding business. b) Follow the instruction of Foreign Exchange guideline and FEPD circulars (if needed). c) Identify the source of fund with supporting documents. d) Obtain license from competent authority.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer is involved in business defined as high risk in KYC profile by BFIU, but not mentioned above	Likely	Major	High 3	<ul style="list-style-type: none"> a) Complete CDD as well as EDD. b) Obtain information about necessary documents with respect to nature of business. c) Regular monitoring on regular basis.
Customer is involved in Manpower Export Business	Likely	Major	High 3	<ul style="list-style-type: none"> a) Obtain supporting documents as a source of fund regarding their nature of business. b) Complete proper CDD. c) Check license issued by Ministry of Expatriates Welfare and Overseas employment and membership certificate. d) Monitoring of Transaction. e) Check Sanction list. f) Keep in touch with media regarding the customer. g) Perform EDD
Customer has been refused to provide banking facilities by another bank	Likely	Major	High 3	<ul style="list-style-type: none"> a) Check the genuineness of NID/Passport etc. with recent photograph. b) Complete CDD as well as EDD. c) Try to know the reason of refusal. d) Check additional ID like driving license, E-TIN, Utility bill, etc.
Accounts opened before 30 April, 2002	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Update KYC profile. b) Obtain recent photograph. c) Obtain photo ID d) If KYC not possible mark as dormant as per master circular of BFIU. e) Monitor transaction regularly.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customers with complex accounting and huge transaction	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Monitor transaction regularly and justify whether it commensurate with source of fund. b) Obtain supporting documents of income like sales proceeds, balance sheet, etc. c) If suspicious, then perorated as STR.
Receipt of donor fund , fund from foreign source by micro finance institute (MFI)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Check Sanction list of the donor. b) Obtain supporting documents (approval from appropriate authority). c) Monitor transaction. d) Identification of beneficial owner. e) If suspicious, then perorated as STR.
Customer which is a reporting organization under MLP Act 2012 appears not complying with the reporting requirements (MFI) as per reliable source	Unlikely	Moderate	Low 1	<ul style="list-style-type: none"> a) Obtain declaration whether the organization follow the instruction of MLP guideline. b) Complete the CDD of the customer properly. c) Monitor the transactions.
Wholesale Banking Customer				
Entity customer having operations in multiple locations	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Obtain information regarding their operation in multiple locations. b) Monitor the transactions regularly. c) Check their balance sheet. d) If suspicious, then perorated as STR.
Customers about whom BFIU seeks information (large corporate)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Try to know the reason of seeking information by BFIU from reliable source or media. b) Monitoring of transaction. c) Obtain update KYC of the customer. d) Perform EDD

STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary





Risk	Likelihood	Impact	Risk Score	Treatment/Action
Owner of the entity that are Influential Persons (IPs) and their family members and Regular associates	Likely	Major	High 3	a) Take prior approval from Senior Management before opening account. b) Obtain CDD as well as EDD. c) Regularly monitoring of transaction.
A new customer who wants to carry out a large transaction. (i.e. transaction amounting 10 million or above)	Very Likely	Moderate	High 3	a) Obtain information regarding source of fund with supporting documents. b) Identify the beneficial owner. c) Check whether TP of customer Commensurate with nature of business and transaction pattern. d) Check TP. e) Check cash flow statement and sales register. f) Verify the business address of the customer.
A customer or a group of customers making lots of transactions to the same individual or group (wholesale).	Very Likely	Moderate	High 3	a) Obtain information of KYCC. b) Check TP. c) Check online transaction. d) Obtain justification of such transaction. e) Review of Statement regular basis.
A customer whose identification is difficult to check.	Unlikely	Major	Medium 2	a) Personally visit the place and try to identify the customer. b) If not satisfied don't open the account. c) In case of existing customer close the account prior notice to customer. d) Obtain information regarding the customer from other reliable sources.
Owner of the entity that are Politically Exposed Persons (PEPs) or chief / senior officials of International Organizations and their family members and close associates.	likely	Major	High 3	a) Obtain Senior Management approval before establishment of relationship. b) Complete Enhance Due Diligence. c) Follow the instruction of Foreign Exchange guideline and FEPD circulars.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Owner of the entity that are Politically Exposed Persons (PEPs) or chief / senior officials of International Organizations and their family members and close associates.	likely	Major	High 3	d) Regular monitoring of transaction.
Charities or NPOs (especially operating in less privileged areas).	likely	Major	High 3	a) Identification of beneficial owner. b) Complete CDD. c) Monitoring of transactions. d) Identification of source of fund from reliable sources. e) Obtain the permission/ license required by customer from competent authority. f) Perform EDD.
Credit Card Customer				
Customer who changes static data frequently.	Likely	Major	High 3	a) Obtain supporting documents for changing information. b) Obtain customer acknowledgement by sending letter to old and new address. c) Monitoring of transactions.
SBL Tijarah Card customer.	Very Likely	Moderate	High 3	a) Check Sanction list before providing the credit card. b) Collect required documents as per PPG and Bank Policy. c) Obtain KYC. d) Verify the address and contact number. e) Obtain CIB report. f) Confirm that whether the client is using other card or not. g) Regular monitoring of transaction.
Customer doing frequent transaction through card (Prepaid & Credit card) and making quick adjustments.	Very Likely	Moderate	High 3	a) Monitoring of transaction. b) Justification of transaction with his income. c) If found suspicious then submit STR.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Prepaid Card customer	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Check Sanction list. b) Collect CIB report. c) Obtain KYC. d) Verify the address and contact number. e) Collect required document as per PPG and bank policy. f) Check whether customer already availing bank card. g) Monitoring of transaction.
Customer doing frequently online cash transaction in a same time from credit card but declined	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Talk with the client immediately and confirm whether he is doing transaction or not. b) If found anything wrong then take necessary steps. c) Regular monitoring of transaction.
International Trade Customer				
A new customer (Outward remittance-through SWIFT)	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Check Sanction lists. b) Purpose of the remittance. c) Collect supporting documents. d) Obtain KYC. e) Follow the instruction of Foreign Exchange guideline and FEPD circular.
A new customer (Import/Export)	Very Likely	Moderate	High 3	<ul style="list-style-type: none"> a) Screening against Sanction List. b) Obtain CDD. c) Old customer of other bank: Obtain certificate from previous bank on "no overdue or outstanding bill of entry" d) New Customer: Confirm that all relevant documents including IRC/ERC are in place. e) Follow the instruction of foreign exchange guideline and FEPD circulars. f) Physical verification, where necessary.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
A new customer (Inward remittance-through SWIFT)	Very Likely	Minor	Medium 2	a) Check the SANCTION list. b) Obtain KYC/CDD of the beneficiary. c) Purpose of the remittance with supporting documents. d) Collect "Form C" where applicable. e) Follow the instruction of Foreign Exchange guideline and other circulars.
A new customer who wants to carry out a large transaction(Import/Export)	Likely	Moderate	Medium 2	a) Obtain CDD. b) Obtain respective IRC/ERC issued mentioning bank. c) If customer is old for other bank then collect "no overdue or outstanding bill of entry". d) Follow the instruction of foreign exchange guideline and FEPD circulars.
A new customer who wants to carry out a large transaction (Inward/outward remittance)	Unlikely	Major	Medium 2	a) Obtain KYC/CDD of the client. b) Obtain information regarding the transaction related to his/her nature of business. c) Follow the instruction of foreign exchange guideline and FEPD circulars.
A customer wants to conduct business beyond its line of business (import/export/ remittance)	Unlikely	Major	Medium 2	a) Obtain KYC of the customer. b) Obtain information regarding the diversification of the business. c) Check the justification of diversification of business. d) If suspicious, then perorated as STR.
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates	Likely	Major	High 3	a) Check the UN/OFAC/EU & other Sanction List and local black list issued by Competent Authority. b) Obtain Enhanced Due Diligence (EDD). c) Obtain CAMLCO's approval before establishing relationship.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Owner/ director/ shareholder of the customer is influential person(s) or their family members or close associates				d)Regular monitoring of transaction. e) Check whether the source of fund commensurate with the designation/position.
Correspondent Banks	Likely	Major	High 3	a) Follow the instruction of the master circular BFIU circular no. 26 at the time of establishing relationship. b) Obtain information regarding nature of business of the correspondence/ respondent bank. c) Update KYC on regular basis
Money services businesses (remittance houses, exchange houses)	Likely	Major	High 3	a) Follow the instruction of the master circular BFIU circular no. 26. b) Obtain information regarding the correspondence/ respondent bank. c) Update KYC on regular basis.

b. ML & TF Risk Register for Products & Services

A comprehensive ML & TF risk assessment must take into account the potential risks arising from the transactions, products and services that the Standard Bank offers to its customers and the way these products and services are delivered to the customer. The Branch should pay particular attention to ML & TF risk which may arise from the application of new technologies. In identifying the risks of transactions, products, and services, the following factors are some example of ML & TF risk that Bank may face and the possible ways to reduce and manage those risks:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Retail Banking Product				
Accounts for students where large amount of transactions are made (student file)	Likely	Major	High 3	a)Obtain purpose of opening account with supporting document if needed. b)If student is a minor then collect birth certificate and collect guardian information with documents.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary

[Handwritten Signature]

[Handwritten Signature]

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Accounts for students where large amount of transactions are made (student file)				c) Obtain information regarding the beneficial owner. c) Obtain the reason behind the large transaction. Obtain TP related with the source of fund.
Locker Service	Likely	Major	High 3	a) Make sure customer have maintained account with us. b) Obtain KYC of the client. c) Confirm the source of fund. d) Update KYC periodically. e) Monitor customer's activity when he/she is using locker.
Foreign currency endorsement in Passport	Very Likely	Moderate	High 3	a) Check the visa of the customer. b) Follow the instruction of foreign exchange guideline and circulars regarding endorsement. c) Complete the TM form with duly signed by the customer.
Large transaction in the account of under privileged people	Unlikely	Major	Medium 2	a) Obtain CDD of the customer. b) Obtain documents regarding source of fund. c) Justification from the customer regarding the purpose of transaction.
MTDR (less than 2 million)	Very Likely	Minor	High 3	a) Obtain CDD of the customer. b) Obtain information regarding the source of fund.
MTDR (2 million and above)	Likely	Moderate	Medium 2	a) Obtain CDD of the customer. b) Obtain information regarding the source of fund. c) If source of fund is not provided by the customer. d) Check customer has other FDR maintaining with the bank.
Special scheme deposit accounts opened with big installment and small tenure	Very Likely	Moderate	High 3	a) Obtain KYC. b) Obtain supporting documents regarding source of fund.
Multiple deposit scheme accounts opened by same customer in a branch	Very Likely	Minor	Medium 2	a) Obtain KYC. b) Obtain supporting documents regarding source of fund.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Multiple deposit scheme accounts opened by same customer from different location	Likely	Moderate	Medium 2	a) Obtain KYC. b) Obtain supporting documents regarding source of fund. c) Obtain justification regarding opening of multiple deposit scheme in different locations. d) Monitoring of online transactions.
Open DPS in the name of family member or Installments paid from the account other than the customer's account	Very Likely	Moderate	High 3	a) Obtain written documents mentioning the reason of this kind of transaction. b) Obtain information of beneficial owner. c) Regular monitoring of transaction.
Early encashment of MTDR, special scheme etc.	Very Likely	Minor	Medium 2	a) Collect information regarding early encashment.
Non face to face business relationship /transaction	Likely	Major	High 3	a) Collect information from the relationship officer. b) Collection of data other reliable sources. c) Justification of source of data. d) Check the relationship of the client and banker.
Payment received from unrelated/un-associated third parties	Likely	Major	High 3	a) Obtain evidence of actual relationship or reason for such receipt. b) Perform EDD. c) If anything suspicious report as SAR. d) Don't allow transaction until risk is reduced.
SME Banking Product				
Want to open MTDR where source of fund is not clear	Likely	Major	Extreme 4	a) Obtain CDD. b) Obtain supporting documents regarding source of fund. c) If not satisfied don't open FDR.
Early encashment of MTDR	Very Likely	Minor	Medium 2	a) Collect information regarding early encashment.
Repayment of investment EMI from source that is not clear	Likely	Moderate	Medium 2	a) Obtain information of source of fund. b) Monitor transaction.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Repayment of full investment amount before maturity	Likely	Moderate	Medium 2	a) Ensure source of fund of repayment before early adjustment of investment. b) Obtain reason behind early adjustment of investment.
Investment amount utilized in sector other than the sector specified during availing the investment	likely	Major	High 3	a) Monitor the utilization investment. b) If found suspicious, then send STR.
In case of fixed asset financing, sale of asset purchased immediately after repayment of full investment amount	likely	Major	High 3	a) Obtain information of repayment of investment. b) If found suspicious, then send STR.
Source of fund used as security not clear at the time of availing investment	Unlikely	Moderate	Medium 2	a) Collect information and confirm the security. b) If found clear then provide sanction.
Wholesale Banking Product				
Development of new product & service of bank	Likely	Moderate	Medium 2	a) Identify feasibility of the product & service. b) Identify the ML & TF risk of the product & service.
Payment received from unrelated third parties	Unlikely	Moderate	Medium 2	a) Obtain relationship of the parties. b) Complete short KYC of depositor. c) Received payment only from the distributors, agents and suppliers of the customer. d) Monitoring the transaction regularly.
High Value MTDR	Very Likely	Minor	Medium 2	a) Obtain CDD. b) Obtain supporting documents regarding source of fund.
Murabaha Term investment, Bai Muajjal (FO), Bai Muajjal (G-work order), Bai Muajjal (Garment), Bai Muajjal (PO), Investment General, Corporate HPSM Lease finance, IHP Corporate Bai - Salam (Pre-Shipment), BTB L/C	Likely	Minor	Medium 2	a) Obtain CDD. b) Analysis the credit worthiness of the customer. c) Visit customer's office, factory and mortgaged properties. d) Monitor the transaction.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
BG (bid bond), BG(PG), BG (APG)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Verify the work order from the concern authority. b) Ensure assignment of bill from the concerned authority. c) Perform CDD. d) Obtain margin. e) Obtain sufficient collateral.
L/C Subsequent Murabaha term investment, DP L/C	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Obtain certificate from the respective countries chamber of commerce. b) Ensure proper verification of the price of the imported items from the international market/website. c) Obtain undertaking from the customer regarding the fair price.
Quard (Earnest Money), STL	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Check the work order. b) Verify the tender notice. c) Follow up the client whether the client get the work order or not. d) Verify other sources of income of the customer.
OBU	Unlikely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Confirm Enhance Due Diligence. b) Obtain information about the customer from the media, International market, web, etc. c) Obtain credit report of the customer. d) Preserve the permission obtained by the customer from competent authority. e) Confirm that advance is allowed considering the category.
Syndication Financing	Likely	Major	High 3	<ul style="list-style-type: none"> a) Perform CDD of the customer. b) Verify the value of plants, machinery and imported items. c) Obtain certificate from the respective chamber of commerce. d) Obtain information from lead bank regarding payment system. e) Physical verification.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Credit Card				
Supplementary SBL Tjarah Card Issue	Very Likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Obtain required documents as per Product Program Guideline (PPG) and bank's policy. b) Collect relationship of supplementary card holder with customer. c) Obtain KYC of supplementary cardholder. d) Collect CIB report. e) Keep transaction under monitoring. f) Check the Sanction list. g) Check whether customer is already availing Bank Credit card.
Frequent use of Card Cheque	Very Likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Update KYC. b) Obtain the purpose of the transaction. c) The account where the fund is transferred. d) Monitoring of transaction.
SBL Tjarah Card issuance against ERQ and RFCD accounts	Likely	Major	High 3	<ul style="list-style-type: none"> a) Check SANCTION LIST list. b) Collect CIB report of the customer. c) Verification of address of the client. d) Obtain KYC. e) Check the customer is availing the other bank credit card. f) Confirm that transactions are conducted as per foreign exchange guideline and FEPD circulars. g) Collect required documents as per PPG and Bank's policy.
International Trade				
Line of business mismatch (import/export/remittance)	Likely	Major	High 3	<ul style="list-style-type: none"> a) Perform EDD of the customer. b) Check the diversification of business. c) If found suspicious then send for STR.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Under / Over invoicing (import/export/remittance)	Very Likely	Major	Extreme 4	a) Perform EDD. b) Check the unit price of the product intended for import and export with the present international market price through internet. c) If found suspicious then send for STR.
Retirement of import bills in cash import / export/ remittance)	Very Likely	Major	Extreme 4	a) Check the size of the transaction with the cash flow. b) Background checking of beneficial owner. c) Confirm EDD.
Wire transfer	Very Likely	Moderate	High 3	a) Follow the instruction of the BFIU circular no. 26 before conducting the transaction. b) Obtain information of applicant and beneficiary as per BFIU circular no. 26.
Relationship between the remitter and beneficiary and purpose of remittance mismatch (outward/inward remittance)	Likely	Moderate	Medium 2	a) Confirm the purpose of the remittance with supporting documents. b) Collect information of applicant and beneficiary as per BFIU circular no. 26. c) If found suspicious then send for STR.

c. ML & TF Risk Register for Business practices/delivery methods or channels

These are some example of ML & TF risk in terms of business practices/delivery methods or channels that Bank may face and the possible ways to reduce and manage those risks:

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Online (multiple small transaction through different branch)	Very Likely	Moderate	High 3	a) Obtain justification regarding the transaction pattern from the customer. b) Obtain KYC of the bearer as per BFIU circular no. 26. c) Monitor online transaction. d) If found any suspicious then send for STR.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




Risk	Likelihood	Impact	Risk Score	Treatment/Action
BEFTN/RTGS	Very Likely	Minor	Medium 2	<ul style="list-style-type: none"> a) Obtain information regarding the purpose of the transaction. b) Obtain information regarding relationship of the customer and beneficiary. c) Monitor transaction pattern. d) Update TP.
BACH	Likely	Moderate	Medium 2	<ul style="list-style-type: none"> a) Check the four corners of cheque. b) Check the amount of cheque. c) Check the cheque number. d) Check TP of the client. e) Check the signature card of the client.
IDBP (Inland Documentary Bill Purchase)	Very Likely	Minor	Medium 2	<ul style="list-style-type: none"> a) Confirm CDD. b) Check the genuineness of LC and acceptance from BB dashboard.
Agent Banking				
Mudaraba savings account(MSA)	Very Likely	Minor	Medium 2	<ul style="list-style-type: none"> a) Check Sanction List. b) Open through biometric and capture other related documents in the system along with attaching hard copy with AOF. c) Confirm the source of the agent client d) Strictly follow CDD process. e) Confirm the dual control in Account approval and internal verification over phone. f) Confirm the Limited Cash withdrawal limit.
Al-Wadiah Current account(AWCA)	Minor	Medium	High 3 On the basis of subjective judgment	<ul style="list-style-type: none"> a) Check Sanction List. b) Open through biometric and capture other related documents in the system along with attaching hard copy with AOF. c) Confirm the source of the agent client d) Strictly follow CDD process. e) Confirm the dual control in Account approval and internal verification over phone. f) Confirm the Limited Cash withdrawal limit.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Mudaraba Term Deposit account	Likely	Moderate	Medium 2	a) Only Savings/Current account holder can open the account. b) No walking customer is allowed to open the account. c) TDS account open by debiting linked account and also credit the linked account after maturity or pre-mature tenure.
Mudaraba Deposit Pension Scheme	Very Likely	Minor	Medium 2	a) Only Savings/Current account holder can open the account. b) No walking customer is allowed to open the account. c) DPS account open by debiting linked account and also credit the linked account after maturity or pre-mature tenure.
Mobile Banking	Likely	Moderate	Medium 2	a) Obtain KYC. b) Confirm CDD & EDD. c) Monitor transaction regularly. d) Check NID/ Passport/ Birth Certificate along with photo. e) Check additional documents like trade license, E-TIN, utility bill, etc.
SBL Tijarah Card				
New Merchant sign up	Unlikely	Minor	Low 1	a) Confirm KYC of merchant. b) Visit merchant physically. c) Collect documents as per PPG and bank's policy.
High volume transaction through POS	Very Likely	Moderate	High 3	a) Check merchant product & price and match with POS transactions. b) Check transaction profile of the merchant. c) Obtain justification from merchant regarding any unusual transaction.
Alternate Delivery Channel				
Large amount withdrawn from ATMs	Likely	Moderate	Medium 2	a) Check the timing of transaction. b) Obtain justification of transaction. c) If found any suspicious send STR.
Larger amount transaction from different location and different time(mid night) through ATM	Likely	Major	High 3	a) Check the timing of transaction. b) Obtain justification of transaction. c) If found any suspicious send STR.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Huge fund transfer through internet	Likely	Major	High 3	a) Check the transaction limit and number through internet banking. b) Generate report regarding high value of transaction through internet from the system. c) Monitor transaction.
International Trade				
Customer sending remittance through SWIFT under single customer credit transfer (fin-103)	Very Likely	Moderate	High 3	a) Check the Sanction list of the parties involved with this transaction. b) Confirm whether the transaction meets the central bank circulars or guideline. c) Obtain purpose of the remittance. d) Confirm the KYC. e) Obtain information as per BFIU circular no. 26.
Existing customer/ other bank customer receiving remittance through SWIFT under single customer credit transfer (fin-103).	Very Likely	Major	Extreme 4	a) Obtain documents related to this transaction. b) Obtain Form C from the client before release the remittance.

d. ML & TF Risk Register for Country/jurisdiction

Country or geographical risk may arise because of the location of a customer, the origin of destination of transactions of the customer, but also because of the business activities of the Bank itself, its location and the location of its organizational units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to money laundering and terrorism financing.

There is no general definition based on which particular countries or geographical areas can be categorized as low, medium or high risk. The factors which may define if a specific country or geographical area is more vulnerable to money laundering and terrorism financing, may include different criteria. These are some example of ML & TF risk that Bank may face and the possible ways to reduce and manage those risks:

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




Risk	Likelihood	Impact	Risk Score	Treatment/Action
Import and export from/to sanction country	Very likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Inform AML & CFT Division/CAMLCO's Office immediately and take the opinion. b) Check the Sanction List. c) Inform BFIU through AML & CFT Division/CAMLCO's Office without delay.
Transshipments, container, flag vessel etc. under global sanction	Very likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Inform AML & CFT Division/CAMLCO's Office immediately and take the opinion. b) Check the Sanction list. c) Inform BFIU through AML & CFT Division/CAMLCO's Office without delay.
Establishing correspondent relationship with sanction bank and/or country	Very likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Inform AML & CFT Division/CAMLCO's Office immediately and take the opinion. b) Check the Sanction list. c) Inform BFIU through AML & CFT Division/CAMLCO's Office without delay.
Establishing correspondent relationship with poor AML & CFT practice country	Very likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Confirm the EDD before establishing relationship with the correspondent bank. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the correspondent bank.
Customer belongs to higher -risk geographic locations such as High Intensity Financial Crime Areas	Very likely	Major	Extreme 4	<ul style="list-style-type: none"> a) Confirm the EDD before establishing relationship with the correspondent bank. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the correspondent bank.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Customer belongs to countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.	Very likely	Major	Extreme 4	a) Confirm the EDD before establishing relationship with the correspondent bank. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the correspondent bank.
Customer belongs to High Risk ranking countries of the Basel AML index.	Very likely	Major	Extreme 4	a) Confirm the EDD before establishing relationship. b) Obtain specific purpose of establishing relationship. c) Obtain KYC of the bank/entity.
Customer belongs to the countries identified by the bank as higher -risk because of its prior experiences or other factors.	Likely	Major	High 3	a) Confirm the specific reason of transaction. b) Obtain EDD of the customer.
Any country identified by FATF or FSRBs-(FATF Style Regional Body) as not having adequate AML & CFT systems	Very Likely	Major	Extreme 4	a) Don't accept as a customer.
Any country identified as destination of illicit financial flow	Likely	Major	High 3	a) Confirm Customer Due Diligence and Enhanced Due Diligence.
Border Area	Likely	Major	High 3	a) Update KYC of the account holder periodically. b) Confirm EDD if needed. c) Monitor cash deposit and online transaction. d) Monitor high risk customer on regular basis.
Countries subject to UN embargo/ sanctions	Very Likely	Major	Extreme 4	a) If there is any existing customer stop the transaction immediately and inform BFIU through AML & CFT Division/CAMLCO's Office. b) Don't accept as a new customer.

7.1.2 Register for Regulatory Risk

Regulatory risk is associated with not meeting all the obligations of Bank under the Money Laundering Prevention Act 2012 (Amendment 2015), Anti-Terrorism Act 2009, (amendment 2012 & 2013). Following are some example of ML & TF risk the Bank may face in terms of noncompliance of regulations and the possible ways to reduce and manage those risks.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Not having AML & CFT guideline	Likely	Major	High 3	a) Develop AML & CFT guideline. b) Update guideline time to time.
Not forming a Central Compliance Committee (CCC)	Likely	Major	High 3	a) Formation of Central Compliance Committee as per BFIU Circular no. 26.
Not having an AML & CFT Compliance Officer	Likely	Moderate	Medium 2	a) Nominate the compliance officer name as per requirement of BFIU Circular No. 26.
Not having Branch Anti Money Laundering Compliance Officer	Likely	Moderate	Medium 2	a) CCC will advise branch for nominate the AML & CFT compliance officer as per BFIU Circular no. 26. b) Branch will send the Office Order to the CCC regarding nomination of compliance officer name.
Not having an AML & CFT program	Likely	Major	High 3	a) Develop AML & CFT program. b) Update program time to time.
No senior management commitment to comply with MLP and AT Act.	Likely	Moderate	Medium 2	a) Provision of commitment of senior management to be included in the AML & CFT policy guideline.
Failure to follow the AMLD/BFIU circular, circular letter, instructions etc.	Likely	Major	High 3	a) Follow the AML & CFT & BFIU circulars, circular letters, instruction issued from time to time.
Uniform account opening form not followed while opening account	Likely	Moderate	Medium 2	a) Develop the unique account opening form while opening new account as per BFIU Circular No. 26.
Non screening of new and existing customers against UNSCR and OFAC lists	Likely	Major	High 3	a) Before establishing any kind of relationship with customer must check SANCTION LIST sanction and OFAC lists.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Violation of Foreign Exchange Regulation Act, 1947 while dealing with NRB accounts.	Likely	Major	High 3	a) Must follow the instruction of Foreign Exchange Regulation Act 1947 while dealing with NRB accounts.
Complete and accurate information of customer not obtained	Likely	Major	High 3	a) Follow the instruction of BFIU Circular no. 26 regarding complete and accurate information of the customer. b) Update KYC periodically. c) If fails to update then close the account prior notice to customer.
Failure to verify the identity proof document and address of the customer	Likely	Major	High 3	a) Verify (business unit) the identity proof document and address of the customer b) Verify the ID from the competent authority. c) Verify the address by collecting other documents like utility bill, phone bill, etc.
Beneficial owner identification and verification not done properly	Likely	Major	High 3	a) Monitor transaction and find out the beneficial owner of the account. b) Collect KYC of beneficial owner.
Customer Due Diligence (CDD) not practiced properly	Likely	Major	High 3	a) Perform CDD of the customer as per BFIU Circular No. 26.
Failure to perform Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, family members and close associates of PEPs and influential person and senior official of international organization.)	Likely	Major	High 3	a) Perform EDD for the high risk customer. b) Confirm the Senior Management approval before opening account.
Failure to complete KYC of customer including walk in customer	Likely	Major	High 3	a) Complete KYC of customer including walk in customer as per BFIU circular no. 26
Failure to update TP and KYC of customer	Likely	Major	High 3	a) Update TP & KYC as per BFIU circular no. 26.
Keep the legacy accounts operative without completing KYC	Unlikely	Major	Medium 2	a) Update the KYC of the legacy accounts. b) If failed then follow the instruction of the BFIU circular no. 26.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to assess the ML & TF risk of a product or service before launching	Unlikely	Major	Medium 2	a) Assess the ML and TF risk of a product or service before launching.
Failure to complete the KYC of Correspondent Bank	Likely	Major	High 3	a) Complete the KYC of correspondent Bank reciprocally. b) Update KYC of correspondent bank time to time.
Senior Management approval not obtained before entering into a Correspondent Banking relationship	Unlikely	Major	Medium 2	a) Must obtain Senior Management approval not obtained before entering into a Correspondent Banking relationship.
Failure to comply with the instruction of BFIU by bank Foreign subsidiary	Likely	Moderate	Medium 2	a) Obtain confirmation from the subsidiary on compliance. b) Monitor the AML & CFT activity of subsidiary.
Failure to keep record properly	Likely	Major	High 3	a) Follow the instruction of BFIU Circular No. 26 regarding record keeping.
Failure to report complete and accurate CTR on time	likely	Major	High 3	a) Rectify the irregularities of the information in CBS and FIU software module. b) Branch and AML & CFT Division will monitor the CTR transaction. c) Send the CTR through goAML software and FIU software (CD copy).
Failure to review CTR	Likely	Moderate	Medium 2	a) Generate the CTR from CBS. b) Monitor transaction report by both AML & CFT Division and Branch on monthly basis.
Failure to identify and monitor structuring	Likely	Major	High 3	a) Set up a mechanism for finding out structuring and generate report from CBS. b) Identity & Monitor structuring report regular basis.
Failure to provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity	Likely	Major	High 3	a) Monitor structuring report, high value transaction report, TP changing report and identify STR. b) Develop monitoring system to identify STR.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to conduct quarterly meeting properly	likely	Moderate	Medium 2	a) Conduct meeting on quarterly basis and discuss regarding the recent circulars, laws and guideline of AML & CFT matters and its implementation. b) Send the meeting minutes to AML & CFT Division on quarterly basis.
Failure to report suspicious transactions (STR)	Very Likely	Major	Extreme 4	a) Both Branch and AML & CFT Division will monitor monthly CTR report at the time of finding suspicious transaction. b) Monitor other transaction and activity of the customer at the time of finding suspicious.
Failure to conduct self-assessment properly	Likely	Major	High 3	a) Branch will mention the actual position of strength and weakness of the branch. b) Cross check with the Independent Testing Report and Inspection Report.
Failure to submit statement/report to BFIU on time	likely	Major	High 3	a) Submit all the statements and reports to BFIU on time.
Submit erroneous statement/report to BFIU	Likely	Major	High 3	a) Statement/report must be checked carefully before sending to BFIU.
Not complying with any order for freezing or suspension of transaction issued by BFIU or BB	Very Likely	Major	Extreme 4	a) Must comply with any order for freezing or suspension of transaction issued by BFIU or BB timely. b) AML & CFT Division will check the order for freezing or suspension of transaction.
Not submitting accurate information or statement sought by BFIU or BB.	Likely	Major	High 3	a) Must submit accurate information or statement to BFIU or BB on time.
Not submitting required report to senior management regularly	likely	Moderate	Medium 2	a) Submit the respective report to senior management on regular basis.

Risk	Likelihood	Impact	Risk Score	Treatment/Action
Failure to rectify the objections raised by BFIU or bank inspection teams on time	Very Likely	Major	Extreme 4	a) Must regularized the objections raised by the BFIU or Bank inspection teams timely. b) AML & CFT Division will follow up the irregularities.
Failure to obtain information during wire transfer	Likely	Major	High 3	a) Must obtain information during wire transfer as per BFIU Circular No. 26. b) Inspection team will check the compliance regarding wire transfer.
Failure to comply with the responsibilities of ordering, intermediary and beneficiary bank	Likely	Major	High 3	a) Comply with the responsibilities of ordering, intermediary and beneficiary bank perfectly.
Failure to scrutinize staff properly	Unlikely	Major	Medium 2	a) PMD must scrutinize the background of the newly recruited employees properly. b) Must conduct reference check.
Failure to circulate BFIU guidelines and circulars to branches	Likely	Major	High 3	a) AML & CFT Division must circulate all the circulars and guidelines issued by BFIU to branches on time.
Inadequate training/ workshop arranged on AML & CFT	Unlikely	Major	Medium 2	a) Workshop regarding AML & CFT matters on regular basis to build up the knowledge of all employees. b) Conduct the evaluation test at the time of training. c) Maintain the database of training list of employees.
No independent audit function to test the AML program	likely	Major	High 3	a) ICCD will inspect the AML program and conduct the Independent Testing Procedure.

CHAPTER VIII: COMPLIANCE STRUCTURE OF STANDARD BANK LTD

Compliance structure of Standard Bank is an organizational setup that deals with AML, CFT & CPF compliance of the bank and the reporting procedure. This includes-

- Central Compliance Committee (CCC),
- Chief Anti Money Laundering Compliance Officer (CAMLCO),
- Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO),
- Branch Anti Money Laundering Compliance Officer (BAMLCO),
- Deputy BAMLCO
- Departmental/Divisional Anti Money Laundering Compliance Officer (DAMLCO)

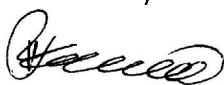
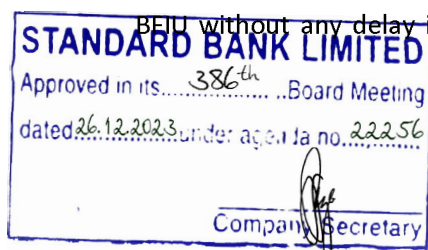
8.1 Central Compliance Committee:

Under the obligation of BFIU Circular No. 26 dated June 16, 2020, "To keep the banking sector free from the risks related to Money Laundering & Terrorist Financing and for the effective/proper compliance of all existing acts, rules and issued instructions time to time by BFIU, every bank must set up a Central Compliance Committee (CCC) that will be directly monitored by the Managing Director or the Chief Executive Officer of the bank."

As per guideline of BFIU, the central compliance unit shall be headed by a high official, who will be known as the Chief Anti Money Laundering Compliance Officer (CAMLCO). In this case, 'High official' will be considered as an official within 2 (two) tier of the Managing Director/Chief Executive Officer. In line with the BFIU guideline, Standard Bank has nominated CAMLCO with a designation of Additional Managing Director. Before assigning the CAMLCO to other duties of the Bank, the management has to ensure that the AML, CFT & CPF activities of the bank will not be hampered for it.

As per guideline of BFIU, Bank can also nominate one or more Deputy of the CAMLCO, who will be known as the Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO). The DCAMLCO will be at least in the rank of 'Deputy General Manager' or 'Senior Vice President' or 'Equivalent' of the bank. In line with the BFIU guideline, Standard Bank has designated both the CAMLCO and DCAMLCO who have detailed knowledge in the existing acts, rules and regulations, instructions issued by BFIU from time to time and international standards on preventing ML,TF & PF.

The AML & CFT Division shall issue instructions for the branches, where transaction monitoring system, internal control system, policies and techniques will be included to prevent Money Laundering and Terrorist Financing as and when required. The AML & CFT Division will report to BFIU without any delay in case of any account/business relationship found with any person/entity



whose name/names appeared to the mass media (TV/News Paper) regarding ML, TF, PF or any predicate offences under MLPA, 2012 (Amendment, 2015). The AML & CFT can also make a Suspicious Transaction Report (STR) or Suspicious Activity report (SAR) directly to BFIU in this regard.

8.2 Formation of Central Compliance Committee (CCC), Head Office:

Central Compliance Committee at Head Office of Standard Bank Ltd shall be constructed by the Heads of Division/ Department & Officials of different Division/Department including CAMLCO and DCAMLCO excluding the officials of ICCD under the directives of BFIU. CCC has been constructed by comprising the following:

1.	Additional Managing Director & CAMLCO	Chairman
2.	Head of AML & CFT Division & DCAMLCO	Member Secretary

and as member the Head of (HRD, IT, Corporate Banking, SME, IRM, ID, BOD, CARDS, ADC, Training Institute and so on).

8.3 Responsibilities and Authorities of the CCC:

CCC is the prime mover of the Standard Bank for ensuring the compliance of AML, CFT & CPF measures. Its main responsibilities are to--

- develop the bank’s policy, procedure and strategies in preventing ML, TF & PF;
- coordinate bank AML & CFT compliance initiatives;
- coordinate the ML & TF risk assessment of the bank and review thereon;
- present the compliance status with recommendations before the Managing Director & CEO on half yearly basis;
- forward STR/SAR and CTR to BFIU in time and in proper manner;
- report summary of self-assessment and independent testing procedure to BFIU in time and in proper manner;
- impart training, workshop, seminar related to AML, CFT & CPF for the employee of the bank;
- take required measures to submit information, report or documents in time.

For shouldering these responsibilities bank authority may consider to give the following authority to CCC-

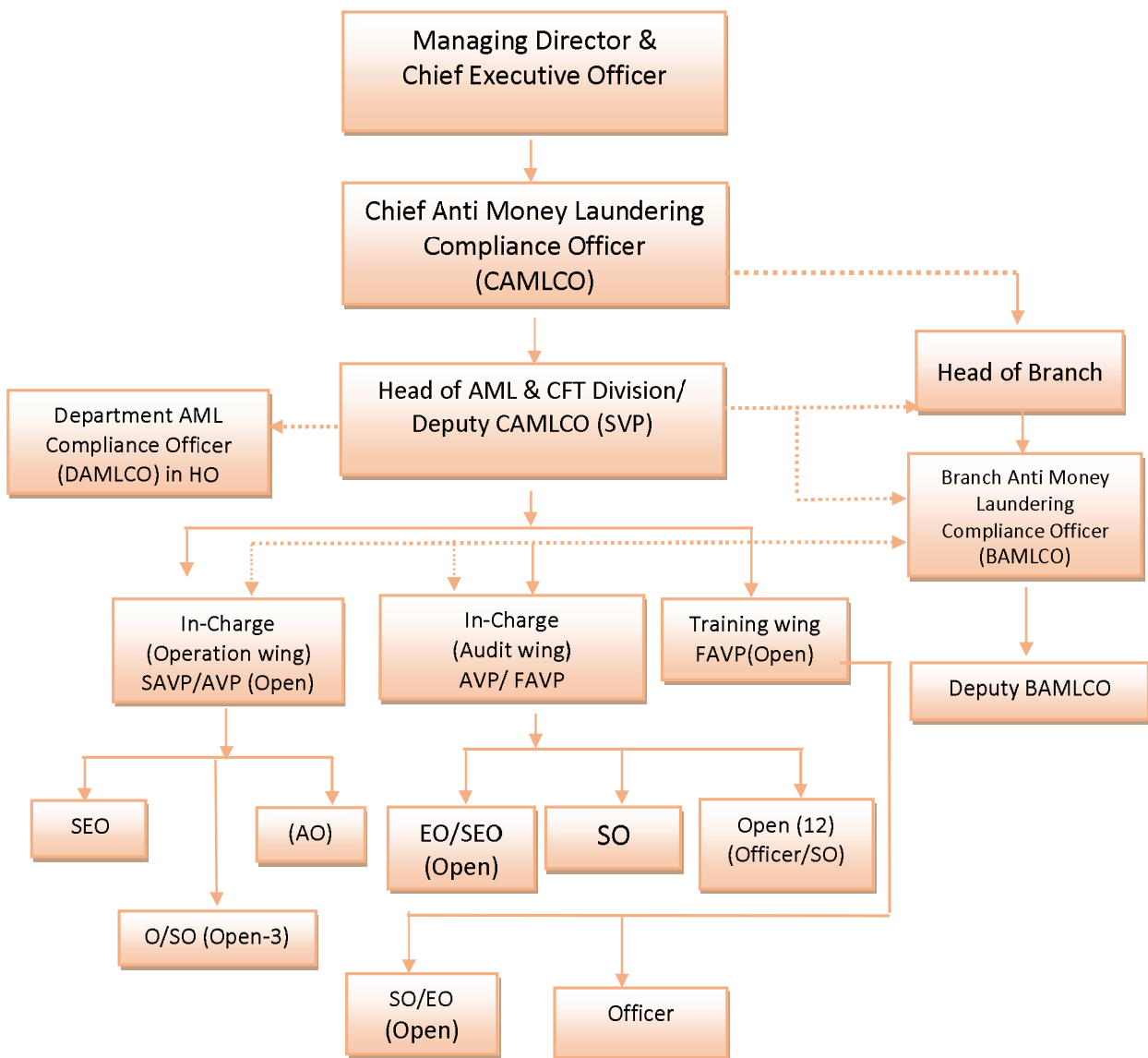
- appointment of BAMLCO & Deputy BAMLCO and assign their specific job responsibilities;

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




- requisition of human resources and logistic supports for CCC;
- make suggestion or administrative sanction for non-compliance by the employees.

Organogram of the AML & CFT Division:



8.4 Separation of CCC from Internal Control & Compliance Department (ICCD):

- Under the BFIU Circular No. 26 dated June 16, 2020 for ensuring the independent audit function CCC of Standard Bank Ltd. is completely separated from Internal Control & Compliance Department (ICCD). Either the two divisions may perform same job but in different and independent way. In this regard, ICCD may add values for good performance of CCC and the bank's AML, CFT & CPF compliance program. To ensure this autonomy there shall not be any member from ICCD to CCC 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 CCC and vis-à-vis but no one should be posted in these 2 (two) departments at the same time.

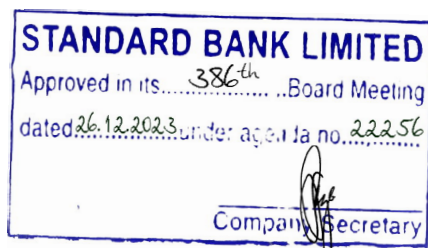
8.5 Chief Anti Money Laundering Compliance Officer (CAMLCO):

Standard Bank Ltd has designated Chief Anti Money Laundering Compliance Officer (CAMLCO) at its Head Office with sufficient authority to implement and enforce corporate wide AML, CFT & CPF policies, procedures and measures and who will report directly to Managing Director & CEO. This provides evidence of senior management's commitment to efforts to combat money laundering, terrorist financing & proliferation financing and, more importantly, provides added assurance that the officer will have sufficient influence to enquire about potentially suspicious activities. The CAMLCO is responsible for oversight of the Bank's compliance with the regulatory requirements on systems and controls against money laundering (ML), terrorist financing (TF) & proliferation financing (PF).

The designated CAMLCO, directly or through the CCC, is the central point of contact for communicating with the regulatory agencies regarding issues related to the bank's AML, CFT & CPF program.

All staffs engaged in the Standard Bank Ltd at all levels must be aware of the identity of the CAMLCO, DCAMLCO and the Officials of AML & CFT Division, branch & Division/Department in Head Office level AML, CFT & CPF compliance officers, and the procedure to follow when making a suspicious transaction/activity report. All relevant staffs must be aware of the chain through which suspicious transaction/activity reports should be passed to the CAMLCO.

As the CAMLCO is responsible for the oversight of all aspects of the bank's AML, CFT & CPF activities and is the focal point for all activity within the bank relating to ML, TF & PF his/her job description should clearly set out the extent of the responsibilities given to him/her. The CAMLCO will need to be involved in establishing the basis on which a risk-based approach to the prevention of ML, TF & PF is put into practice.



8.6 Authorities and Responsibilities of CAMLCO :

Authorities-

- CAMLCO shall act on his own authority;
- He/she shall not take mandatorily any permission or consultation from/with the Managing Director & CEO before submission of STR/SAR and any document or information to BFIU;
- He/she shall maintain the confidentiality of STR/SAR and any document or information required by laws and instructions by BFIU;
- He/she must have access to any information of the bank;
- He/she shall ensure his/her continuing competence.

Responsibilities-

- CAMLCO must ensure overall AML, CFT & CPF compliance of the bank;
- oversee the submission of STR/SAR or any document or information to BFIU in time;
- maintain the day-to-day operation of the bank's AML, CFT & CPF compliance;
- CAMLCO will inform to Managing Director & CEO or Board of Director for proper functioning of CCC/AML & CFT Division ;
- CAMLCO shall review and update ML, TF & PF risk assessment of the bank;
- take corrective actions have taken by the bank to address the deficiency identified by the BFIU or BB.

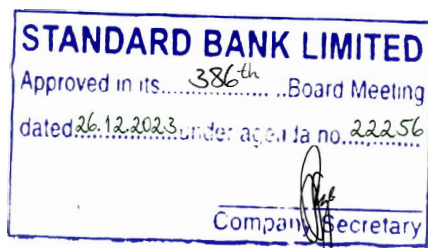
8.7 Branch Anti Money Laundering Compliance Officer (BAMLCO):

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 on preventing ML, TF & PF, bank shall nominate Head of Branch or Deputy -Manager or Manager Operation of the Branch or even Experienced General Banking/Credit or investment /Foreign Exchange In-charge as Branch Anti Money Laundering Compliance Officer (BAMLCO) in every branch."

In Standard Bank Ltd (SBL), under the directive of BFIU, the Deputy Manager/ Manager Operations of the Branch will be nominated as the "BAMLCO" in maximum cases. SBL is desire to maintain the highest level of AML, CFT & CPF compliance, Branch will also nominate another official as "Deputy BAMLCO". Both BAMLCO and Deputy BAMLCO have to have sufficient knowledge in the existing acts, rules and regulations, BFIU's instructions (circulars, circular letters, etc.) and our own policies on preventing Money Laundering, Terrorist Financing and Proliferation Financing. Deputy BAMLCO will assist BAMLCO to do the job successful and effective regarding AML, CFT & CPF issues. In absence of BAMLCO, Deputy BAMLCO will act as BAMLCO to mitigate the AML, CFT & CPF matters.

8.8 Responsibilities and Authorities of BAMLCO:

AML & CFT Division has circulated different Instruction Circulars time to time in branches for monitoring and supervising AML, CFT & CPF issues. Hence, BAMLCO & Deputy BAMLCO will be responsible to monitor & supervise all AML & CFT issues/matters as per Acts and Circulars of BFIU, Bangladesh Bank.



Responsibilities of BAMLCO

BAMLCO will perform the following responsibilities:

Knowledge on AML, CFT & CPF issues:

1. 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.
2. 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.
3. Make sure all the on boarding customer and transaction have been screening by the system and report to competent authority, if any.

Branch Compliance Program:

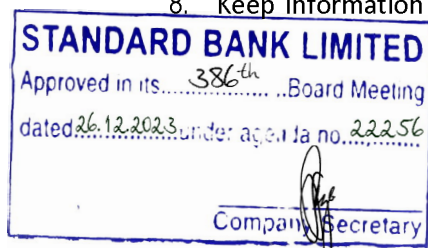
1. Implement all instructions of AML & CFT Division/CCC regarding AML & CFT issues time to time.

Sanctions Screening:

1. Ensure sanction list screening like UN Sanction list, OFAC and EU list and list of organization banned by Bangladesh Government before opening of account and while making any transaction.
2. Reviews suspected matches and reports valid matches to the AML & CFT Division/CCC, Head Office for onward submission to regulatory authority.

Customer Due Diligence:

1. Identify and verify the identity of the customer information and documents obtained from the reliable source.
2. Ensure the KYC of all customers have done properly.
3. Ensure the update of KYC of the customer have done timely.
4. Ensure due diligence while establishing relationship with the new customer and also while conducting financial transaction with the existing customer.
5. Ensure due diligence when there is a suspicion of ML, TF & PF.
6. Ensure due diligence of walk-in customer, online customers and depositor or withdrawer other than account holder.
7. Identify the beneficial owner of the account and conduct due diligence of the beneficial owners as per "Guidelines for Beneficial Owner" circulated by BFIU.
8. 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;

Enhance Due Diligence (EDD):

1. Confirm Head Office, CCC/ AML & CFT Division approval before opening of PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates as per instruction circular no SBL/HO/AML & CFT/ Instruction Circular/2020/1159 dated June 30, 2020.
2. Confirm EDD of PEPs, Influential Person and Senior Officials of International Organization and their family members as well as close associates.
3. Comply Enhance Due Diligence (EDD) for the high risk customer and obtain additional information/documents.
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, terrorist financing and proliferation financing.

Transaction Monitoring:

1. Introduce self-auditing, self-assessment and independent testing procedure in the branch and report to ICCD & AML & CFT Division in time.
2. Ensure regular transaction monitoring to find out any unusual transaction. Records of all transaction monitoring should be kept in the file.
3. Review cash transaction to find out any structuring;
4. Ensure monitoring of account transaction as per instruction of BFIU as well as AML & CFT Division.

Risk Grading of Customer:

1. Ensure proper risk grading of the customer with compare to his occupation, source of fund, transaction profile (TP) and geographical location of the customer.
2. Detect high risk customer using subjective/objective judgment and ensure proper filing.

Update Customer Information and TP & KYC:

1. Update/Review of Transaction Profile and KYC of the customer as per BFIU circular no. 26 dated June 16, 2020.
2. Update customer information with proper justification if any changes required.

Arrangement of AML & CFT Meeting:

1. BAMLCO shall arrange meeting regarding AML, CFT & CPF issues as per instruction of BFIU circular no. 26 dated 16.06.2020 in the branch level and confirm all the employees are present in the meeting.



2. BAMLCO shall take effective measures on the following matters after reviewing the compliance of the existing rules, 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.

Report Submission to AML & CFT Division:

1. Review Monthly Cash Transaction Report (CTR), Quarterly (Meeting Minutes), Half-yearly (Self-Assessment) statements and send these to AML & CFT Division within the stipulated time period without any fail. Conduct meeting before finalization of Self-Assessment report.
2. Review information and documents before submitting those reports to AML & CFT Division for onward submission to BFIU.

STR/SAR Identification and Reporting:

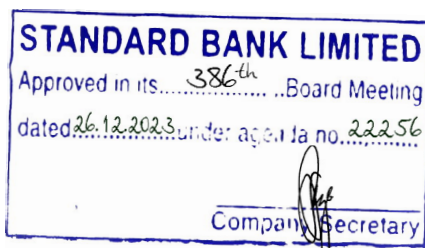
1. Report STR/SAR by monitoring and analyzing transaction.
2. Review the CTR of each month and find out STR/SAR and send it to AML & CFT Division.
3. Ensure that all the employees of the branch are well aware and capable to identify any unusual transaction or any attempt of unusual transaction;
4. Analyze the Cash Transactions immediate below the CTR threshold limit to identify structuring.
5. Monitor customer unusual behavior and unusual transaction pattern.
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.

Record Keeping:

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

Training of employees:

1. Provide/arrange training to new employees immediately and refresher training to the employees who obtain training regarding AML, CFT & CPF issues two years before.
2. Take initiative for training to all officials of the branch.



Others responsibilities:

1. Ensure all the required information and document are submitted properly to CCC/AML & CFT Division and any freeze order or stop payment order are implemented properly and without delay;
2. 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;
3. Create awareness regarding AML, CFT & CPF among the customer of the branch.
4. Ensure that corrective actions have taken by the branch to address the deficiency identified by the BFIU or BB.
5. Monitor the staff of the branch to check whether any of them are directly or indirectly involved in or is facilitating Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF).
6. Any other responsibility assigned by the CCC/ AML & CFT Division.

Authorities of BAMLCO

For shouldering these responsibilities and preventing ML, TF & PF in the branch, Standard Bank Ltd. will consider to give the following authority to

BAMLCO:

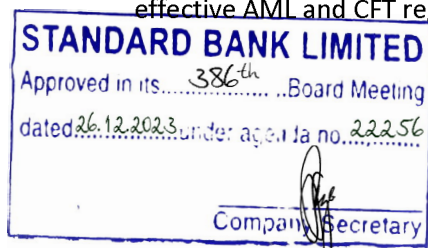
- Generally BAMLCO will report to Head of Branch regarding all the matters of AML, CFT & CPF.
- BAMLCO can independently send STR/SAR to CCC/ AML & CFT Division if needed.
- BAMLCO can act independently for ensure compliance regarding AML, CFT & CPF issues.

Deputy BAMLCO will be reliever of BAMLCO at the time of absence and all responsibilities then will be applicable upon Deputy BAMLCO.

DAMLCO: In addition, Standard Bank Ltd. has assigned a Departmental/Divisional AML Compliance Officer (DAMLCO) under the letter reference no SBL/HO/AML & CFT/2021/3125 dated October 24, 2021 to comply the departmental/divisional AML, CFT & CPF related compliance smoothly.

8.9 Internal Control and Compliance:-

Under the obligation of BFIU Circular No. 26 dated June 16, 2020, "with a goal of establishing an effective AML and CFT regime, it shall have to be ensured that the Internal Audit Division of the bank



is equipped with enough manpower who have enough knowledge on the existing acts, rules and regulations, BFIU's instructions on preventing money laundering(ML), terrorist financing (TF) & proliferation financing (PF) and bank's own policies in this matter to review the Self-Assessment Report received from the branches and to execute the Independent Testing Procedure appropriately."

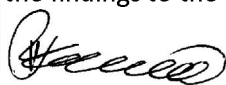
Internal Control & Compliance Division (ICCD) of Standard Bank Ltd. shall have an important role for ensuring proper implementation of bank's AML, CFT & CPF Compliance Program. ICCD of Standard Bank is equipped with enough manpower and autonomy to look after the prevention of ML, TF & PF. The ICCD has to oversee the implementation of the AML, CFT & CPF 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.

To ensure the effectiveness of the AML, CFT & CPF compliance program, bank should assess the program regularly and look for new risk factors. FATF recommendation 18 suggests that-

"Financial institutions should be required to implement programs against money laundering and terrorist financing. Financial groups should be required to implement group wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML, CFT & CPF 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".

An institution's internal auditors should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable. The internal audit must-

- understand ML, TF & PF risk of the bank and check the adequacy of the mitigating measures;
- examine the overall integrity and effectiveness of the AML, CFT & CPF Compliance Program;
- examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- determine personnel adherence to the bank's AML, CFT & CPF Compliance Program;
- perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations);
- assess the adequacy of the bank's processes for identifying and reporting suspicious activity;
- communicate the findings to the board and/or senior management in a timely manner;



- recommend corrective action to address the identified deficiencies;
- track previously identified deficiencies and ensures correction made by the concerned person;
- examine that corrective actions have taken on deficiency identified by the BFIU;
- assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- determine when assessing the training program and materials:
 - the importance of the board and the senior management place on ongoing education, training and compliance,
 - employee accountability for ensuring AML, CFT & CPF compliance,
 - comprehensiveness of training, in view of specific risks of individual business lines,
 - training of personnel from all applicable areas of the bank,
 - frequency of training,
 - coverage of bank policies, procedures, processes and new rules and regulations,
 - coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity,
 - penalties for noncompliance and regulatory requirements.

8.10 Employee Training and Awareness Program:

A formal AML, CFT & CPF 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 financial institution's policy, procedures, and controls affect them in their day to day activities which has been narrated under FATF recommendation 18. As per AML circular, each financial institution shall arrange suitable training for their officials to ensure proper compliance of ML, TF and PF prevention activities.

The Need for Staff Awareness:

The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the seriousness of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

It is, therefore, important that financial institutions introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.



Education and Training Programs:

All relevant staff should be educated in the process of the “Know Your Customer” requirements for ML, TF and PF prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer’s transactions or circumstances that might constitute criminal activity.

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

General Training:

A general training program should include the following:

- General information on the risks of money laundering, terrorist financing and proliferation financing schemes, methodologies, and typologies;
- Legal framework, how AML & CFT related laws apply to banks and their employees;
- Institution’s policies and systems with regard to customer identification and verification, due diligence, monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

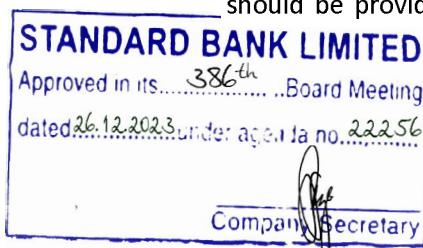
The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training should present real life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable,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

Job Specific Training:

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

i) New Employees :

A general appreciation of the background to money laundering, terrorist financing & proliferation financing and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or



their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so. The new or fresh employee may be trained up within a year.

ii) Customer Service/Relationship Managers:

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

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

Processing (Back Office) Staff:

The staffs, who receive completed Account Opening, MTDR 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 organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML & CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

iii) Investment Officers:

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

iv) Audit and compliance staff :

These are the people charged with overseeing, monitoring and testing AML, CFT & CPF controls, and they should be trained about changes in regulation, ML, TF and PF methods and enforcement, and their impact on the institution.



v) Senior Management/Operations Supervisors and Managers:

A higher level of instruction covering all aspects of ML, TF and PF 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.

vi) Senior Management and Board of Directors:

ML, TF and PF issues and dangers should be regularly and thoroughly communicated to the board. It is important that the Compliance Division has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering and terrorist financing poses to the institution. Major AML, CFT & CPF compliance related circulars/circular letters issued by BFIU should be placed to the board to bring it to the notice of the Board members.

vii) AML & CFT Compliance Officer :

The CAMLCO, DCAMLCO, and AML & CFT Compliance Officer should receive in depth training on all aspects of the ML, TF & PF Prevention Legislation, BFIU directives and internal policies and standards.

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

viii) Training Procedures:

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

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick “why are they here” assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.



- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

x) Refresher Training:

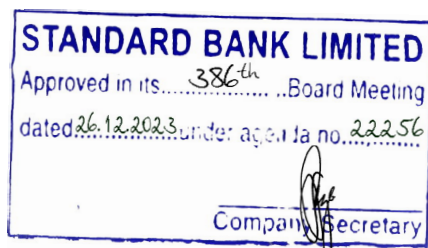
In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Some Banks/FIs may wish to provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction/juxtaposition with compliance monitoring.

Training should be conducted ongoing basis, incorporating trends and developments in an institution's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions/unusual activity.

8.11 External Auditor:

External auditor shall play an essential part in reviewing the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External audit should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors.

External auditor of Standard Bank will review the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report.



CHAPTER IX: CUSTOMER DUE DILIGENCE OF STANDARD BANK

9.1 Preamble

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.

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. 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).

Therefore, Standard Bank demonstrate supervisory authority to put in place, implement adequate CDD measures considering the risks of money laundering and terrorist financing. Such risk sensitive CDD measures should be based on-

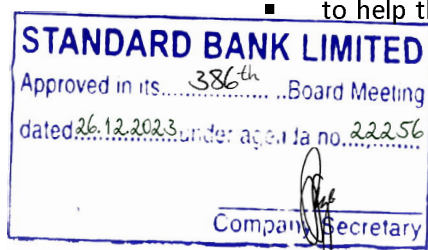
- a) Type of customers;
- b) Business relationship with the customer;
- c) Type of banking products; and
- d) Transaction carried out by the customer.

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

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

Standard Bank therefore, need to carry out customer due diligence for two broad reasons:

- to help the organization, at the time due diligence is carried out, to be reasonably



A handwritten signature in blue ink.



A handwritten signature in blue ink.

- satisfied to those customers who they say about, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government or international sanctions) to provide them with the product or service requested; and
- to enable the organization in investigation, law enforcement by providing available information about customers in due process.

It may be appropriate for the bank to know more about the customer by being aware of the nature of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the bank is consistent with that business.

9.2 Legal Obligations of CDD

Under the obligation of MLPA, 2012, *"The branch shall have to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts and provide with the information maintained under the clause to BFIU, Bangladesh Bank."*

According to MLP Act 2012, SRO No. 357-Law/2013 dt. 21/11/2013, part-vi, sec-17(3) under MLP rules 2013, 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.

- (1) 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.
- (2) 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.
- (3)(a) 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.
- (3)(b) 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 risk categories customers with utmost care and need to mitigate any sort of risk.



9.3 General Rule of CDD

Completeness and Accuracy of the customer information

Branch must take customer's identity and underlying purpose of establishing relationship with the branch, and should collect sufficient information up to its satisfaction. "**Satisfaction of the bank**" means satisfaction of the appropriate authority that is necessary due diligence has been conducted considering the risks of the customers in the light of existing directions.

It is an obligation for branches to maintain **complete** and **accurate** information of their customer and person acting on behalf of a customer. '**Complete**' refers to combination of all information for verifying the identity of the person or entity. *For example: name and detail address of the person, profession, source of funds, Passport/National Identity Card/Birth Registration Certificate with acceptable ID card with photo, phone/ mobile number etc.* '**Accurate**' refers to such complete information that has been verified for accuracy.

KYC procedures refer knowing a customer physically and financially. This means to conduct an effective KYC, it is essential to accumulate **complete** and **accurate** information about the prospective customer.

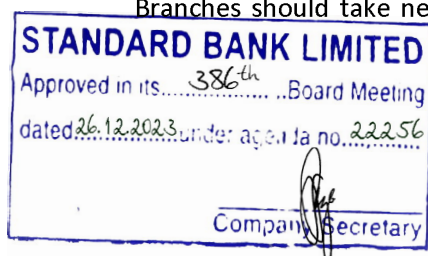
Branch should verify this information using reliable, independently sourced documents and data. Documentary verification procedures include:

- Confirming the identity from an unexpired official document that bears a photograph of the customer.
- Confirming the validity of the official documentation (like NID checking through software provided by Election Commission).
- Confirming the residential address (by obtaining Utility Bill/physical verification/sending thanks letter).

If the Branch is unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information, unable to identify the beneficial owner taking reasonable measures, 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. **Annexure-A (KYC Documentation)** provides an example of collection of documents and verification process of customer before opening account or conducting any transaction.

Ongoing CDD measures (Review and update)

Branches should take necessary measures to **review** and **update** the KYC of the customer after a



certain interval. This procedure shall have to be conducted in every two years in case of low risk customers. Furthermore, this procedure shall have to be conducted in every year in case of high risk customers. But, branches should update the changes in any information on the KYC as soon as branch gets to be informed. Moreover, branches should update KYC information anytime if there is any particular necessity realized. Depending on the updated information, the risks associated with these accounts shall have to be assessed again without any delay.

Branch should collect the Transaction Profile of customer account in the specified form. After reviewing the nature of the customer, the source of money/fund in the account and the nature of transaction, branch should again collect the Transaction Profile along with the amendments in it from the customer by reviewing the transactions of the customer within 6 (six) months of establishing business relation and assessing the effectiveness with a logical consideration.

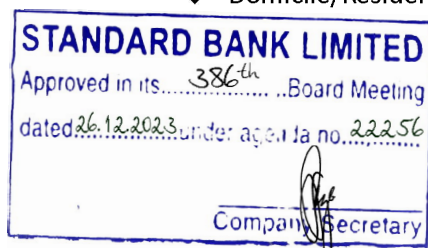
Enhanced CDD measures for high risk customer

Branches should conduct Enhanced CDD measures, when necessary, in addition to normal CDD measures. Branch should conduct Enhanced Due Diligence (EDD) under the following circumstances in line with BFIU:

- ❖ Individuals or legal entities scored with high risk;
- ❖ Individuals who are identified as Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top level officials of any international organization;
- ❖ Transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes;
- ❖ While establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering and terrorism financing (such as the countries and territories enlisted as High-Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement).

Higher risk customers and their transactions should be reviewed even more closely at account opening and more frequently during their account relationships. Branch should consider obtaining additional information from high risk customers such as:

- ❖ Source of funds and wealth
- ❖ Identifying information on individuals with control over the account, such as signatories or guarantors
- ❖ Occupation or type of business
- ❖ Financial statements
- ❖ Reference checking
- ❖ Domicile/Residence



- ❖ Proximity of the customer's residence, place of employment, or place of business
- ❖ Description of the customer's primary trade area and whether international transactions are expected to be routine.
- ❖ Description of the business operations, the anticipated volume of currency and total sales, and list of major customers and suppliers.
- ❖ Explanation of changes of account activity.

Simplified CDD measures

Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of the services or customer becoming involved in money laundering or terrorist financing. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). The possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

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

9.4 Timing of CDD

A branch must apply CDD measures when it 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.

9.5 Transaction Monitoring

Branch needs to monitor the transactions of customer on a regular basis. The complex transaction, transactions with deviation from normal transaction and the transactions that does not have reasonable purpose or the transaction with unusual pattern shall have to be more emphasized



during monitoring. An effective system has to be developed by the banks to review the risk by maintaining a specific time interval; and according to the review, Enhanced Due Diligence has to be maintained for accounts that are in high risk category.

Branch should put in place various ways of transaction monitoring mechanism within their branches that includes but not limited to the followings:

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

9.6 Exception when opening a bank account with Standard Bank

The verification of the documents of account holder may take place after the account has been opened, provided that there are adequate safeguards in place to ensure that, before verification has been completed

- a) the account is not closed;
- b) transaction is not carried out by or on behalf of the account holder (including any payment from the account to the account holder)

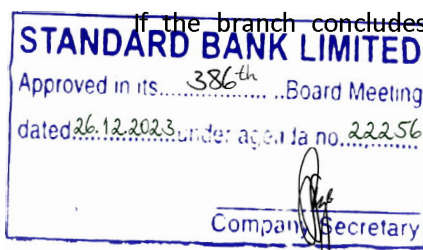
9.7 In case where conducting the CDD measure is not possible

If conducting the CDD measure becomes impossible because of the non-cooperating behavior of the customer or if the collected information seemed to be unreliable, that is, branch could not collect satisfactory information on customer identification and could not verify that, branch should take the following measures:

- (a) must not carry out a transaction with or for the customer through a bank account;
- (b) must not establish a business relationship or carry out an occasional transaction with the customer;
- (c) must terminate any existing business relationship with the customer;
- (d) must consider whether it ought to be making a report to the BFIU through an STR/SAR.

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

If the branch concludes that the circumstances do give reasonable grounds for knowledge or



suspicion of money laundering or terrorist financing, a report must be sent to the BFIU. The branch must then retain the funds until consent has been given to return the funds to the source from which they came.

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

9.8 Customer Identification

Customer identification is an essential part of CDD measures. For the purposes of this Guidance Notes, a customer includes:

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

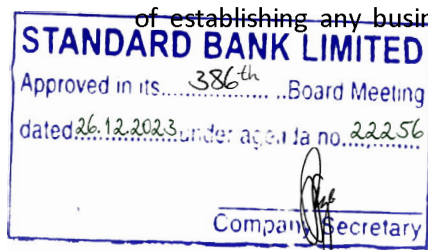
The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for branches to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware of 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.

Whenever the opening of an account or business relationship is being considered, or a one-off transaction or series of linked transactions is to be undertaken, identification procedures must be followed. Identity must also be verified in all cases where money laundering is known, or suspected.

Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained as set out Chapter VII (Record Keeping), and information should be updated or reviewed as appropriate.

9.9 Verification of Source of Funds

Branch should collect and verify the document supporting source of fund of the person at the time of establishing any business relationship or while conducting CDD. The document could include



present employment identity, salary certificate/copy/advice, pension book, financial statement, income tax return, business documents or any other documents that could satisfy the branch. The branch should request the person to produce E-TIN (Electronic Tax Identification Number) certificate which declares taxable income.

9.10 Verification of Address

Branch should verify the address of the person at the time of establishing any business relationship or while conducting CDD. This could be done through the physical verification by the branch or by standard mail or courier service correspondence. The branch could collect any other document (recent utility bill mentioning the name and address of the customer) as per their satisfaction.

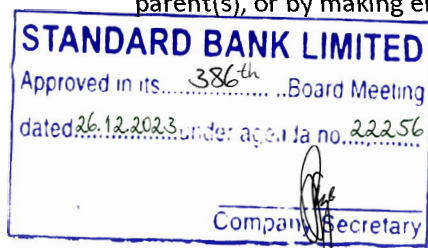
Verification of the information obtained must be based on reliable and independent sources – which might either be a document or documents produced by the customer, or electronically by the branch, or by a combination of both. Where business is conducted face-to-face, branch should see original of any documents involved in the verification.

9.11 Persons without Standard Identification Documentation

Most of the 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, street children or people, students and minors shall not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approaches and some flexibility considering risk profile of the prospective customers without compromising sufficiently rigorous anti money laundering procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances.

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 Head of Branch 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.

For students or other young people, the normal identification procedures set out as above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant's educational institution.



Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

9.12 Walk-in/one off Customers

Branch should collect complete and accurate information while serving Walk-in customer, i.e. a customer without having account. Branch should know the sources of fund and motive of transaction while issuing DD/PO or serving for TT/MT.

Branch must collect complete and accurate information of any person other than customer deposit or withdrawal using on-line facilities. Additionally, in regards to on-line deposit, branch should identify sources of funds as well.

9.13 Non Face to Face Customers

'Non face to face customer' refers to *"the customer who opens and operates his account by agent of the bank or by his own professional representative without having physical presence at the premises of bank branch"*. To avoid money laundering and terrorist financing risks while providing service to non-face to face customer, branch should apply one or more of the following measures of control:

- a) Ensuring that the customer's identity is established by additional ID documents, information provided by the Government Department or agency should be verified.
- b) Certified true copy of Passport/NID must be collected, where there is a non face to face contract.

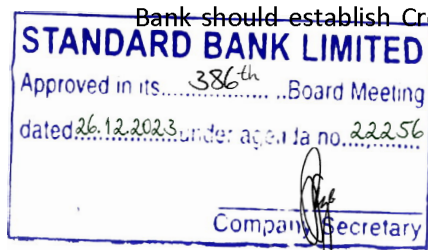
9.14 Customer Unique Identification Code

Branch should use unique identification code for any customer maintaining more than one account or availing more than one facilities from our bank. Such unique identification system could facilitate banks to avoid redundancy, and saves time and resources. This mechanism also enables banks to monitor customer transactions effectively.

9.15 Corresponding Banking

'Cross Border Correspondent banking' shall refer to "providing banking services to another bank (respondent) by a bank (correspondent). These kinds of banking services shall refer to credit, deposit, collection, clearing, payment, cash management, international wire transfer, drawing arrangement for demand draft or other similar services.

Bank should establish Cross Border Correspondent Banking relationship after being satisfied about



the nature of the business of the correspondent or the respondent bank through collection of information as per BFIU circular-26 dated 16th June, 2020. The Bank should also obtain approval from its senior management before establishing and continuing any correspondent relationship. The Bank must be sure about the effective supervision of that foreign bank by the relevant regulatory authority. Bank should not establish or maintain any correspondent relationship with any shell bank and not to establish or maintain any relationship with those correspondent or respondent banks that establish correspondent banking relationship or maintain accounts with or provide services to a shell bank.

Bank should pay particular attention or conduct Enhanced Due Diligence while establishing or maintaining a correspondent banking relationship with banks incorporated in a jurisdiction that do not meet or have significant deficiencies in complying international standards for the prevention of money laundering and terrorist financing (such as the countries and territories enlisted in High-Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force’s Public Statement). Detailed information on the beneficial ownership of such banks and extensive information about their policies and procedures on preventing money laundering and terrorist financing shall have to be obtained.

The bank will not allow third parties use its correspondent bank account(s) i.e. in the form of “Payable through account”.

9.16 Politically Exposed Persons (PEPs), Influential Persons and Chief Executives or Top Level Officials of any International Organization:

All Clients must be subject to an assessment to determine whether they are PEP’s or Influential Persons or chief executives or top level officials of any international organization and their linked entities. These customers pose a higher risk of money laundering, bribery, corruption and reputational risk to the bank due to their current or former position of political power or influence, which makes them more vulnerable to corruption. Relationships with these customers may increase the risk to the bank due to the possibility of that individuals holding such positions may misuse their power and influence for personal gain or advantage or for the personal gain or advantage of their Close Family Members and Close Associates. The person’s status (PEP’s, Influential Persons and chief executives or top level officials of any international organization) itself does not incriminate individuals or entities. It does, however, put a prospective or existing Client into a higher risk category.

As per BFIU circular 26 dated 16.06.2020, the process of the approval of these types of account is - **“Branch will send the Account Opening Form (AOF) of PEPs, Influential Person, Higher Management employees of International Organization and their close family members and close associates to AML & CFT Division before establishing relationship with them. After scrutinizing the said AOF, AML & CFT Division will send it for approval to Chief Anti Money Laundering Compliance**

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



Officer (CAMLCO), if found in order. Then the AOF will be returned to the respective branch (es) and the Management of the said branch(es) is hereby instructed to closely monitor them.”

Definition of PEPs:

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

- i) heads and deputy heads of state or government;
- ii) senior members of ruling party;
- iii) ministers, deputy ministers and assistant ministers;
- iv) members of parliament and/or national legislatures;
- v) members of the governing bodies of major political parties;
- vi) members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- vii) heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
- viii) heads of state-owned enterprises.

CDD measures of PEPs:

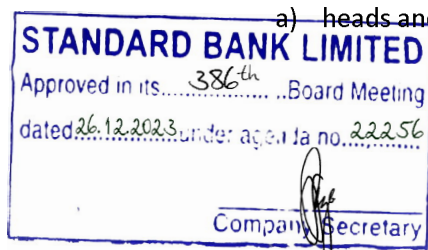
Branch need to identify whether any of their customer is a PEPs. Once identified branch need to apply enhanced CDD measures. Moreover, they need to perform the following-

- a) Branch have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP;
- b) obtain senior managements’ approval before establishing such business relationship;
- c) take reasonable measures to establish the source of fund of a PEP’s account;
- d) monitor their transactions in a regular basis; and
- e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

Definition of Influential Persons:

‘**Influential persons**’ refers to, “Individuals who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.” The following individuals must always be classed as Influential persons:

- a) heads and deputy heads of state or government;



- b) senior members of ruling party;
- c) ministers, state ministers and deputy ministers;
- d) members of parliament and/or national legislatures;
- e) members of the governing bodies of major political parties;
- f) Secretary, Additional secretary, joint secretary in the ministries;
- g) Judges of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- h) governors, deputy governors, executive directors and general managers of central bank;
- i) heads of the armed forces, other high ranking members of the armed forces and heads of the intelligence services;
- j) heads of state-owned enterprises;
- k) members of the governing bodies of local political parties;
- l) ambassadors, *chargés d'affaires* or other senior diplomats;
- m) city mayors or heads of municipalities who exercise genuine political or economic power;
- n) board members of state-owned enterprises of national political or economic importance.

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

CDD measures for influential persons:

Branch need to identify whether any of their customer is an Influential Person (IP). Once identified branch need to apply enhanced CDD measures. Moreover, they need to perform the following-

- a) Branch has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is an IP;
- b) obtain senior managements' approval before establishing such business relationship;
- c) take reasonable measures to establish the source of fund of a IP's account ;
- d) monitor their transactions in a regular basis; and
- e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

Definition of Chief Executives or Top Level Officials of any International Organization:

'Chief executive of any international organization or any top level official' refers to, "Persons who



are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the boards or equivalent functions.” The heads of international organizations and agencies that exercise genuine political or economic influence (e.g. the United Nations, the International Monetary Fund, the World Bank, the World Trade Organization, the International Labour Organization) must always be classed as this category.

CDD measures for Chief Executives or Top Level Officials of any International Organization:

Branch need to identify whether any of their customer is a CEO or top level officials of any international organization. Once identified branch need to apply enhanced CDD measures. Moreover, they need to perform the following-

- a) Branch has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a CEO or top level officials of any international organization;
- b) obtain senior managements’ approval before establishing such business relationship;
- c) take reasonable measures to establish the source of fund of the account of a CEO or top level officials of any international organization;
- d) monitor their transactions in a regular basis; and
- e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

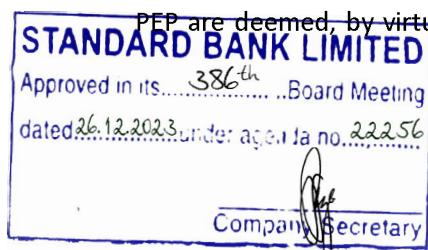
Close Family Members and Close Associates of PEPs, Influential Persons and Chief Executives or Top Level Officials of any International Organization:

In addition, close family members and close associates of these categories will also be classified as the same category. Close Family Members include:

- a) the PEP’s/influential persons/chief executive of any international organization or any top level official’s **spouse** (or any person considered as equivalent to the spouse);
- b) the PEP’s/influential persons/chief executive of any international organization or any top level official’s **children and their spouses** (or persons considered as equivalent to the spouses); and
- c) the PEP’s/influential persons/chief executive of any international organization or any top level official’s **parents**;

There may be exceptional circumstances where the individual should not be classified as a ‘Close Family Member’ of the PEP, such as estrangement, divorce etc. In such cases, the circumstances must be thoroughly investigated, examined and caution exercised.

In addition, where other family members such as the siblings, cousins, relatives by marriage of the PEP are deemed, by virtue of the nature of the relationship, to have a close relationship with the



PEP, they should also be classified as PEPs.

A Close Associate of a PEP/Influential Person/Chief executive of any international organization or any top level official includes:

- a) an individual who is known to have joint beneficial ownership or control of legal entities or legal arrangements, or any other close business relations with the PEP; and
- b) an individual who has sole beneficial ownership or control of a legal entity or legal arrangement which is known to have been set up for the benefit of the PEP.

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

CDD measures for Close Family Members and Close Associates of PEPs, Influential Persons and Chief Executives or Top Level Officials of any International Organization:

Branch need to identify whether any of their customer is a family member or close associates of a PEP, IP or CEO or top level officials of any international organization. Once identified branch need to apply enhanced CDD measures. Moreover, they need to perform the following-

- a) Branch has to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a family member or close associates of a PEP, IP or CEO or top level officials of any international organization;
- b) obtain senior managements' approval before establishing such business relationship;
- c) take reasonable measures to establish the source of fund of the account of a family member or close associates of a PEP, IP or CEO or top level officials of any international organization;
- d) monitor their transactions in a regular basis; and
- e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied accordingly.

9.17 Wire Transfer

"Wire transfer" refers to such financial transactions that are carried out on behalf of an originator (person or institution) through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution.

9.17.1 Cross-Border Wire Transfers

Branches or Authorized Subsidiaries or concerned Head Office Divisions which are the ordering banks/Branches are required to ensure that the message or payment instruction for all cross- border wire transfers involving an amount equivalent to USD.1000.00 and above are accompanied by the following information before transmitting the same to Intermediary/Beneficiary Banks:



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

(i) name; (ii) account number (or a unique reference number if there is no account number) which permits traceability of the transaction; (iii) residential or mailing address ; (iv) Passport/NID/Birth Registration/Any acceptable ID with Photo; (v) Phone/Active Mobile No.

Collected & preserved the meaningful beneficiary information such as:

(i) name; (ii) account number (or a unique reference number if there is no account number), which permits traceability of the transaction; and (iii) Details Address.

Furthermore, for cross-border wire transfers, below the threshold (USD.1000.00) full and meaningful originator information has to be preserved. For providing money of cross-border wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved.

Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file has to contain required and accurate originator information, and full beneficiary information. In addition, bank should include the account number of the originator.

9.17.2 Domestic Wire Transfers

In case of threshold domestic wire transfers of at least BDT 25,000/- (twenty five thousands), complete and accurate information of the originator has to be collected, preserved and has to be sent to intermediary/beneficiary bank/institutions. Furthermore, for domestic wire transfers below the threshold full and meaningful originator information has to be preserved. For providing money of domestic wire transfers to beneficiary, full and meaningful beneficiary information has to be preserved. Mobile financial services providing department should use KYC format provided time to time by Payment System Department, Bangladesh Bank, in addition to aforesaid instructions. In case of wire transfer by using debit or credit card (except buying goods and services), similar information as above has to be preserved in the payment related message/instructions.

9.17.3 Duties of Ordering, Intermediary and Beneficiary Bank in case of Wire Transfer

Ordering Bank:

The ordering bank should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information. These information has to be preserved minimum for 5 (five) years.



Intermediary Bank:

For cross-border and domestic wire transfers, any bank working as an intermediary between ordering bank and beneficiary bank, should ensure that all originator and beneficiary information that accompanies a wire transfer is retained. A record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution (or as necessary another intermediary financial institution).

An intermediary financial institution should have effective risk-based policies and procedures for determining reasonable measures to identify wire transfers that lack required originator information or required beneficiary information such as execution, rejection, or suspension of that wire transfer and the appropriate follow-up action. Such measures should be consistent with straight-through processing.

Beneficiary Bank:

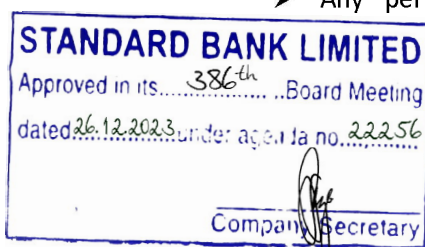
A beneficiary financial institution should initiate risk based procedure to identify wire transfers that lack required originator or required beneficiary information. In case of insufficient originator information concerned parties should collect those information through mutual communication or using any other means. During the payment to receiver/beneficiary, the bank should collect complete and accurate information of receiver/beneficiary and should preserve those information for 5 (five) years.

An intermediary financial institution should have effective risk-based policies and procedures for determining reasonable measures to identify wire transfers that lack required originator information or required beneficiary information such as execution, rejection, or suspension of that wire transfer and the appropriate follow-up action. Such measures should be consistent with straight-through processing.

9.18 CDD for Beneficial Owner:

Branch should apply CDD obligations for the beneficial owners of the accounts before or during the course of establishing a business relationship or conducting occasional transactions. In doing so, banks should put in place appropriate measures to identify beneficial owner. Branch, upon its own satisfaction ensure CDD of beneficial ownership by collecting information and documents from independent and reliable sources that includes publicly available information, information from customer or information from other reliable sources. Banks should consider following aspects while identifying beneficial ownership includes:

- Any natural person operating accounts on behalf of customer;
- Any person (whether acting alone or together) who has controlling profit



/income or ownership profit /income on a customer who might be legal entity or legal arrangements. Where there is any doubt identifying controlling interest, the banks should consider other means to determine controlling profit /income or ownership of a legal entity or arrangements. In addition to that bank should also consider reasonable measures to verify the identity of the relevant natural person who hold senior management position;

- Any person or entity who has controlling or 20% or above shareholding within any or legal entity.
- The settler(s), trustee(s), the protector, the beneficiaries or class of beneficiaries, or any other natural person who exercises control over the trust.
- Any person in equivalent or similar position for trust (as mentioned above) should consider for other types of legal arrangements.

Where, a natural or legal persons who holds controlling interest, listed on a stock exchange and subjects to disclosure requirements or majority owned subsidiaries of such listed companies may exempted from identifying or verifying beneficial ownership requirements.

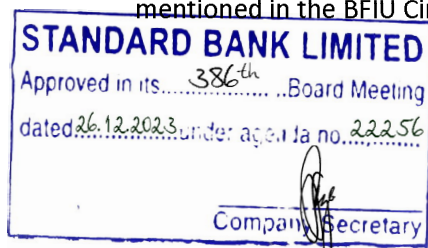
9.19 Agent Banking:

Agent Banking means providing limited scale banking and financial services to the underserved/unbanked population through engaged agents under a valid agency agreement, rather than a teller/cashier. It is the owner of an outlet who conducts banking transactions on behalf of a bank. Agent Banking is a most important distribution channel for financial inclusion. Standard Bank has decided to promote this complimentary channel to reach to the poor segment of the society as well as existing bank customer with a range of financial services specially to geographically dispersed locations.

A bank agent is supposed to be equipped with Biometric device, PIN input pad or EMV certified P.O.S. terminal with which they can process withdrawals and deposits of the customer. These P.O.S. devices connect to the core banking system via internet connectivity.

The Bank agency model has been a hub and spoke model, with agents being associated with a nearby bank's branch from which their liquidity is managed by the bank. The agent banking outlet must have at least 2 (two) persons (a manager and a teller) with required managerial and financial expertise for this purpose and 1 (one) counter for cash transaction.

For Agent Banking activities, agent outlets and tagged branch must follow the guidelines issued by the Agent Banking Division. Agent outlets and Branches shall also follow the respective agent banking guidelines, circulars issued by Bangladesh Bank, BFIU and ensure its implementation of AML & CFT related instruction contained therein. For Agent Banking activities, SBL follow the guidance mentioned in the BFIU Circular No. 26 dated 16.06.2020:



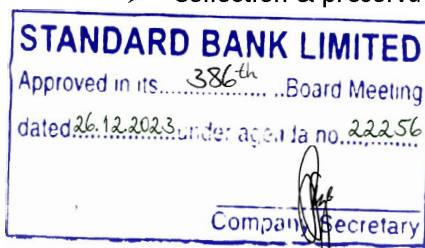
1. Uniform account Opening Form (UAOF) as per BRPD circular 02 dated 23.02.2020 should be used for opening account of agent and customers of the Bank.
2. Bank should be conscious regarding detecting & reporting of suspicious transactions or activity of agent and customer.
3. Activities of prevention of money laundering and terrorist financing shall be included in the compliance program of Agent Banking, and
4. Proper training of Agent on prevention of money laundering, terrorist financing and proliferation financing.

Selection criteria of Standard Bank Agent:

- Agent must have a permanent resident (As per as NID/Passport).
- Agent must have enough infrastructures for conducting Agent banking.
- Agent should be financially solvent & have ability to hard cash transaction.
- Agent should have ability to meet commitment with customer under adverse situation.
- Agent should have knowledge and ability to handle Technology based financial services.
- All deeds/transaction's record should be preserved for internal audit with enough securities.
- Agent cannot be engaged with any subversive activities.
- Agent should have ability to perform his/her responsibility properly.
- Agent must be concerned about the reputation of the institution.
- Agent should not be a investment defaulter and not penalized by any civil or criminal court
- For cash transaction, Agent have to maintain an account in Agent Banking system, which is fetched for cash deposit and withdrawal transaction by customers and system automatically debit or credit agent account and customer account simultaneously.
- Agent has to maintain sufficient balance to accommodate customer transaction value. The Agent account balance is determined on the volume of transaction and Agent account have to maintain sufficient balance and Cash in hand balance for uninterrupted transaction of customers.

Agent Responsibilities :

- Agent must be honest, professional & ethical to his / her duties;
- Agent must have proper knowledge about his duties & serve customer Agent Banking facilities;
- Maintenance of electronic device (Computer, POS Printer, Finger print machine etc.) and ensures enough security;
- Agent preserves all sorts of transaction record, evidence & deeds;
- Agent displays fixed charge of agent banking services in his/her booth;
- After a certain period of Agent submit regular/daily activities to respective officer;
- Agent must be bound to maintain internal rules & regulation of Standard Bank ;
- Agent is cordially cooperating to all sort of audit;
- Beside these other facilities directed by Standard Bank;
- Collection & preservation of A/C opening Form & others receipts copy;



- Facilitating small value investment disbursement and recovery of investment installments;
- Cheque receive for clearing;
- Provide salary, pension scheme & other gratuity services;
- Collection & preservation of necessary banking E-mail & letters.

As per BFIU Circular No. 26 dated 16.06.2020, Bank shall follow the following steps for appointment of Agent and monitoring their activities:

- i. Bank shall follow the proper screening mechanism for selecting agent and confirm the full and accurate information of the agent.
- ii. Risk grading of the agent on the basis of (i) transaction number and amount, (ii) geographical location, (iii) business & nature of ownership and (iv) other reasonable subject and monitoring of the transactions & activities of the agent.
- iii. Ongoing assessment of the risk (high, medium & low) of the agent by the institution.
- iv. Verification of the AML & CFT compliance level of the agent.
- v. Conducting audit and inspection related to AML & CFT of the high risk graded agent annually by the ICCD and the report will send to AML & CFT Division.
- vi. Conducting audit and inspection related to AML & CFT of medium & low risk graded agent at regular interval.
- vii. Updated list of Agent based on January to June should be disclosed in the website.
- viii. List of terminated Agent due to different irregularities or non-compliance should be disclosed in the website.

9.20 Mobile Banking:

Mobile Banking is the new era of banking to carry the banking facility to the door step of the customer under financial inclusion. Rapid growth of mobile phone users and wider range of the coverage of Mobile Network Operators (MNOs) has made their delivery channel an important tool-of-the-trade for extending banking services to the unbanked/banked population. In order to ensure the access of unbanked people by taking advantage of countrywide mobile network coverage, Mobile Banking services is introduced by the commercial banks of Bangladesh as per Bangladesh Bank guideline.

Mobile Financial Services:

Bangladesh Bank may allow the following Mobile Financial Services (in broad categories) -

- i. Disbursement of inward foreign remittances,
- ii. Cash in /out using mobile account through agents/Bank branches/ ATMs/Mobile Operator's outlets.
- iii. Person to Business Payments - e.g. a. utility bill payments, b. merchant payments
- iv. Business to Person Payments e.g. salary disbursement, dividend and refund warrant payments, vendor payments etc.



- v. Government to Person Payments e.g. elderly allowances. Freedom-fighter allowances, subsidies, etc.
- vi. Person to Government Payments e.g. tax, levy payments.
- vii. Person to Person Payments (One registered mobile Account to another registered mobile account).
- viii. Other payments like microfinance, overdrawn facility, insurance premium, DPS, etc.

Permissible Models:

Depending on the operation, responsibility and relationship(s) among banks, MNOs, Solution Providers and customers mainly two types of mobile financial services (Bank led and Non -Bank led) are followed worldwide. From legal and regulatory perspective, only the bank-led model will be allowed to operate. The bank-led model shall offer an alternative to conventional branch-based banking to unbanked population through appointed agents facilitated by the MNOs/Solution Providers. Customer account, termed "Mobile Account" will rest with the bank and will be accessible through customers' mobile device. Mobile Account will be a non-chequing limited purpose account.

Opening of Mobile Accounts:

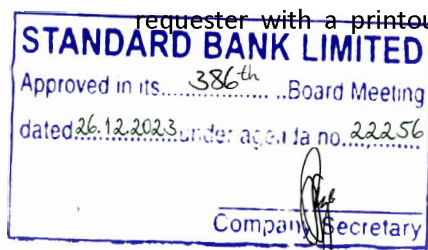
Banks must ensure that a 'Mobile Account' has been opened for each customer seeking to avail Mobile Financial Services with all the required documents and accurate KYC as per Bangladesh Bank Guideline.

AML & CFT Compliance:

1. Banks and its partners shall have to comply with the prevailing Anti Money Laundering (AML) & Combating the Financing of Terrorism (CFT) related laws, regulations and guidelines issued by BFIU, Bangladesh Bank from time to time.
2. Banks shall have to use a new 'Know Your Customer (KYC)' format as given in the guideline of Mobile Financial Services provided by Bangladesh Bank. The Bank will be responsible for authenticity of the KYC of all the customers.
3. Banks shall have to follow full KYC format issued by Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank for the cash points/agents/partners.
4. Banks shall ensure that suspect transactions can be isolated for subsequent investigation. Banks shall develop an IT based automated system to identify suspicious activity/transaction report (STR/SAR) before introducing the services.
5. Banks shall immediately report to BFIU, Bangladesh Bank regarding any suspicious, unusual or doubtful transactions likely to be related to money laundering or terrorist financing activities.

Record Retention:

MFS transaction-records must be retained for six (06) years from the origination date of the entry. The Participating Bank(s) must, if requested by its customer, or the Receiving Bank(s), provide the requester with a printout or reproduction of the information relating to the transaction. Banks



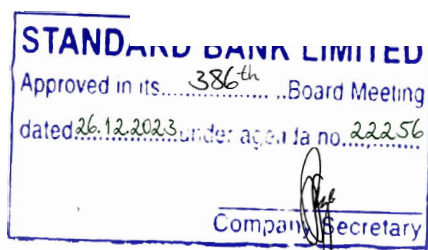
should also be capable of reproducing the MFS transaction-records for later reference, whether by transmission, printing, or otherwise.

Security Issues:

1. Banks shall have to follow the Guidelines on ICT Security for Scheduled Banks and Financial Institutions, 2010 issued by the Bangladesh Bank and ICT Act, 2006 to address the security issues of Mobile Financial Services.
2. The following properties need to be addressed to offer a secure infrastructure for financial transactions using mobile technology :
 - a. **Confidentiality:** Property that ensures transaction information cannot be viewed by unauthorized persons.
 - b. **Integrity:** Property that the transaction information remains intact during transmission and cannot be altered.
 - c. **Authorization:** Property that the authentic user has proper permission to perform the particular transaction. It ensures how the system decides what the user can do.
 - d. **Nonrepudiation:** Property that the particular transaction initiated by a user cannot be denied by him/her later.
3. All the transactions must be authenticated by the account holders using their respective Personal Identification Number (PIN) or similar other secured mechanism. To facilitate the mobile financial services, the said PIN may be issued and authenticated by the bank maintaining proper protection and security features.
4. The banks should ensure that a proper process is put in place to identify the customer when the service is being enabled.
5. A second factor of authentication should be built-in for additional security as chosen by the bank.

9.21 Management of Legacy Accounts

Legacy accounts refers those accounts opened before 30 April, 2002 and yet to update KYC procedures. These legacy accounts should be treated as "Dormant". No withdrawal should be permitted in those accounts; however, deposit can be permitted. These accounts will be fully functional only after conducting proper CDD measures. Central Compliance Unit should preserve data of such accounts at their end.



CHAPTER X: TRADE BASED MONEY LAUNDERING

10.1 Definition of TBML:

According to the International Narcotics Control Strategy Report (INCSR), hundreds of billions of dollar are laundered annually by way of Trade-Based Money Laundering (TBML). It is one of the most sophisticated and complex methods of cleaning dirty money, and trade-based money laundering red flags are among the hardest to detect.

FATF defines “Trade Based Money Laundering” as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin. Like money laundering through the financial system, TBML may occur in three stages. At the placement stage, the offender transforms illicit proceeds into a transferable asset (e.g., by purchasing goods); at the layering stage, the offender attempts to obscure the link between the illicit proceeds and their criminal source (e.g., by trading the goods across borders); and at the integration stage, the offender re-introduces the illicit proceeds into the legitimate economy (e.g., through resale of the goods).

10.2 Basic Trade Based Money Laundering Techniques

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 partners, who then sells them in the open market at their true value. The 2006 FATF study concluded that TBML represents an important channel of criminal activity and, given the growth of world trade, an increasingly important money laundering and terrorist financing vulnerability. Understanding the commercial purpose of any trade transaction is a key requirement in determining its money laundering risk. The basic techniques of trade based money laundering include:

- ❖ over- and under-invoicing of goods and services;
- ❖ multiple invoicing of goods and services;
- ❖ over- and under-shipments of goods and services; and
- ❖ falsely described goods and services.

10.2.1 Over- and Under-Invoicing of goods and services

According to the FATF, money laundering through over-and under-invoicing goods and services is one of the most commonly used methods for laundering funds across borders.



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).

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 receives when it is sold on the open market).

These types of transactions generally require collusion by both parties and can have significant tax implications. Also, products or complex products that travel through supply chains are more appropriate to be used in these types of over and under invoicing activities because they complicate the ability of customs officials to determine the true market value of such goods and services.

10.2.2 Multiple Invoicing of goods and services

By providing multiple invoices for the same transaction, a money launderer or terrorist financier can justify multiple payments for the same goods or services. In addition, by using a number of financial institutions to make these multiple payments, a money launderer or terrorist financier can increase the level of complexity of the transaction and complicate efforts at detection. If the transaction is detected, a launderer can offer a number of plausible explanations that compound efforts by officials to detect.

10.2.3 Over- and Under-Shipments of goods and services

In addition to manipulating the prices of goods and services, a money launderer can misstate the quantity of goods and services that are exported or imported. In the extreme, exporters and importers can collude in not shipping any goods at all but proceed with processing the necessary shipping and customs documents. Banks and other financial institutions may be unaware that these “phantom” transactions are occurring.

10.2.3 Falsely described goods and services

Money launderers also can misstate the quality, identity or the type of a good or service that is being traded. Such a misstatement creates a discrepancy between the value of a good that is stated on the shipment or customs forms and what is actually shipped.



10.3 Trade Based Money Laundering Risk

TBML is 'an increasingly important money laundering and terrorist financing vulnerability'. The features of trade make it highly attractive to money launderers. The chain of supply comprises many links, including transport, insurance and finance. More links provide more opportunity to launder money. International trade also involves different legal systems, different procedures and often different languages. These differences and discrepancies in communication and exchange of information between jurisdictions, compound to make international trade fertile ground for money laundering.

10.4 Instruments of Trade Finance and their vulnerabilities

The drawing of a '**bill of exchange**' (also referred to as a 'draft') is commonly used by exporters as a means of obtaining payment from buyers for goods shipped. Bills of exchange protects (reduces transactional risk) of both parties. Documentary credits issued for buyers by banks usually require bills of exchange to be drawn, and frequently bills of exchange are drawn by the seller in terms of the commercial contract of sale with the buyer or Proforma invoice.

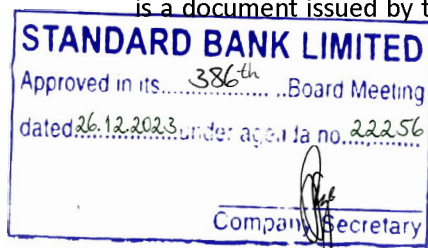
The Draft or Bill of Exchange (not always required) provides formal evidence of debt under a letter of credit and is presented with all other documents unless stipulated otherwise. A Draft may contain information on:

- Value of Draft or Bill of Exchange, date of payment and payment terms e.g. "at sight", "30 days after sight", "60 days after Bill of Lading Date" and so on.
- Date of presenting documents of Exporter to the "available with" Bank (not normally required).
- Letter of credit number assigned by the Issuing Bank (if required by credit).
- Date the letter of credit was issued (not normally found on a Bill of Exchange).
- Name and address of the Issuing Bank (if the Bill of Exchange is drawn on the issuing bank).
- Name and address of the bank on which the bill of exchange is to be drawn.
- Signature of an authorized signing officer of the Company and the Beneficiary's name as shown on the letter of credit.

The **Commercial Invoice** is the accounting document through which the exporter charges the importer for goods and services purchased. The Invoice gives details about:

- Merchandise weight, quantity and price and currency.
- The name and address of Exporter and the Importer.
- The number of copies presented and signed if required.
- The trade term listed, e.g. FOB, CFR, CIF, etc.

The **Transport Document** (or Bill of Lading, Airway Bill, Railway Consignment Note, Truck Receipt, etc.) is a document issued by the carrier that describes the goods that have been accepted for carriage. In







some forms, the Bill of Lading may also act as a document of title to the goods and should include information that is consistent with the letter of credit:

- Information on the merchandise (usually a general description).
- The points of loading and discharge.
- To whom the Bill of Lading is consigned.
- The date of shipment.

The **Insurance Document** is a guarantee in part or in whole (depending on the terms and conditions) by an insurance company, specifying the goods shipped on a named vessel, indicating the applicable coverage, and showing to whom loss is payable.

The **Certificate of Origin** notes the country where the goods were produced. The Certificate of Inspection offers an opinion that the specified quality and quantity related conditions have been met. These documents should be dated on or before the Bill of Lading date. In maximum cases, certificate of origin is issued by the Chamber of Commerce of the country or as per condition stipulated in the L/C.

A **Packing List** is usually supplied by the exporting shipper in cases where a diversified shipment is packed in several packages or containers. The list will show the contents of each box or case identified by a specific number. A Weight Certificate is supplied by the Exporter, at the request of the Importer. It certifies the weight of each large unit in a shipment or the net and gross weights of packages containing smaller units. It is of particular value when the price of the goods is based on weight and, also, is often used by the carrier in arriving at the weight to be recorded on the Bill of Lading as a basis for the freight charges.

The quantity of units/weights should match the Commercial Invoice (this may or may not agree based on how the weights are calculated by the various parties involved). The breakdown of merchandise/weight per carton, package or container should be shown if requested in the letter of credit.

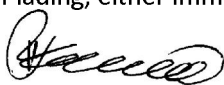
Vulnerabilities:

- a) Undertaken and paid for without any form of due diligence by an intermediary in the supply chain because the parties are complicit.
- b) Phantom trades maybe the cause of unrealistic timeframes or unrealistically short supply chains.

Documentary Credit (Letter of Credit, etc.)

Generally the exporter requires an importer to prepay in cash for goods shipped. The importer naturally wants to reduce risk by asking the exporter to acknowledge through documents that the goods have been shipped. The importer's bank assists by providing a letter of Credit (Documentary credits) to the exporter (or the exporter's bank) providing for payment upon presentation of certain

documents, such as a bill of lading, either immediately or at a prescribed date.



A letter of credit is a precise document whereby the importer's bank extends credit to the importer and assumes responsibility in paying the exporter. Aside from the letter of credit document, other documents used in legitimate Trade include shipping and insurance documents, and commercial invoices. The documentary credit arrangement offers an internationally recognized and used method of attaining a commercially acceptable undertaking by providing for payment to be made against presentation of documentation representing the goods, making possible the transfer of title to those goods.

Vulnerabilities:

- a) Even in this simple form the true value of goods transferred between countries can be masked through misrepresentation of price, quantity and quality. Letters of Credit may be generated to create a veneer.
- b) The documentation generated in the process leaves a paper trail which money launderer may rely upon to disguise illegal proceeds.

Bai –Salam (Pre-Shipment Finance)

This is financing for the period prior to the shipment of goods, to support pre-export activities like wages and other costs. It is especially needed when inputs for production must be imported. It also provides additional working capital for the exporter. Bai- Salam (Pre-shipment) financing is especially important to smaller enterprises because the international sales cycle is usually longer than the domestic sales cycle. Bai- Salam (Pre-shipment) financing can take the form of short-term investments named Packing Credit in maximum conventional banks, overdrafts and cash credits.

Vulnerabilities:

- a) Bai- Salam (Pre-shipment) finance especially its application to 'inputs for production that must be imported' provides the money launderer with an ability to engage a third party in another jurisdiction thus moving value to all venues in which the criminal syndicate are operating and thus widen the scope for TBML.
- b) Short-term investments, Bai- Muajjal (overdrafts) and Bai- Muajjal general (cash credits) may allow launderers to make business claims on the relevant revenue agencies in those countries thus supplementing their reasons for the value they hold.

Post-Shipment Finance

This is financing for the period following shipment. The ability to be competitive often depends on the trader's credit term offered to buyers. Post-shipment financing ensures adequate liquidity until the purchaser receives the products and the exporter receives payment. Post-shipment financing is usually short-term. In Standard Bank it can be in mechanism of Foreign Documents Bill Purchased (FDBP), discounting the export bill, etc.



A handwritten signature in blue ink.



A handwritten signature in blue ink.

Vulnerabilities:

a) Although this method of financing is short term by nature, cash is usually supplied at time of sale, hence such pretense would not raise suspicion unless intelligence arouse such suspicion.

Buyer's Credit

A financial arrangement whereby a financial institution in the exporting jurisdiction extends a investment directly or indirectly to a foreign buyer to finance the purchase of goods and services from the exporting jurisdiction. This arrangement enables the buyer to make payments due to the supplier under the contract.

Vulnerabilities:

- a) Financing of the importer by an institution in the exporter's jurisdiction widen the scope for TBML, since to exercise due diligence in a foreign jurisdiction may be more difficult.
- b) The money launderers seek this credit to help minimize risk of confiscation.
- c) If a financial institution has a stake in the trade, law enforcement has to account for that stake in any ensuing action unless the law enforcement action can demonstrate that the financial institution in complicit.

Supplier's Credit

A financing arrangement under which an exporter extends credit to the buyer in the importing jurisdiction to finance the buyer's purchases.

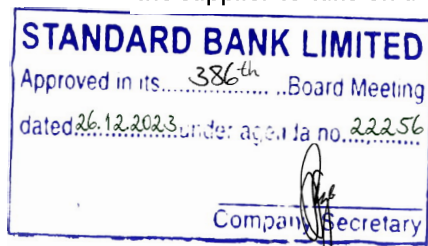
Vulnerabilities:

- a) The utilization of Supplier's Credit arrangements provide a mechanism to move significant amounts of value in most forms irrespective of whether or not the trade is legitimate, inflated or phantom.
- b) This financing arrangement need not involve a financial institution, although to reinforce the veneer, engaging the third party may be undertaken in ML schemes.
- c) If the buyer and seller are in collusion, this mechanism is a channel for TBML.

Countertrade

Countertrade exists where economies face the problem of limited foreign exchange holdings. That is, they do not hold enough currency of the jurisdiction they are trading with to pay the outstanding debt and the cost of buying more foreign currency to service that debt makes the trade uneconomical.

One way to overcome this constraint is to promote and encourage countertrade. It generally encompasses the idea of subjecting the agreement to purchase goods or services to an undertaking by the supplier to take on a compensating obligation in lieu of a cash settlement. The seller is required to



accept goods or other instruments of trade in partial or whole payment for its products. Some of the forms of counter trade include:

- **Barter** – This traditional type of countertrade involving the exchange of goods and services against other goods and services of equivalent value, with no monetary exchange between exporter and importer.
- **Counter purchase** – The exporter undertakes to buy goods from the importer or from a company nominated by the importer, or agrees to arrange for the purchase by a third party. The value of the counter-purchased goods is an agreed percentage of the prices of the goods originally exported.
- **Buy-back** – The exporter of heavy equipment agrees to accept products manufactured by the importer of the equipment as payment.

Vulnerabilities:

The TBML vulnerabilities arise in determination of exchange ratios for the goods to be countertraded. Such ratios may often be determined as a process of negotiation rather than market determined, giving scope to TBML.

Open Account Facilities

Open account transactions can be described as 'buy now, pay later' and are more like regular payments for a continuing flow of goods rather than specific transactions. The pursuit of 'supply chain efficiencies' among larger businesses has encouraged their preference for open account trading. Trade Finance has been shifting away from L/C or documentary credit. Trade Finance should be flexible and that financiers will benefit by adapting product and service offerings to the needs of customers in different segments.

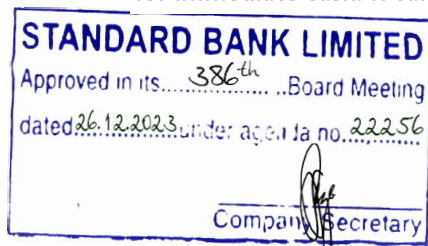
Vulnerabilities:

- a) Open account facilities have caused a disconnect between the movement of the underlying trade and the money used to finance it.
- b) Payments against these facilities may or may not be undertaken through an international funds transfer instruction (IFTI) or SWIFT.

A range of Open Account Facilities are set out below.

Factoring

Factoring, also known as invoice discounting, receivables factoring or debtor financing, is where a third party company assumes a debt or invoice from another company. This involves either the sale at a discount of accounts receivable or other debt assets on a daily, weekly or monthly basis in exchange for immediate cash. It can also involve the charging of profit /income on the debt. The debt assets are



sold by the exporter at a discount to a factoring house, which thereby assumes part of risks of the account receivable. Factoring in international trade is the discounting of a short-term receivable (up to 180 days). The exporter transfers title to its short-term foreign accounts receivable to a factoring house for cash at a discount from the face value. It allows an exporter to ship on open account as the factor assumes the financial liability of the importer to pay and handles collections on the receivables. The factoring house usually works with consumer goods.

Factoring is divided into import factoring and export factoring. Details of each are set out below.

Export factoring:

In export factoring, the Factor deals directly with the seller of the goods. In this case the debt is a 'recourse' debt, and if the seller goes under, or the purchaser does not pay, the local Factor assumes the risk. In Export factoring the local Factor, deals with a counterparty Factor, who will check out the creditworthiness of the purchaser.

In this case the seller will provide documentation to show that the goods have been shipped prior to payment. Payment is usually made on an 80/20 split, 80% is paid to the seller at the time of the invoice/goods shipment. This amount is investmented to the seller by the Factor and profit /income charged until the purchaser pays. When the purchaser pays the 100% of the invoice the Factor pays the seller the other 20% of the invoice. There is usually a small activity fee (around 1% of the invoice that is also charged, so it is typically a 80/1/19 split).

Import Factoring:

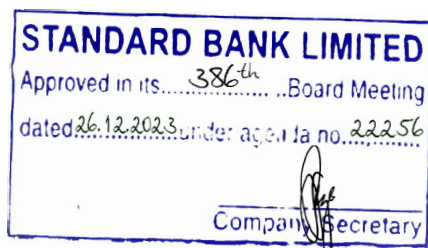
Import factoring is a reverse of the scenario set out for export factoring, but differs slightly. The local Factor will insure the risk on a usually 80% basis, and will therefore carry a 20% risk. This is called a 'non-recourse debt'. The local Factor will check out the bona fide credit history etc. of the purchaser of the goods. Credit lines etc. are usually established.

The foreign factor will examine the bills of lading shipping documents etc. and confirm with the Local Factor. International factoring (as opposed to domestic factoring) have more to do with the counterpart abroad and with insuring risk.

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 factors' 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.

1. The parent company ships goods to its subsidiary, which sells and ships the goods to the debtors in the import factor's country.
2. The seller assigns his invoices on the subsidiary via export factor to import factor.



3. The subsidiary assigns its receivables to the import factor with or without credit risk coverage.
4. The export factor pays the parent company the agreed advances.
5. The subsidiary's debtors pay the import factor.

Vulnerabilities:

- Often the factor may be left with losses after the so-called traders disappear, after having indulged in TBML, by moving illicit funds through 'sham trade'.

Forfaiting

Forfaiting is the purchase of an exporter's receivables (the amount importers owe the exporter) at a discount by paying cash. The purchaser of the receivables, or forfaiter, must now be paid by the importer to settle the debt. As the receivables are usually guaranteed by the importer's bank, the forfaiter frees the exporter from the risk of non-payment by the importer. The receivables have then become a form of debt instrument that can be sold on the secondary market as bills of exchange or promissory notes. Forfaiting is a method of trade financing that allows the exporter to sell its medium-term receivables (180 days to 7 years) to the forfaiter at a discount, in exchange for cash. With this method, the forfaiter assumes all the risks, enabling the exporter to extend open account terms and incorporate the discount into the selling price. Forfaiters usually work with capital goods, and large projects.

Vulnerabilities:

- These instruments (exporter's receivables) are capable of being sold on the secondary market as 'bills of exchange' or 'promissory notes', provides a money launderer with an enhanced mechanism to move value.
- If the launderer, through collaboration inflates the value of receivables more value can be moved.

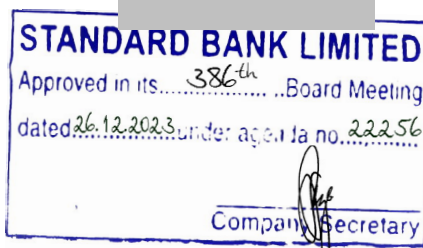
10.5 Main Risks Associated with Trade Finance

Although Trade Finance was traditionally considered a lower-risk activity, due to its short-term, self-liquidating, and collateralized characteristics, growing complexities and volume of trade flows create opportunities for criminal activities. And with that, grows the need for increasingly comprehensive risk control measures. There are different types of risks involve with trade finance like credit, profit /incomerate, liquidity, price, strategic, **operational, compliance and reputational**.

AML Related Risks

Operational Risk

- Heavy reliance on manual processing and paper documentation
- Susceptibility to missing, incomplete, or fraudulent documentation
- Unclear terms or nonstandard language may nullify traditional protection to a bank



Compliance Risk

- Including risk of failure to comply with AML & different Sanctions Screening
- Risk of failure to comply with similar requirements in a foreign counterpart's country

Reputational Risk

- Bank's reputation is important for Trade Finance activities, and lack of due diligence or compliance with regulatory authority may ultimately reduce the number of business opportunities

10.6 Standard Bank Role

Bank facilitates global trade by offering various financial products (e.g. Letters of credit, guarantees, etc.) and thus play a vital role in mitigating the risk associated with Trade Based Money Laundering. In order to effectively minimize this risk, AD branch/Corporate Office Division must effectively perform the following:

KYC & Customer Relationship:

Maintaining an effective "Know Your Customer" (KYC) Program is critical to assess and monitor customer risk. KYC refers to the steps taken by the bank to:

1. Establish the identity of the customer;
2. Understand the nature of the customer's activities; and
3. Assess the customer money laundering risks to establish the necessary level of monitoring

Trade-related Due Diligence:

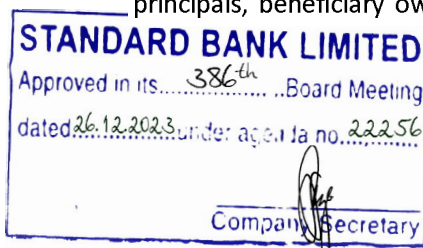
Due diligence should include gathering sufficient information on Applicants and Beneficiaries as well as information on the goods traded and the methods of transportation (i.e. vessels).

Transaction Monitoring:

Transaction Monitoring Program should monitor and alert transactions for potential violations of Anti Money Laundering Laws and Sanctions Programs.

10.7 General CDD requirements in Trade Finance

Standard Bank provides export and import business and other trade transaction to their customers. In trade finance different types of customer involve like importers, exporters, foreign/local suppliers, foreign/local buyers, agents of the foreign suppliers, agents of the foreign buyers, agents of foreign principals, beneficiary owners, authorized persons or entities related to an international/local trade



transaction.

Branch, authorized subsidiaries and concern corporate office division must comply the CDD measures, which is discussed in the chapter number six before executing any international and/or local trade transaction in favor of their customers or offering any trade finance and trade service related facility to their customers.

10.7.1 CDD Measures for Import Business

10.7.1.1 KYC Policy & Procedures

For any new import customer in Standard Bank, Branches or Authorized Subsidiaries or concerned Corporate Office Divisions are required comply the customer acceptance policy.

Branches or authorized subsidiaries or concerned Corporate Office Divisions are required to collect or ensure the collection of complete & accurate KYC information of the customers before or during executing any import related international and/or local trade transaction in favor of their customers or offering any import related trade finance and trade service facility to their customers.

Branches or authorized subsidiaries or concerned Corporate Office Divisions may collect additional information about the KYC & the purpose and intended nature of the business relationship up to their satisfaction which are required to conduct appropriate due diligence considering the risk of the customer. Additional information may be related to:

- the countries with which the importer trades;
- the goods they trade;
- demand of the goods in local market;
- sale or consumption of imported goods by the importer in different time frame;
- the role & location of the parties with whom the importer does business (e.g. customers, suppliers, etc.);
- the role & location of the agents and other third parties used by the importer in relation to the business;
- business performance; and
- any other required information up to satisfaction.

10.7.1.2 Collection & Verification of Import Related Documents

Branches or authorized subsidiaries or concerned Corporate Office are required to collect the following applicable documents and verify the same using reliable, independent source, documents or data before executing any import transaction.

- a. Importers in both public sector and private sector:

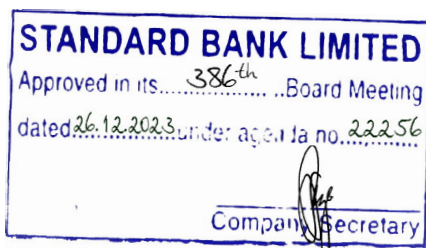


- ✓ L/C Authorization (LCA) Form for import or opening Letter of Credit;
 - ✓ Import application or L/C Application Form duly signed by the importer;
 - ✓ Indents for goods issued by Indentor or a Proforma Invoice obtained from the foreign supplier, as the case may be;
 - ✓ Insurance Cover Note;
 - ✓ IMP Forms duly signed by importer; and
 - ✓ any other documents required by the branches.
- b. For public sector importers, the following additional document is required besides the above mentioned documents:
- ✓ the attested photocopy of sanction letter from the administrative Ministry or Division or Authority, wherever applicable;
- c. For private sector importers- the following additional documents are required besides the above mentioned documents:
- ✓ Valid Membership certificate from the registered local Chamber of Commerce and Industry or any Trade Association established on all Bangladesh basis, representing any special trade/business;
 - ✓ Renewed Import Registration Certificate for the concerned financial year;
 - ✓ a declaration, in triplicate, that the importer has paid income-tax or submitted income tax return for the preceding year;
 - ✓ proof of having Tax Identification Number (TIN) in all cases of imports, excepting personal use;
 - ✓ any such document as may be required as per Public Notice, or Order issued by Chief Controller, from time to time under the Import Policy Order in force;
 - ✓ any other necessary papers or documents according to the Import Policy Order in force;
 - ✓ Insurance Cover Note from Insurance Company and duly stamped insurance policy against this cover-note, which shall have to be submitted to the Customs Authority during release of goods.

Assessment and Evaluation of KYC Information and Documents

AD branches or authorized subsidiaries or concerned Corporate Office Divisions are required to review and evaluate KYC information and documents to find out the likelihood & impact of the inherent risk, categorize the customer as low or high risk customers, apply CDD measures. Branch may require to apply EDD measures where:

- i. Importer falls into a higher risk category or where the nature of their trade as disclosed during the standard due diligence process suggests that enhanced due diligence would be prudent;



- ii. The nature of business and the anticipated transactions as described and disclosed in the initial due diligence stage may not necessarily suggest a higher risk category but if, during the course of any transaction any high risk factors become apparent, this may warrant additional due diligence;
- iii. Transaction includes third party (i.e. parties not associated with Standard Bank), middlemen or traders using back to back or transferable LCs or payments from offshore deals;
- iv. Customer/importer is a middle man or trader.

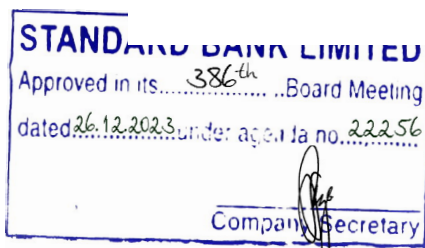
AD branches, authorized subsidiaries or concerned Corporate Office Divisions may consider the following where enhanced due diligence is required:

- i. Identifying & verifying trade cycle of the importer;
- ii. Identifying & verifying the cross border customs & licensing regulations;
- iii. Establishing physical control over the goods; and
- iv. Identifying & verifying of the payment flows.

Assessment and Evaluation of Import Documents submitted by Importer

AD branches or authorized Corporate Office Division shall review the Letter of Credit application or import requests when received from importer in the following manure:

- i. Screen the Sanctions lists (OFAC, EU, UNSC & local list) which may affect:
 - a) Supplier as a named target;
 - b) The country in which supplier is located;
 - c) The goods involved;
 - d) The country where the goods are shipped from, disclosed transshipment points and destination points;
 - e) Other names appearing in the LC or sales contract.
- ii. Check the countries which are rated as high risk for ML & FT in which:
 - a) Supplier or their bank are located;
 - b) The transportation of goods occurs through those countries;
- iii. The goods described in the transaction to check that:
 - a) The type, quantity and value of goods are consistent with what is known business of importer;
 - b) Price is internationally competitive;
 - c) There are no generally known embargoes other than those arising from sanctions (local law and UNSC sanctions)



- iv. The seller (supplier) to check through collection of credit report that:
- The type, quantity and value of goods to be imported are consistent with business of the supplier;
 - Official name, address, phone number, fax number, etc. are consistent with what are provided by the importer; Means, standing, commitment, credibility, goodwill, market reputation, operational status and length of business are acceptable to bank.
- v. Check the documents and be confirmed that the documents submitted by importer comply:
- the Bangladesh Bank Guidelines for Foreign Exchange Transactions;
 - circulars issued by Bangladesh Bank & BFIU;
 - import policy order in force;
 - Foreign Exchange Regulation Act 1947; and
 - other applicable acts, rules & regulations.
- vi. Confirm that the importer has no overdue bill of entry;
- vii. Checking for indicators of unusual aspects such as:
- Over-invoicing or under-invoicing;
 - Involve unrelated parties;
 - Involve highly unorthodox documentation;
 - Involve a complex structure obscuring the true nature of the transaction;
 - Involve other parties which as a result of any screening activity bank regards as unacceptably high risk;
 - Create an unusual trigger point for the payment to be made under the LC/sales contract (e.g. Goods are shipped without the need for relevant documentation).

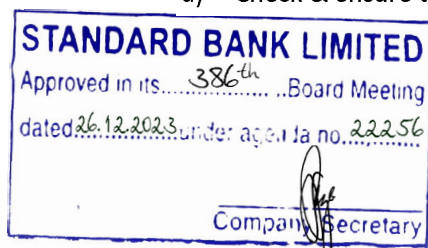
Depending on the information arising from this reviewing process:

- Make further internal enquiries as to the appropriate course of action;
- Request more information from Importer before agreeing to proceed with the transaction;
- Allow the transaction to proceed but make a record of the circumstances for review purposes where appropriate or take senior management approval;
- Decline the transaction if enquiries do not provide reasonable explanations and submit a suspicious transaction/activity report to CAMLCO Office/AML & CFT Division, Head Office.

Assessment and Evaluation of Import Documents Submitted by Supplier's Bank

AD branches or authorized Corporate Office Division shall review the documents received from importer's bank against the Letter of Credit or LCAF which takes account of the following:

- Check & ensure that documents complies all local regulatory requirements;



- b) The screening of new parties involved against current applicable lists sanction lists;
- c) The extent to which the documents presented comply with the information already checked in the LC;
- d) Check & ensure that documents presented constitute complying presentation, i.e., documents are presented as per LC terms, UCP 600;
- e) Check the known red flag indicators (discussed in appendix C) of TBML/FT.

Depending on the information arising from this reviewing process:

- a) Make further internal & external enquiries as to the appropriate course of action;
- b) Request more information from Importer as well as supplier's bank before agreeing to proceed with the document lodgment, retirement & payment;
- c) Allow the transaction to proceed but make a record of the circumstances for review purposes where appropriate or take senior management approval;
- d) Refuse & return the documents if enquiries do not provide reasonable explanations and submit a suspicious transaction/activity report to CAMLCO Office/AML & CFT Division, Head Office & update the Bangladesh Bank import monitoring system accordingly.

Assessment and Evaluation of Import Payment

AD branches or authorized Corporate Office Division in relation to make payments to importer's bank or other entities as per instruction of importer's against the Letter of Credit or LCAF which may take account of the following:

- a) Check & confirm that payment is made from importer's account;
- b) Screen the names in the payment instruction, including the names of any new banks;

Assessment and Evaluation of Custom's Certified Invoice or Bill of Entry

AD branches or authorized Corporate Office Division in relation to payments made against the Letter of Credit or LCAF which may take account of the following:

- a) Whether documentation showing a higher or lower value or cost of merchandise than that which was declared to Customs or paid by the importer (i.e. commodity over-valuation or undervaluation);
- b) Whether significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped as per Bill of Entry;
- c) If any mismatch or discrepancy is found, it is immediately required to inform the Bangladesh and submit a suspicious transaction/activity report to CAMLCO Office/AML & CFT Division, Head Office.



10.7.2 CDD Measures for Export Business

10.7.2.1 KYC Policy & Procedures

For any new export customer in Standard Bank, Branches or Authorized Subsidiaries or concerned Corporate Office Divisions are required comply customer acceptance policy.

Branches or authorized subsidiaries or concerned Head Office Divisions are required to collect or ensure the collection of complete & accurate KYC information of the export customers before or during executing any export related international and/or local trade transaction in favor of their customers or offering any export related trade finance and trade service facility to their customers.

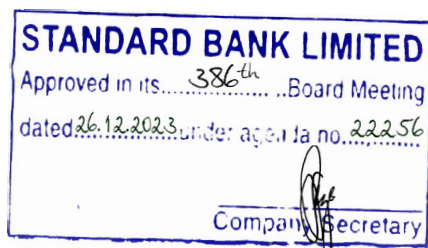
Branches or authorized subsidiaries or concerned Corporate Office Divisions may collect additional information about the KYC & the purpose and intended nature of the business relationship up to their satisfaction which are required to conduct appropriate due diligence considering the risk of the customer. Additional information may be related to:

- a) The countries with which the exporter trades/exports;
- b) The goods they trade/export/produce;
- c) Demand of the goods in local/global market;
- d) Production capacity, if applicable;
- e) Sale or consumption of imported raw-materials by the exporter;
- f) The role & location of the parties with whom the exporter does business (e.g. buyers, suppliers, etc.);
- g) The role & location of the agents and other third parties used by the foreign importer/buyer in relation to the business;
- h) The role & location of the agents and other third parties used by the exporter in relation to the business;
- i) previous export performance; and
- j) any other required information up to satisfaction of the branch or authorized subsidiary or concerned Head Office Divisions.

10.7.2.2 Collection & Verification of Export Related Documents

For identification & verification of the exporter/customer as specified in the, branches or authorized subsidiaries or concerned Corporate Office are required to collect the following applicable documents and verify the same using reliable, independent source, documents or data before executing any export transaction.

- a) Trade License;
- b) Export Registration Certificate (E.R.C);
- c) Import Registration Certificate (I.R.C), if applicable;
- d) VAT Certificate, if applicable;



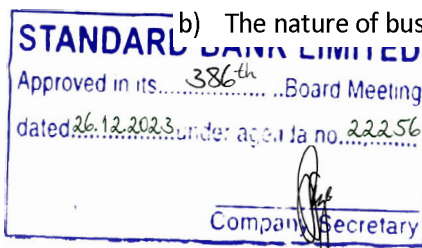
- e) TIN Certificate, if applicable;
- f) EPB Enrolment Certificate, if applicable;
- g) Environment Certificate, if applicable;
- h) Fire license, if applicable;
- i) License from labor directorate, if applicable;
- j) Factory Layout Plan Approval, if applicable;
- k) Permission from Ministry of Textile, if applicable;
- l) Registration and recommendation issued by Board of Investment, if applicable;
- m) Production capacity of the factory, if applicable;
- n) List of Machinery with commercial invoice, if applicable;
- o) Boiler Certificate, if applicable;
- p) Fire License, if applicable;
- q) Bonded Warehouse License, if applicable;
- r) Tenancy agreement copy, if applicable;
- s) Membership Certificate from recognized Chamber/Trade Association, if applicable;
- t) Membership & certification of Bangladesh Garments Manufacturers & Exporters Associate, if applicable;
- u) Memorandum and Articles of Association and Certificate of Incorporation (in case of Limited Company) , if applicable;
- v) Certificate of commencement, if applicable;
- w) Resolution of the company stating financial assistance from Bank/ Branch, if applicable;
- x) Declaration Regarding Liability with Other Bank in Party's Letter Pad, if applicable;
- y) Declaration of Assets & Liabilities of Director, if applicable;
- z) Any other required documents up to satisfaction of the AD branch or authorized subsidiary or concerned Head Office Division.

Assessment and Evaluation of KYC Information and Documents

AD branches or authorized subsidiaries or concerned Corporate Office Divisions are required to review and evaluate KYC information and documents to find out the likelihood & impact of the inherent risk, categorize the customer as low or high risk customers, apply CDD measures.

AD branches or authorized subsidiaries or concerned Corporate Office Divisions may require to apply enhanced due diligence where:

- a) Exporter falls into a higher risk category or where the nature of their trade/business as disclosed during the standard due diligence process suggests that enhanced due diligence would be prudent;
- b) The nature of business and the anticipated transactions as described and disclosed in the initial



due diligence stage may not necessarily suggest a higher risk category but if, during the course of any transaction any high risk factors become apparent, this may warrant additional due diligence;

- c) Transaction includes third parties (i.e. parties not associated with Standard Bank), middlemen or traders using back to back or transferable LCs or payments from offshore deals;
- d) Customer/exporter is a middle man or trader or agent of the buyer.

AD branches or authorized subsidiaries, if any or concerned Corporate Office Divisions may consider the following where enhanced due diligence is required:

- a) Identifying & verifying trade cycle of the exporter;
- b) Identifying & verifying the cross border customs & licensing regulations;
- c) Identifying & verifying actual procurement or production capacity of the exporter;
- d) Establishing physical control over the goods; and
- e) Identifying & verifying of the payment flows.

Assessment and Evaluation of Export LC/ Sales Contract Submitted by Exporter

AD branches or authorized Corporate Office Division should evaluate the Letter of Credit application or import requests when received from importer and do the following:

- a. Screen the Sanctions & terrorist lists (OFAC, EU, UNSC and local lists) which may affect:
 - i. Buyer as a named target;
 - ii. The country in which buyer is located;
 - iii. The goods involved;
 - iv. The country where the goods are trans-shipped and destination points;
 - v. Other names appearing in the Export LC or sales contract.
- b. Check the countries which are rated as high risk for ML & FT in which:
 - i. buyer or notify party or consignee or their bank is located;
 - ii. The transportation of goods occurs through those countries.
- c. The goods described in the transaction to check that:
 - i. The type, quantity and value of goods is consistent with what is known business of exporter & his/her production capacity;
 - ii. Price is competitive;
 - iii. There are no generally known embargoes other than those arising from sanctions (local law and UNSC sanctions).
- d. The buyer (importer) to check through collection of credit report that:
 - i. On the face of it they are the kind of counterparty which is consistent with what is known of the



business of exporter.

- e. Check the documents and be confirmed that the documents submitted by importer comply:
- the Bangladesh Bank Guidelines for Foreign Exchange Transactions;
 - circulars issued by Bangladesh Bank & BFIU;
 - export policy in force;
 - Foreign Exchange Regulation Act 1947; and
 - other applicable acts, rules & regulations.
- f. Check and confirm that the importer has no overdue export bills or EXP Forms;
- g. Export L/C Workability with Exporter's Bank:
- export L/C is available at the counter of the exporter's bank;
 - beneficiary can present documents under the export L/C, and
 - it does not depend on any other factors.
- h. Checking Export LC terms for indicators of unusual aspects such as:
- Involve unrelated parties;
 - Involve highly unorthodox documentation;
 - Involve a complex structure obscuring the true nature of the transaction;
 - Involve other parties which as a result of any screening activity bank regards as unacceptably high risk;
 - Create an unusual trigger point for the payment to be made under the L/C sales contract (e.g. Goods are shipped without the need for presentation of documents).

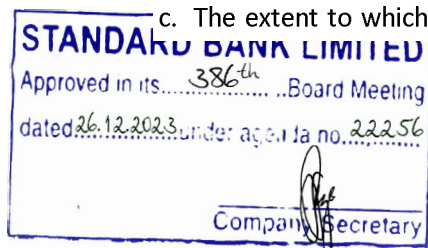
Depending on the information arising from this reviewing process:

- Make further internal enquiries as to the appropriate course of action;
- Request more information from Importer before agreeing to proceed with the transaction;
- Allow the transaction to proceed but make a record of the circumstances for review purposes where appropriate or take senior management approval;
- Decline the transaction if enquiries do not provide reasonable explanations and submit a suspicious transaction/activity report to CAMLCO Office/AML & CFT Division, Head Office.

Assessment and Evaluation of Export Documents Submitted by Exporter

AD branches or authorized Head Office Division should review the documents received from exporter against the Export Letter of Credit or Sales Contract and do the following:

- Check & ensure that documents complies all local regulatory requirements;
- The screening of new parties, is any, involved against current applicable lists sanction lists;
- The extent to which the documents presented comply with the information already checked in



the LC;

- d. Check & ensure that documents presented constitute complying presentation, i.e., documents are presented as per Export LC terms, UCP 600
- e. Check the known red flag indicators of TBML/FT

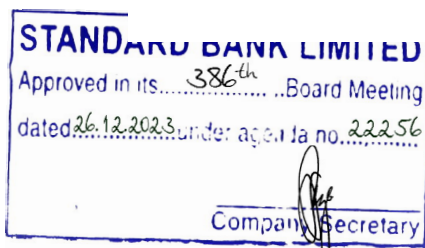
Depending on the information arising from this reviewing process:

- i. Make further internal & external enquiries as to the appropriate course of action;
- ii. Request more information from exporter before agreeing to proceed with the document lodgment & providing any post shipment finance;
- iii. Allow the transaction to proceed but make a record of the circumstances for review purposes where appropriate or take senior management approval;
- iv. Refuse & return the documents and arrange to return the goods if enquiries do not provide reasonable explanations and submit a suspicious transaction/activity report to CAMLCO Office/AML & CFT Division, Head Office & update the Bangladesh Bank export monitoring system accordingly.

Assessment and Evaluation of Export Payment

AD branches or authorized Corporate Office Division should make payments to exporter or other entities as per instruction of exporter and do the following:

- i. Check & confirm that full EXP value repatriated;
- ii. Check & confirm that payment is made to exporter's account;
- iii. Screen the name of the person or entity and conduct appropriate CDD when export payment is made to other than exporter.



CHAPTER XI: INVESTMENT BACKED or BASED MONEY LAUNDERING

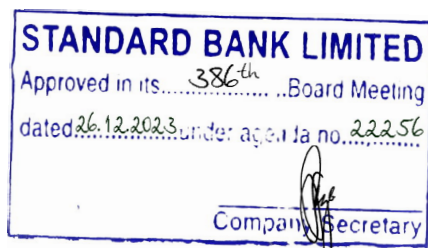
11.0 Definition & Process: Credit/Investment backed method of money laundering involves cleaning of money obtained from criminal activities such as insider trading, extortion, illegal gambling, and drug trafficking to appear to have been derived from legal activities in order for financial institutions to deal with it without any suspicion. Money can be laundered using various methods which vary in terms of sophistication and complexity. Investments and mortgages are usually taken as a cover to launder money proceedings, and lump sum cash repayments are used to repay the investments or mortgages.

In the “investment backed” money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a “investment or mortgage” back to the money laundering for the same amount with all the necessary “investment 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 investment by the money launderer.

Most often, the money launderer establishes an apparent legal origin of money through fabrication of transactions like agreements, bookkeeping, and invoices, deeds, reports, and spoken/written statements. The common methods used to justify money laundering is fabricating a investment/credit, also referred to as back-to-back or investment/credit - back. The most popular investment/credit -back form of laundering money is when criminals borrow their own criminal money. This is usually done through the creation of a investment/credit agreement between the criminal and a third party. Most used third parties are offshore corporations who are controlled by the criminals. Although back-to-back investment/credit are the common ways that money can be washed.

11.1 Money laundering through Real Estate Sector:

The real-estate sector may be one of the many vehicles used by criminal organizations to launder their illicitly obtained money. The emerging markets seem to be more vulnerable to misuse of the real estate sector. Due to the worldwide market growth of real estate-backed securities and the development of property investment funds, the range of options for real estate investments has also grown. This effect has not gone without notice in emerging markets. Money laundering transactions can be easily camouflaged in genuine commercial transactions among the huge number of real estate transactions taking place. Complicating matter is the fact that often these less developed economies do not have an average market price for real estate, but rather prices varying across



sectors and districts. To complete real estate transactions in some stage of the process involvement of legal expert is inevitable.

The real estate sector merits closer consideration given the large scope of monetary transactions, its significant social impact, and because of the number of cases in which money laundering, and in limited circumstances terrorist financing and tax fraud schemes, have been detected. Abuse in this sector also has the undesirable effect of political, institutional and economic destabilization. Moreover, due to the international nature of the real-estate market, it is often extremely difficult to identify real estate transactions associated with money laundering or terrorist financing.

In order to misuse the real-estate sector, a number of methods, techniques, mechanisms, and instruments are available. Many of these methods are in and of themselves illegal acts; however, certain of them might be considered perfectly legal if they were not associated with a money laundering or terrorist financing scheme.

A series of the more common or basic methods is used which are mentioned as under:

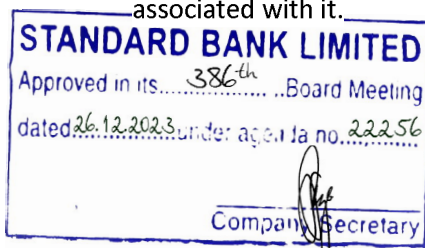
- a) Use of complex investments or credit finance.
- b) Use of non-financial professionals.
- c) Use of corporate vehicles.
- d) Manipulation of the appraisal or valuation of a property.
- e) Use of monetary instruments.
- f) Use of mortgage schemes.
- g) Use of investment schemes and financial institutions.
- h) Use of properties to conceal money generated by illegal activities.

11.1.1 Complex Investments and Credit Finance:

Intercompany investments have become a frequent instrument used as a means for raising funds. The ease with which such investments can be arranged makes them popular with the general public. These investments are also used in the real estate sector. Where an instrument is frequently used, misuse of the instrument becomes a possibility as well. Depending on the way in which the investment is structured, two different schemes have been detected.

11.1.2 Investment-Back Schemes:

Intelligence and law enforcement reports indicate "investment-back" transactions are used by suspected criminals to buy properties – either directly or indirectly – through the purchase of shares in property investment funds. Essentially, suspected criminals lend themselves money, creating the appearance that the funds are legitimate and thus are derived from a real business activity. The purpose of the investment is to give the source of the money an appearance of legitimacy and to hide the true identity of the parties in the transaction or the real nature of the financial transactions associated with it.



11.1.2.1 Indicators and methods identified in the scheme:

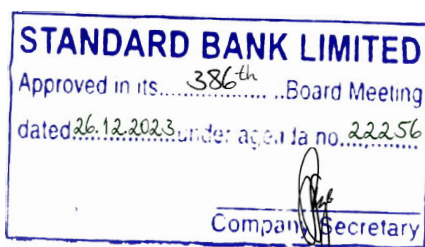
- a) The source of the funds used to finance the real estate transaction was from abroad, in particular from offshore jurisdictions and jurisdictions with strict bank secrecy.
- b) The lender of the money, an offshore company, had no direct relation with the borrower of the money.
- c) A financial institution was not involved in the investment structure.
- d) There was no investment agreement between the lender and borrower.
- e) The investment agreement was legally invalid.
- f) The information in the investment agreement was inconsistent or incorrect.
- g) The conditions in the investment agreement were unusual (for example, no collateral was required).
- h) No payment of profit /income or repayment of the principal.
- i) Transaction monitoring by financial institutions showed payable-through accounts, by which incoming payments from abroad were immediately transferred abroad without a logical reason.

11.1.3 Back-to-Back Investment Schemes:

As with investment-back schemes, back-to-back investments are also known to be used in real-estate related money laundering schemes. In this case, a financial institution lends money based on the existence of collateral posted by the borrower in the usual way. However, the collateral presented to the financial institution originates from criminal or terrorist activities. Although financial institutions are obligated to disclose the existence of these funds on a risk dossier, there are occasions where this analysis may contain shortcomings. Instances where the collateral posted is not specified in the investment agreement or unreliable information as to the nature, location and value of the collateral make it very difficult to recognize a back-to-back investment.

11.1.3.1 Indicators and methods identified in the scheme:

- a) No reference in the investment agreement to the underlying collateral.
- b) The collateral provided was not sufficient.
- c) The collateral provider and other parties involved in the investment structure were not known.
- d) The borrower of the money was not willing to provide information on the identity and background of the collateral provider and/or the other parties involved in the investment structure.
- e) The complex nature of the investment scheme could not be justified.
- f) There was an unexpected investment default.



11.1.4 The Role of Non-Financial Professionals:

In recent years, money launderers are increasingly forced to develop elaborate schemes to work around AML & CFT controls. This has often meant seeking out the experience of professionals such as lawyers, tax advisors, accountants, financial advisors, notaries and registrars in order to create the structures needed to move illicit funds unnoticed. These professionals act as gatekeepers by providing access to the international financial system, and knowingly or not, can also facilitate concealment of the true origin of funds.

11.1.4.1 Obtaining Access to Financial Institutions through Gatekeepers:

Criminals and terrorists have used non-financial professionals or gatekeepers to access financial institutions. This is especially important during the process of determining eligibility for a mortgage, opening bank accounts, and contracting other financial products, to give the deal greater credibility. It has also been documented that bank accounts are opened in the name of non-financial professionals in order to carry out various financial transactions on their behalf. Examples include depositing cash, issuing and cashing cheques, sending and receiving international fund transfers, etc., directly through traditional saving accounts or indirectly through correspondent accounts.

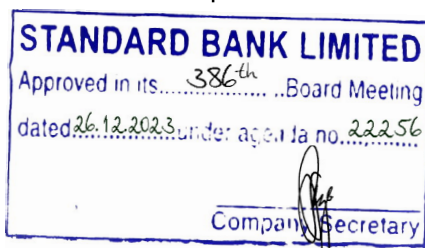
11.1.4.2 Indicators and methods identified in the scheme:

- a) **Instrument:** real estate, investment.
- b) **Mechanisms:** bank, trust, real-estate agent.
- c) **Techniques:** offshore customer, non-account holder customer, physical person intermediary, high risk jurisdiction, investment, purchase of real estate.
- d) **Opportunity taken:** using a trust and appealing to a non-financial profession was clearly done to disguise the identity of the beneficial owner.

11.1.5 Assistance in the Purchase or Sale of Property:

Non-financial professionals such as notaries, registrars, real-estate agents, etc., are sometimes used by suspected criminals on account of their central role in carrying out real-estate transactions. Their professional roles often involve them in a range of tasks that place them in an ideal position to detect signs of money laundering or terrorist financing.

The role of non-financial professionals in detecting illegal activity can also be significant in this area. There have been examples of notaries and registrars detecting irregularities in the signing of the property transfer documents (for example, using different names or insisting on paying a substantial part of the cost of the transaction in cash). Other examples include buying land designated as residential through a legal person and then reclassifying it a short time later for commercial development. Professionals working with the real-estate sector are therefore in a position to be key



players in the detection of schemes that use the sector to conceal the true source, ownership, location or control of funds generated illegally, as well as the companies involved in such transactions.

11.1.5 .1 Indicators and methods:

- a) Instruments:** check, wire transfers, real estate.
- b) Mechanisms:** notary, bank.
- c) Techniques:** business account, front company customer, purchase of real estate, cross border transaction, incoming wire transfer, reverse/flip real estate, unknown source.
- d) Opportunity taken:** use of a notary when buying a real estate. Since the company's bank account was not used for any other transaction, it can be deduced that this company was a front company set up for the mere purpose of carrying out the property transaction.

11.1.6 Trust Accounts:

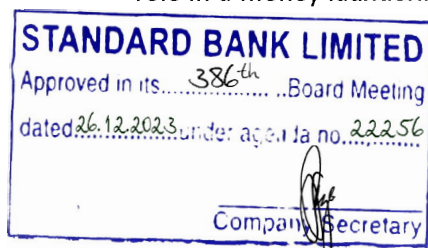
A trust account is a separate bank account, which a third party holds on behalf of the two parties involved in a transaction. Funds are held by the trustee until appropriate instructions are received or until certain obligations have been fulfilled. A trust account can be used during the sale of a house, for example. If there are any conditions related to the sale, such as an inspection, the buyer and seller may agree to use a trust account. In this case, the buyer would deposit the amount due in a trust account managed by, or in the custody of, a third party. This guarantees the seller that the buyer is able to make the payment. Once all the conditions for the sale have been met, the trustee transfers the money to the seller and the title to the property is passed to the buyer.

11.1.6 .1 Indicators and methods:

- a) Instruments:** cash deposits, real estate.
- b) Mechanisms:** solicitor, trust accounts.
- c) Techniques:** structured cash transactions, establishment of trust accounts to purchase properties and pay off mortgages, purchase of property in the names of the main target.
- d) Opportunity taken:** the solicitor set up trust accounts on behalf of the target and organized for transactions to purchase the property, pay off mortgages, and shares were purchased to avoid detection. In some cases properties were purchased in the names of relatives of the target.

11.1.7 Management or Administration of Companies:

There have been documented cases of non-financial professionals approached by money launderers and terrorists not just to create legal structures, but also to manage or administer these companies. In this context, these professionals may have been generally aware that they are taking an active role in a money laundering operation. Their access to the companies' financial data and their direct



A handwritten signature in blue ink.



A handwritten signature in blue ink.

role in performing financial transactions on behalf of their clients make it almost impossible to accept that they were not aware of their involvement.

11.1.7.1 Indicators and methods:

- a) **Instruments:** cheque, cash, wire transfers, real estate.
- b) **Mechanisms:** notary, bank.
- c) **Techniques:** intermediary account, purchase of real estate, incoming wire transfer.
- d) **Opportunity taken:** by using the company and the notary's client account money was laundered by investing in real estate and the links between the individual and the company were concealed in order to avoid suspicions.

11.1.8 Corporate Vehicles:

Corporate vehicles – that is, legal persons of all types and various legal arrangements (trusts, for example) – have often been found to be misused in order to hide the ownership, purpose, activities and financing related to criminal activity. Indeed that practice is so common that it almost appears to be ubiquitous in money laundering cases. The misuse of these entities seem to be most acute in tax havens, free-trade areas and jurisdictions with a strong reputation for banking secrecy; however, it may occur wherever the opacity of corporate vehicles can be exploited.

Apart from obscuring the identities of the beneficial owners of an asset or the origin and destination of funds, these corporate vehicles are also sometimes used in criminal schemes as a source of legal income. In addition to shell companies, there are other specialized companies that carry out perfectly legitimate business relating to real estate, which have sometimes been misused for money laundering purposes. This aspect is illustrated by the use, for example, of property management or construction companies. The use of corporate vehicles is further facilitated if the company is entirely controlled or owned by criminals.

11.1.9 Offshore Companies:

Legal persons formed and incorporated in one jurisdictions, but actually used by persons in another jurisdiction without control or administration of a natural or legal resident person and not subject to supervision, can be easily misused in money laundering transactions. The possibilities for identifying the beneficial owner or the origin and destination of the money are at times limited. In these scenarios actors with wrongful intentions have the distinct advantage of extra protection in the form of bank secrecy.

11.1.9.1 Indicators and methods:

- a) **Instrument:** cash, wire transfers, real estate.
- b) **Mechanisms:** notary, bank.



- c) **Techniques:** personal account, purchase of real estate, incoming wire transfer, dormant account, offshore transactions.
- d) **Opportunity taken:** use of an offshore company to buy real estate. It appeared that the party involved had connections with a company in insolvency and acted in this way to be able to buy the property with a view to getting away from his creditors.

11.1.10 Legal Arrangements:

The use of some legal arrangements such as trusts can play an important role in money laundering. Under certain conditions these legal arrangements can conceal the identity of the true beneficiary in addition to the source and/or destination of the money.

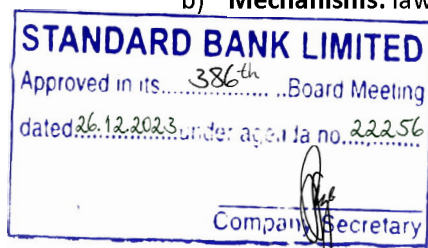
The nature and/or structure of certain trusts can result in a lack of transparency and so allow them to be misused:

- a) Certain trusts may exist without the need for a written document constituting them.
- b) Although there may be a deed defining the trust, in some cases it does not need to identify the depositary and/or a specific beneficiary.
- c) There may be no obligation to register decisions regarding the management of a trust, and it may not be possible to disclose them in writing to anyone.
- d) In some types of trust, such as discretionary trusts, the beneficiary may be named or changed at any time, which makes it possible to safeguard the identity of the beneficiary at all times up until the moment the ownership of the assets is transferred.
- e) Trusts set up to protect assets may protect the depositary against decisions to freeze, seize or attach those assets.
- f) Trusts may be set up to manage a company's shares, and they may make it more difficult to determine the identities of the true beneficiaries of the assets managed by the trusts.
- g) Certain legislation may expressly prohibit the freezing, seizure or attachment of assets held in trust.
- h) Certain clauses commonly referred to as escape clauses, allow the law to which the trust is subject to be changed automatically if certain events arise. Such clauses make it possible to protect the assets deposited in the trust from legal action.

These conditions may create a significant obstacle for the authorities charged with applying anti-money laundering and counter terrorist financing laws – especially in relation to international cooperation – thus significantly slowing the process of collecting information and evidence regarding the very existence of the trust and identifying its ultimate beneficiary. Under these circumstances it may be very difficult, if not impossible, for a bank or other financial institution to comply with the “Customer Acceptance Policies” or KYC policies applicable in the country or territory in which it is located.

11.1.10.1 Indicators and methods:

- a) **Instruments:** wire transfers, real estate.
- b) **Mechanisms:** lawyer, trust, bank.



- c) **Techniques:** trust account, purchase of real estate, legal entity transactor, offshore, and incoming wire transfer.
- d) **Opportunity taken:** use of trusts to buy real estate. The trusts were used to conceal the identity of the true owners.

11.1.11 Shell Companies:

A shell company is a company that is formed but which has no significant assets or operations, or it is a legal person that has no activity or operations in the jurisdiction where it is registered. Shell companies may be set up in many jurisdictions, including in certain offshore financial centres and tax havens. In addition, their ownership structures may occur in a variety of forms. Shares may be held by a natural person or legal entity, and they may be in nominative or bearer form. Some shell companies may be set up for a single purpose or hold just one asset. Others may be set up for a variety of purposes or manage multiple assets, which facilitates the co-mingling of legal and illicit assets.

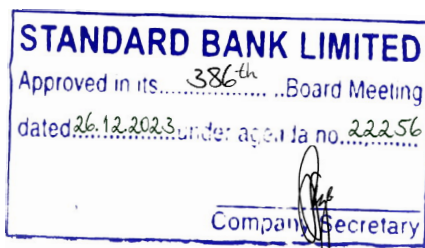
The potential for anonymity is a critical factor in the use of shell companies. They may be used to hide the identity of the natural persons who are the true owners or who control the company. In particular, permissive practices regarding the form of the shares, whether corporate, nominative or bearer, together with the lack of co-operation on the collection of information, represent a significant challenge when seeking to determine the ultimate beneficial owner.

11.1.12 Property Management Companies:

When using the real-estate sector, the purchase or construction of properties is a commonly used means by which criminals carry out financial transactions. However, a property that is bought or constructed using illegally obtained funds may subsequently be rented out to provide an apparently legal source of income in order to camouflage movements of funds between various jurisdictions (for example, the tenant and the landlord are located in different jurisdictions).

11.1.12.1 Indicators and methods:

- a) Instruments: cash, wire transfers, real estate.
- b) Mechanisms: notary, bank.
- c) Techniques: business account, purchase of real estate, transactor inconsistencies, non-resident customer, unknown source.
- d) Opportunity taken: the establishment of a company managed by a family member with the aim of letting real estate paid by a foreign company disguised the link between the origin and the destination of the money.



11.1.13 Non-trading real estate investment companies:

Several characteristics of these companies make them especially vulnerable to abuse by suspected criminals. First, it is often very difficult to identify the real owner or controller. Second, the company can be created very easily with no minimum initial capital and without an authentic deed. Additionally, these entities are only recorded at the trade register. Finally, the shares of such companies can be sold without certification so that the true owner is not easily identified.

11.1.13.1 Indicators and methods:

- a) **Instrument:** real estate, single payment.
- b) **Mechanisms:** bank, SCI (An SCI is a rather specialist type of French company that is constituted for the ownership and management of real estate).
- c) **Techniques:** purchase of real estate and foreign/offshore companies as intermediary, high value, physical intermediaries linked to the beneficial owner.
- d) **Opportunity taken:** the FIU analysis revealed that the managers of the SCI were linked to the beneficial owner through a company owned by him and in which the two managers had senior responsibilities.

11.1.14 Manipulation of the Appraisal or Valuation of a Property:

Manipulation of the real value of properties in relation to real estate involves the overvaluing or undervaluing of a property followed by a succession of sales and purchases. A property's value may be difficult to estimate, especially in the case of properties that might be considered atypical, such as hotel complexes, golf courses, convention centres, shopping centres and holiday homes. This difficulty further facilitates the manipulation when such property is involved.

11.1.14.1 Over-valuation or Under-valuation:

This technique consists of buying or selling a property at a price above or below its market value. This process should raise suspicions, as should the successive sale or purchase of properties with unusual profit margins and purchases by apparently related participants.

An often-used structure is, for example, the setting up of shell companies to buy real estate. Shortly after acquiring the properties, the companies are voluntarily wound up, and the criminals then repurchase the property at a price considerably above the original purchase price. This enables them to insert a sum of money into the financial system equal to the original purchase price plus the capital gain, thereby allowing them to conceal the origin of their funds.



11.1.15 Mortgage Schemes/Murabaha or Bai Muazzel Schemes:

Mortgage investments comprise one of the main assets on the balance sheets of banks and other financial institutions. An inherent risk in this activity arises from the fraudulent or criminal use of these products. Through this misuse of the mortgage lending system, criminals or terrorists mislead the financial institution into granting them a new mortgage or increasing the amount already lent. This use constitutes, in the majority of the cases analyzed, a part of the financial construction established to carry out criminal activities.

It was observed in many instances that financial institutions consider these mortgage products to be low risk. A risk-based approach to monitoring subjects related to money laundering and terrorist financing, similar to those based on customer due diligence or "know your customer" principles, could mitigate some of the risk of this activity.

11.1.16 Illegal Funds in Mortgage Investments and Interest/profit/ Payments:

Illicit actors obtain mortgage investments to buy properties. In many cases, illegal funds obtained subsequently are used to pay the profit /income or repay the principal on the investment, either as a lump sum or in instalments. The tax implications of using these products should also not be overlooked (for example, eligibility for tax rebates, etc.).

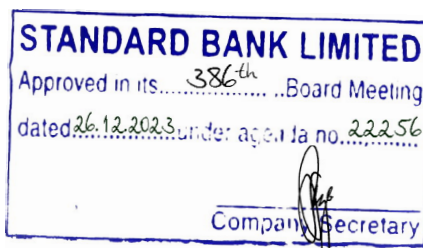
Front men are also sometimes used to buy properties or to apply for mortgages. The analyzed cases seem to indicate that this misuse of mortgages goes hand in hand with a simulated business activity and the related income so as to deceive the bank or other financial institution when applying for the mortgage. On occasion the property is apparently purchased as a home, when in reality it is being used for criminal or terrorist activities (for example, selling or storing drugs, hiding illegal immigrants, people trafficking, providing a safe house for members of the organization, etc.).

Method:

- a) Under-valuation of Real Estate
- b) Over-valuation of Real Estate

11.1.17 Investment Schemes and Financial Institutions:

Direct or indirect investment in the real estate sector by banks and other financial institutions is significant. However, the volume of investment by insurance companies and pension fund managers is also significant, as these institutions place a large part of their long-term liabilities in the property sector at both national and international levels. Bank and other financial institution investment policies demonstrate that investment in property is gaining ground relative to other direct investments.



11.1.18 Concealing Money Generated by Illegal Activities:

The use of real estate to launder money seems to afford criminal organizations a triple advantage, as it allows them to introduce illegal funds into the system, while earning additional profits and even obtaining tax advantages (such as rebates, subsidies, etc.).

Some areas within the real-estate sector are more attractive than others for money laundering purposes, since the financial flows associated with them are considerable. This makes the task of hiding the funds of illegal origin in the total volume of transactions easier. The real estate sector offers numerous possibilities for money laundering: hotel businesses, construction firms, development of public or tourist infrastructure (especially luxury resorts), catering businesses. It is worth highlighting that over the course of the study, trends in these activities were noticed that depend on different regional characteristics: for example, more cases occur in coastal areas, in areas with a pleasant climate, and where non-resident foreign nationals are concentrated, etc. It is also worth noting that countries which have regions of this kind are more aware of the problem and have increasingly begun to establish appropriate measures and controls in the real-estate sector.

11.1.19 Investment in Hotel Complexes, Restaurants and Similar Developments:

Real estate is commonly acquired in what is known as the integration or final phase of money laundering. Buying property offers criminals an opportunity to make an investment while giving it the appearance of financial stability. Buying a hotel, a restaurant or other similar investment offers further advantages, as it brings with it a business activity in which there is extensive use of cash.

11.1.19.1 Indicators and methods:

- a) Instruments:** investment, wire transfer, cash, real estate.
- b) Mechanisms:** bank.
- c) Techniques:** personal account, purchase of real estate, physical person intermediary, cash deposit, withdrawal, outgoing wire transfer
- d) Opportunity taken:** repayment of the mortgage by transfers from an account opened with another bank in name of his spouse.

11.1.20 Personal Investment/Car Investment/Home Investment:

Any person can take personal investment 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 investment or car investment, 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.



11.1.21 SME/Women Entrepreneur Investment:

Small, medium and women entrepreneurs can take investment 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 investment. This way they can bring the illegal money in the financial system.

11.1.22 Money laundering through Credit Cards:

Criminals and terrorist groups are finding new and complex methods to conceal the illegal profits they earn via an online environment. Now a days, an extensive range of payment systems has become available such as PayPal, Google Pay, Amazon Pay, Apple pay etc. This, along with the progressively increasing amounts of e-commerce activities happening online, causes difficulties when it comes to detecting fraudulent financial transactions and money laundering through credit cards, payment service providers and banks.

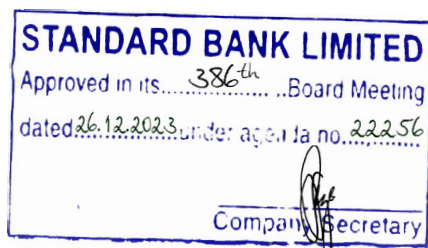
As a prominent payment method, credit cards have been used as a vehicle to conduct money laundering. Therefore, detection and prevention of transaction laundering or credit card money laundering is a pressing concern for financial services. They need to develop rigorous anti money laundering (AML) policies to act on credit card money laundering red flags and mitigate credit card money laundering risk.

a) Transaction Laundering through credit cards:

Transaction laundering or electronic money laundering is an extension of money laundering .It is a streamlined form of money laundering used to secretly processed credit card or other digital payment forms. Transaction Laundering happens when one approved merchant/vendor uses payment credentials to process payments for another undisclosed store often selling illegal products and services.

Structured credit card money laundering schemes help illegal merchandise sellers hide their transactions by entering sales receipts into payment system and washing the dirty money. While these illegal sellers can be a bricks and mortar store, they are primarily set up as web stores in modern days. The largest amount of credit card money laundering is committed by those who sell counterfeit merchandise, drugs, sex services and online casino operators and who operate without a license. Even when the goods and services are sold legally, representing the nature of credit card payment falsely violates the processing merchant's agreement with its acquiring bank. By benefitting from a scheme such as this, the criminals are violating number of state, FIU and AML laws, depending on the nature of the transactions.

b) Forms of Credit card Money Laundering: Transaction laundering or credit card money laundering can take three different forms:



Shell companies use legal businesses as a front for criminal activities. For example as a supplement seller who launders illicit funds by selling drugs which is achieved by inflating the receipts. Another example is someone who sells counterfeit medicines under the vitamin and supplements “Merchant category Code.” Shell companies may usually operate online or out of a physical storefront.

The pass through companies make it easy for illegal business to process their credit card receipts, specifically by allowing them access to the legal companies payments processing account. This is often done by inserting link for payment on the illegal company’s website. Following this, they manually enter illegal sales into their payment systems in order to make them harder to detect.

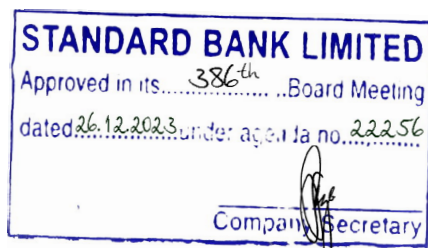
Funnel accounts are similar to pass through companies. Indeed they are legal businesses that accept credit card charges from multiple companies. These companies do not have their own merchant payment account, as they engage in either illicit transactions or are too small. Following this the funnel companies then enter through these payments as legal transactions into card into payment processing system.

C) Credit Card Money Laundering schemes: Credit card money laundering or transaction laundering is also known as “factoring” and un-authorization aggregation. This takes place when one business (often a website) processes payment for another website. This allows the sellers for illicit products (goods & services) to hide their transactions and wash their illegal money by illicitly entering their sales receipt into official and legal payment system. For example, a fashion e-commerce website can help process payment made from illegal drug networks.

In order to target the system, supporting drug businesses, the U.S. Food and drug administration (FDA) set out a series of investigations that were focused on credit card processors involved in the credit card money laundering or transaction laundering arrangements. This operation was a notable example to show the payment industry why transaction laundering monitoring is so important. It also witnessed how law enforcement agencies perceive the role of credit card processors in the network of illegal business.

d) Integrating illegal money into the economy with credit cards: Money Launderers can also use credit cards to integrate illegal money into the financial system. They do this by maintaining an offshore account in another jurisdiction through which payments are made. The criminals limit the financial trail that may lead back to their own country, where they reside. Authorities have now become more aware of this use of offshore credit cards as a credit card money laundering technique. Because of this, certain offshore jurisdictions have now enabled regulators to obtain records from banks of transactions made by their clients who have credit cards.

With the increasing growth of e- commerce and the anonymity offered by the web, money laundering risk with credit cards is surging globally. Keeping this in mind, regulators and credit card



A handwritten signature in blue ink.



A handwritten signature in blue ink.

networks have launched a campaign to deflect the efforts, specifically by holding acquirers and payment processors accountable for their merchant' actions.

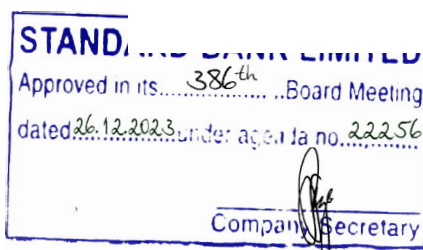
Red Flag Indicators:

The following red flags to be considered when a merchant service provider's licensee acquires vendors/merchants for credit card transactions:

- The principles of the merchant appear to be unfamiliar with, or lack a clear understanding of, the merchant's business.
- The proposed transaction volume and/or refunds are inconsistent compared to the information obtained from on- site visits or merchant peer groups.
- Unusual or excessive cash advances or credit refunds.
- There are indicators showing that a merchant's credit card is being used by any third party.

11.2 The role of current technology in detecting money laundering techniques:

The countries that are suffering the most due to money laundering have complex financial systems, ineffective AML & CFT compliance programs or operations which leads them to become vulnerable to various criminal activities. Current AML programs powered by legacy rule- based systems are proving to be costly to manage and ineffective as criminals constantly improve on their laundering strategies. Modern Regtech solutions powered by artificial intelligence, machine learning and big data analytics can effectively detect layering techniques such as the use of money mules and offshore shell companies.



CHAPTER XII: RECORD KEEPING

12.1 Record Keeping Requirement:

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.

12.2 Legal Obligations:

Under the obligation of MLPA, 2012, "The reporting organizations shall have to preserve previous records of transactions of any close account for at least 5(five) years from the date of such closure and provide with the information maintained under the clause to BFIU, Bangladesh Bank."

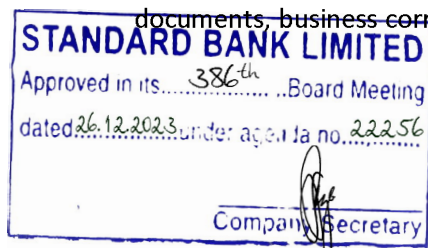
Under the obligation of MLP Rules, 2019, the bank shall maintain all necessary records of all transactions, both domestic and international, for at least five years from the date of the closure of the account or at least five years from the date of the completion of any one-off transaction in following manners:

- 1) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity;
- 2) The bank shall keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction;
- 3) The bank shall ensure that all CDD information and transaction records are available swiftly to BFIU or available to the respective investigation authority upon appropriate court order.

12.3 Obligations under Circulars:

Under the obligations of BFIU Circular No. 26 dated June 16, 2020 –

- (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.
- (2) All information and documents collected during CDD procedure along with KYC, account related documents, business correspondence and any report prepared on a customer has to be preserved



for at least 5(five) years after closing the account.

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

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

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

12.4 Records to be kept

The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a bank meets its obligations and that, in so far as is practicable, in any subsequent investigation the bank can provide the authorities with its section of the audit trail.

The records shall cover:

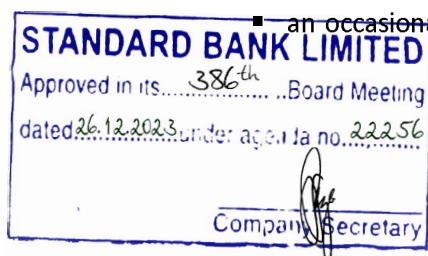
- customer information
- transactions
- internal and external suspicion reports
- report from CCC/CAMLCO
- training and compliance monitoring
- information about the effectiveness of training

12 .5 Customer Information

In relation to the evidence of a customer's identity, branch must keep a copy of or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where a branch has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. A branch may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date when the relationship with the customer ends is the date:

an occasional transaction, or the last in a series of linked transactions, is carried out;



or

- the business relationship ended, i.e. the closing of the account or accounts.

12.6 Transactions

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the branch's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer. Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

12.7 Internal and External Reports

A branch should make and retain:

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

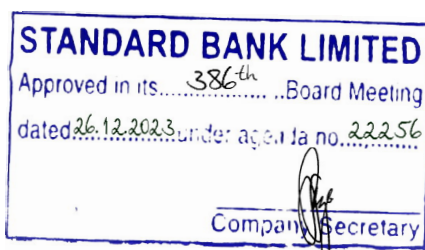
In addition, copies of any STRs made to the BFIU should be retained for five years. Records of all internal and external reports should be retained for five years from the date the report was made.

12.8 Other Measures

Bank's records should include:

- (a) in relation to training:
 - dates AML training was given;
 - the nature of the training;
 - the names of the staff who received training; and
 - the results of the tests undertaken by staff, where appropriate.
- (b) in relation to compliance monitoring
 - reports to senior management; and
 - records of consideration of those reports and of any action taken as a consequence.

12.9 Formats and Retrieval of Records



To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of a 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 reproduced and recollected without undue delay.

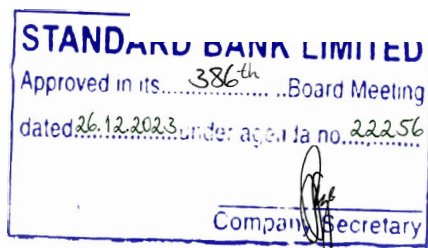
It is not always necessary to retain documents in their original hard copy form, provided that the bank has reliable procedures for keeping records in electronic form, as appropriate, and that these can be reproduced without undue delay.

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.

12.10 Training Records

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

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



CHAPTER XIII: REPORTING TO BFIU

13.1 Legal Obligations

Under the obligations of MLPA, 2012 (amendment 2015), *“The reporting organizations shall have to report any suspicious transaction (defined in Section 2(Z) of MLPA, 2012(amendment 2015) and Section 2(16) of ATA, 2009(amendment 2013)) to the BFIU immediately on its own accord”*

Under the obligations of MLP Rules 2019, *“Every bank is obliged to send various reports (suspicious transaction, suspicious activity, cash transaction, self-assessment, independent testing procedure etc.) to BFIU without any delay or in due time. Besides they have to produce any document that is sought by BFIU.”*

13.2 Suspicious Transaction Reporting

Money Laundering Prevention Act, 2012 (amendment 2015) defines suspicious transaction as follows-

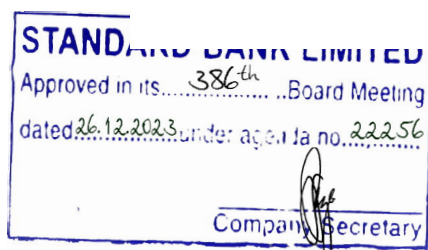
‘Suspicious Transaction’ means such transactions –

- that deviates from usual transactions;
- with regards to any transaction, there is ground to suspect that,
 - the property is the proceeds of an offence,
 - it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- Any transaction or attempted transaction that are delineated in the instructions issued by Bangladesh bank from time to time for the purpose of this act.

Anti Terrorism Act, 2009 (Amendment 2013) defines suspicious transaction as follows-

‘Suspicious Transaction’ means such transactions –

- which is different from usual transactions;
- which invokes presumption that,
 - it is the proceeds of an offence under this Act,
 - it relates to financing of terrorist activities or a terrorist person or entity;
- which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this Act.



The final output of an AML & CFT compliance program 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 AML & CFT risk for branch. Therefore it is necessary for the safety and soundness of the branch.

Generally, STR/SAR means a formatted report of suspicious transactions/activities where there is reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activities or the transactions are not seems to be usual manner. Such report is to be identified by the branch and send to CAMLCO Office/CCC/ AML & CFT Division for onward submission to the competent authorities i.e. to BFIU. Suspicion basically involves a personal and subjective assessment. The branch has to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

13.3 Identified of STR/SAR

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:

- a) Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation;
- b) By monitoring customer transactions;
- c) By using red flag indicators (**Annexure B**).

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

All suspicions reported to the CAMLCO Office/CCC/ AML & CFT Division should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rises to the suspicion. All internal enquiries made in relation to the report should also 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 or disproved.



The following chart shows the graphical presentation of identification of STR/SAR-

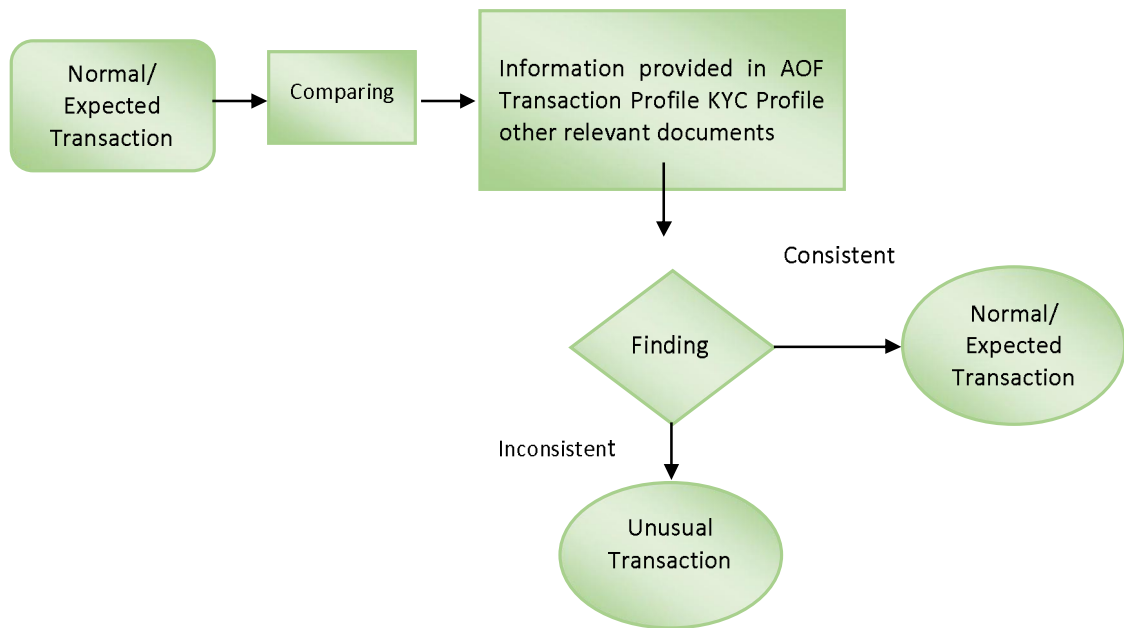


Figure: Identification of STR/SAR

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

a) Identification

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

b) Evaluation

These problems must be in place at Branch level and Central Compliance Committee (CCC)/CAMLCO Office/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 CCC/CAMLCO's Office/AML & CFT Division. After receiving report from Branch, CCC/CAMLCO Office/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/branch should keep records with proper manner.

c) Disclosure

This is the final stage and CCC/CAMLCO's Office/AML & CFT Division should submit STR/SAR to BFIU if it is still suspicious. For simplification the flow chart is given in following page shows STR/SAR identification and reporting procedures:

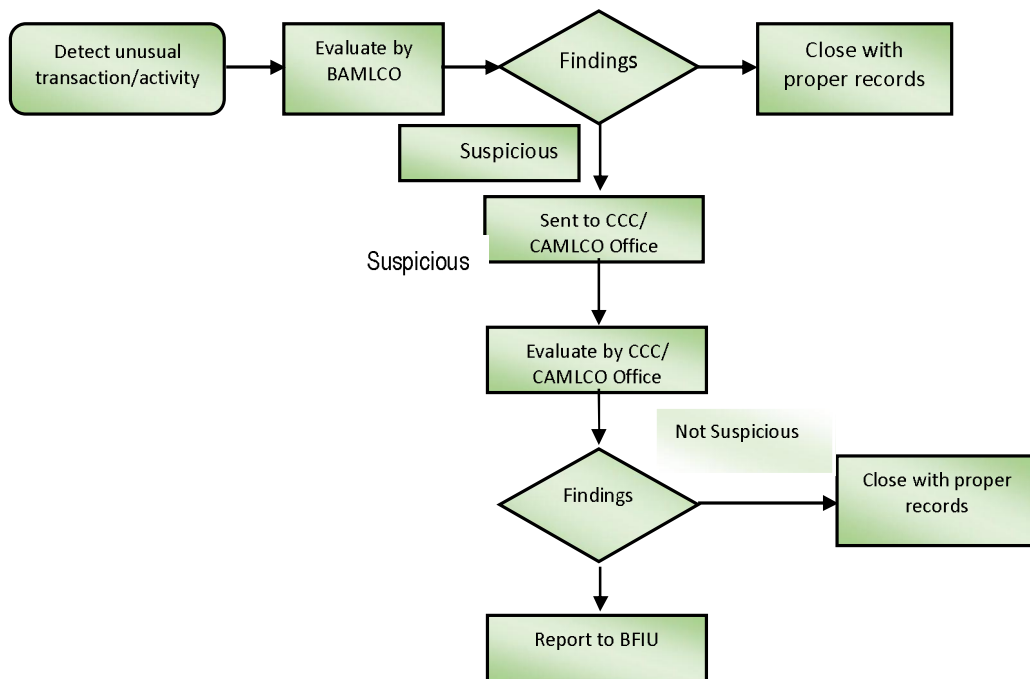


Figure: STR/SAR identification and reporting procedures

13.4 Tipping Off

Bank officials need to consider the confidentiality of the reporting of STR/SAR. They should not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary

[Handwritten signature]

[Handwritten signature]

13.5 Cash Transaction Report

CTR process of bank is fully automated in our bank. Every branch will download CTR through the system and monitor all transactions in due time. If any branch has not any such transaction, branch should report it to the AML & CFT Division, Head Office as 'there is no reportable CTR'. Simultaneously, branches need to identify suspicious transaction while reviewing the cash transactions and preserve the evidence regarding monitoring. If any suspicious transaction is found, the branch will submit it as 'Suspicious Transaction Report' to the CAMLCO's Office/AML & CFT Division. If no such transaction is identified, Branch will inform to the CAMLCO's Office/AML & CFT Division as 'No suspicious transaction has been found'. Besides, every branch needs to preserve its CTR in their branch(es).

The CAMLCO's Office/AML & CFT Division will also review all transactions under CTR of all branches and search for suspicious transaction. If any suspicious transaction is found report it to BFIU through goAML web. The CAMLCO's Office/AML & CFT Division must ensure the accuracy and timeliness while reporting CTR to BFIU. CAMLCO's Office/AML & CFT Division has to inform BFIU through the message board of goAML web in case of no transaction is found to be reported as CTR. Moreover, CAMLCO's Office/AML & CFT Division must ensure the preservation of information related to cash transaction report up to 5 (five) years from the month of submission to BFIU.

13.6 Self-Assessment Report

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 CAMLCO's Office/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 16.06.2020 and BFIU letter reference no BFIU/(Bank Monitoring)/16/2020/2507 dated 24.11.2020. Before finalizing the evaluation report, there shall have to be a meeting presided over by the branch manager 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 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 money laundering and terrorist financing, the progress of the related matters should be discussed.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



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 Department or ICCD of the Head Office and the CAMLCO's Office/AML & CFT Division within the 15th (fifteenth) day of the next month.

13.7 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 has to be done through a checklist that is circulated by BFIU circular no. 26 dated 16.06. 2020.

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.

13.8 ICCD's obligations regarding Self-Assessment or Independent Testing Procedure

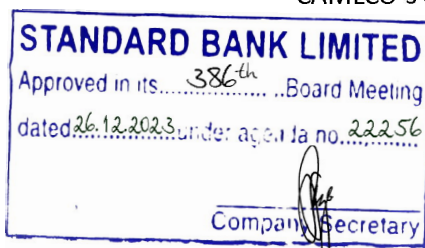
The ICCD shall assess the branch evaluation report received from the branches and if there is any risky matter realized in any branch, it shall inspect the branch immediately and shall inform the matter to the CAMLCO's Office/AML & CFT Division.

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 CAMLCO's Office/AML & CFT Division of the bank.

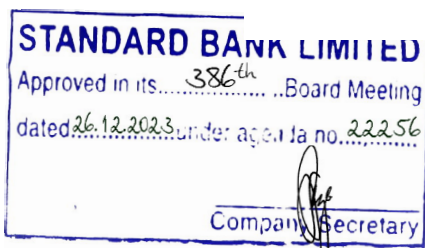
13.9 CAMLCO's Office obligations regarding Self-Assessment or Independent Testing Procedure

Based on the received branch evaluation reports from the branches and submitted inspection/audit reports by the ICCD, the CAMLCO's Office/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:

- a) Total number of branch and number of Self-Assessment Report received from the branches;
- b) The number of branches inspected/audited by the ICCD at the time of reporting and the status of the branches (branch wise achieved number);
- c) Same kinds of irregularities that have been seen in maximum number of branches according to the received Self-Assessment Report and measures taken by the CAMLCO's Office/AML & CFT Division to prevent those irregularities.



- d) The general and special irregularities mentioned in the report submitted by the ICCD and the measures taken by the CAMLCO's Office/AML & CFT Division to prevent those irregularities; and
- e) Measures to improve the ratings by ensuring the compliance activities of the branches that are evaluated as 'unsatisfactory' and 'marginal' in the received report.







CHAPTER XIV: RECRUITMENT, TRAINING AND AWARENESS

14.1 Obligations under Circular

Under obligations of the BFIU Circular No. 26 dated June 16, 2020, "To mitigate the risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, bank should follow proper Screening Mechanism in case of recruitment and ensure proper training for their officials"

14.2 Employee Screening

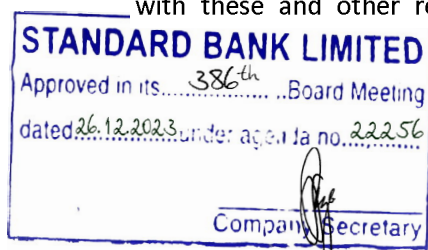
Banks are subject to ML, TF & P F risk from its customers as well as from its employee in absence of proper risk mitigating measures. ML, TF & PF risks arise from customers and its mitigating measures have been discussed in several chapters of this guideline. ML, TF & PF risks arose by or through its employees can be minimized if the bank follows 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 should follow the following measures (at least one from below):

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

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

14.3 Know Your Employee (KYE)

Know-your-customer, an essential precaution, must be coupled with know-your-employees. There are a lot of instances that highlight the involvement of employees in fraudulent transactions and in most cases in association with customers. This therefore brings in sharp focus the need for thorough checks on employees' credentials and proper screening of candidates to prevent the hiring of undesirables. 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 should be firmly in place. And the auditor should be conversant with these and other requirements, and see that they are constantly and uniformly updated.



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

14.4 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. Basic AML & CFT training should be at least day long model having evaluation module of the trainees. Relevant provision of Acts, rules and circulars, guidelines, regulatory requirements, suspicious transaction or activity reporting should be covered in basic AML & CFT training course. To keep the employees updated about AML & CFT measures, bank is required to impart refresher training programs of its employees on a regular basis.

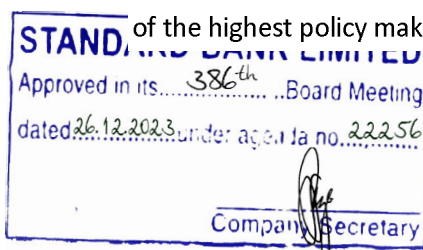
AML & CFT basic training should cover the following-

- an overview of AML & CFT initiatives;
- relevant provisions of MLPA & ATA and the rules there on;
- regulatory requirements as per BFIU circular, circular letters and guidelines;
- STR/SAR reporting procedure;
- ongoing monitoring and sanction screening mechanism;

Besides basic and refresher AML & CFT training, bank shall arrange job specific training or focused training i.e., Trade based money laundering & Credit based/back money laundering training for the trade/credit or investment professional employees who deal with foreign or domestic trade & credit or investment, UNSCR screening related training for all employees who deal with international transactions, customer relations and account opening; credit/investment fraud and AML & CFT related training for all the employees who deal with advance and credit of the bank; customer due diligence and ongoing monitoring of transaction related training for the employees who conduct transaction of customers.

14.5 Awareness of Senior Management

Without proper concern and awareness of senior management of the bank, it is difficult to have effective implementation of AML & CFT measures in the bank. Bank is required to arrange, at least once in a year, an awareness program for all the members of its Board of Directors or members of the highest policy making committee and people engaged with policy making of the bank.



14.6 Customer Awareness Program

Bank should take proper actions for broadcasting awareness building advertisement and documentaries regarding prevention of money laundering and terrorist financing through different mass media under Corporate Social Responsibility (CSR) fund. Branch should arrange awareness build up program for their customer regarding AML & CFT issues.

14.7 Awareness of Mass People

Prevention of ML & TF largely depends on awareness at all level. Public or mass people awareness on AML & CFT measures provides synergies to bank in implementing the regulatory requirement. For this, BFIU, BB, other regulators as well as the government sometimes arrange public awareness programs on AML & CFT issues. Bank shall participate with public awareness programs on AML & CFT issues which will be arranged by the BFIU, Bangladesh Bank or other regulators. Bank shall also take initiative to arrange public awareness programs like advertisements through billboard, poster, festoon and mass media, distribution of handbills, leaflet and so on.



CHAPTER XIV: TERRORIST FINANCING & PROLIFERATION FINANCING

15.1 Risk of Terrorist Financing & Proliferation Financing

Bangladesh has criminalized terrorist financing in line with the International Convention for the Suppression of the Financing of Terrorism (1999). Section 16 of Anti-terrorism Rules, 2013 states the responsibilities of the reporting agencies regarding funds, financial assets or economic resources or related services held in or through them.

A bank that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activity, is committing a criminal offence under the laws of Bangladesh. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism.

Regardless of whether the funds in a transaction are related to terrorists or terrorist activities, business relationships with such individuals or other closely associated persons or entities could, under certain circumstances, expose a bank to significant reputational, operational, and legal risk. This risk is even more serious if the person or entity involved is later shown to have benefited from the lack of effective monitoring or willful blindness of a particular bank and thus was to carry out terrorist acts.

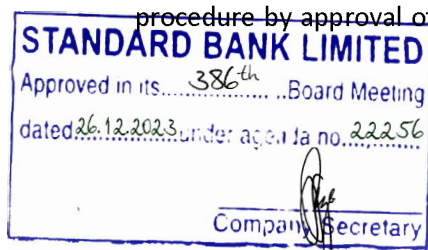
15.2 Legal Obligations

Under obligations of ATA 2009 (amendment 2012 & 2013), “Every Bank should take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009(amendment 2012 & 2013) and if any suspicious transaction is identified, the agency shall spontaneously report it to Bangladesh Bank without any delay”.

“The Board of Directors, or in the absence of the Board of Directors, the Chief Executive, by whatever name called, of each bank should approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by BFIU, Bangladesh Bank under section 15 of ATA, 2009(amendment 2012 & 2013); which are applicable to the bank, have been complied with or not.”

15.3 Obligations under Circular

Under obligations of BFIU Circular No. 26 dated June 16, 2020, “Every bank shall establish a procedure by approval of Board of Directors for detection and prevention of financing of terrorism



and financing of proliferation of weapons of mass destruction, shall issue instructions about the duties of Bank officials, review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.”

“Before any international business transaction, every bank will review the transaction to identify whether the concerned parties of that transactions are individual or entity of the listed individual or entity of any resolution of United Nation Security Council or listed or proscribed by Bangladesh government. Immediately after the identification of any account of any listed individual or entity concerned bank will stop that transaction and inform BFIU the detail information at the following working day.

15.4 Necessity of Funds by Terrorist

Terrorist organizations need money to operate. Weapons and ammunition are expensive. Major international operations require substantial investments for personnel, training, travel and logistics. Organizations must have substantial fundraising operations, as well as mechanisms for moving funds to the organization and later to terrorist operators.

15.5 Source of Fund/Raising of Fund

In general, terrorist organizations may raise funds through: legitimate sources, including through abuse of charitable entities or legitimate businesses and self-financing, criminal activity, state sponsors and activities in failed states and other safe havens.

15.6 Movement of Terrorist Fund

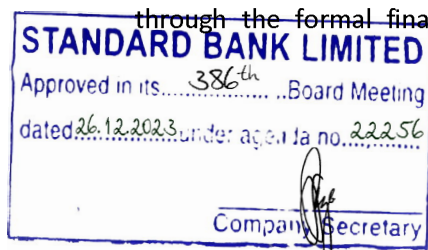
There are three main methods to move money or transfer value. These are:

- (1) the use of the financial system,
- (2) the physical movement of money (for example, through the use of through the use of cash couriers) and
- (3) the international trade system.

Often, terrorist organizations will abuse alternative remittance systems (ARS), charities, or other captive entities to disguise their use of these three methods to transfer value. Terrorist organizations use all three methods to maintain ongoing operation of the terrorist organization and undertake specific terrorist activities.

15.6.1 Formal Financial Sector

Financial institutions and other regulated financial service providers' services and products available through the formal financial sector serve as vehicles for moving funds that support terrorist



organizations and fund acts of terrorism. The speed and ease with which funds can be moved within the international financial system allow terrorists to move funds efficiently and effectively and often without detection between and within jurisdictions.

Combined with other mechanisms such as offshore corporate entities, formal financial institutions can provide terrorists with the cover they need to conduct transactions and launder proceeds of crime when such activity goes undetected.

15.6.2 Trade Sector

The international trade system is subject to a wide range of risks and vulnerabilities which provide terrorist organizations the opportunity to transfer value and goods through seemingly legitimate trade flows. To exploit the trade system for terrorist financing purposes could assist in the development of measures to identify and combat such activity.

15.6.3 Cash Couriers

The physical movement of cash is one way terrorists can move funds without encountering the AML & CFT safeguards established in financial institutions. It has been suggested that some groups have converted cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system. The movement of cash across the borders is prevalent in the cash based economy and where the electronic banking system remains embryonic or is little used by the populace.

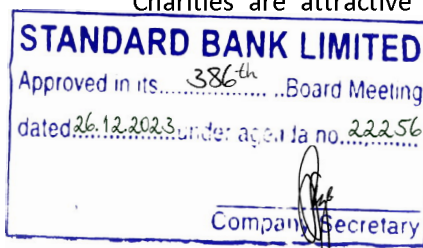
Moving money using cash couriers may be expensive relative to wire transfers. As legitimate financial institutions tighten their due diligence practices, it has become an attractive method of transferring funds without leaving an audit trail. When cross border remittance of cash is interdicted, the origin and the end use of cash can be unclear. Cash raised and moved for terrorist purposes can be at very low levels – making detection and interdiction difficult.

15.6.4 Use of Alternative remittance systems (ARS)

Alternative remittance systems (ARS) are used by terrorist organizations for convenience and access. ARS have the additional attraction of weaker and/or less opaque record-keeping and in many locations may be subject to generally less stringent regulatory oversight. Although FATF standards call for significantly strengthened controls over such service providers, the level of anonymity and the rapidity that such systems offer have served to make them a favored mechanism for terrorists.

15.6.5 Use of Charities and Non Profit Organizations

Charities are attractive to terrorist networks as a means to move funds. Many thousands of



legitimate charitable organizations exist all over the world that serve the interests of all societies, and often transmit funds to and from highly distressed parts of the globe. Terrorist abuses of the charitable sector have included using legitimate transactions to disguise terrorist cash travelling to the same destination; and broad exploitation of the charitable sector by charities affiliated with terrorist organizations. The sheer volume of funds and other assets held by the charitable sector means that the diversion of even a very small percentage of these funds to support terrorism constitutes a grave problem.

15.7 Targeted Financial Sanctions

The term Targeted Financial Sanctions (TFS) means both asset freezing and prohibition to prevent funds on other assets from being available, directly or indirectly, for the benefit of designated persons and entities. This TFS is 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.

15.7.1 TFS related to terrorism and terrorist financing

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 of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolution; or (ii) designated by that country pursuant to resolution 1373(2001)'.

15.7.2 TFS related to Proliferation

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. 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 of the Charter of the United Nations'.



15.8 Automated Screening Mechanism of UNSCRs

As per advise from Bangladesh Financial Intelligence Unit (BFIU), for effective implementation of TFS relating to TF & PF Standard Bank has already been 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 need 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 a word, bank shall ensure that screening has done before-

- any international relationship or transaction;
- opening any account or establishing relationship domestically

For proper implementation of sanction list screening (OFAC, EU, UN, etc.), all officials of Standard Bank must have enough knowledge about-

- legal obligation and consequences of non-compliance;
- sources of information;
- what to do and how to do with sanction list;
- transactional review;
- how to deal with 'false positives';
- how to deal with actual match;
- how to deal with 'aggrieved person or entity';
- how to exercise 'exemption' requirements;
- listing & de-listing process

15.9 Responsibilities of Bank Officials for detection and Prevention of Financing on Terrorism and Financing in proliferation

Standard Bank establish clear lines of internal accountability, responsibility, and reporting system. Duties and responsibilities of the Bank officials/divisions/departments/units in detecting and preventing financing on terrorism and financing in proliferation of weapons of mass destruction are details as under:

Bank officials/divisions/departments/units	Role/Responsibilities
Officials responsible for Account Opening	a) Screening of sanction lists and local black list before account opening. b) Perform due diligence on prospective clients prior to opening account.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




Bank officials/divisions/departments/units	Role/Responsibilities
Officials responsible for Account Opening	<ul style="list-style-type: none"> c) Obtain documents perfectly. d) Be diligent regarding the identification (s) of account holder and the transactions relating to the account. e) Complete the KYC/CDD for new customer.
Operations Officer	<ul style="list-style-type: none"> a) Obtain source of large deposits and preserve the record. b) Ensure that all control points are completed prior to allowing transaction in the account. c) Update customer transaction profiles in the system as and when required.
Teller	<ul style="list-style-type: none"> a) Obtain identity documents of walk-in customer while receiving or paying cash including online transaction. b) Duly checked the signature of signatories before payment of any cheque.
Credit/Foreign Exchange/SME officials of the Branch	<ul style="list-style-type: none"> a) Confirm risk assessment of customer's business. b) Must screen of sanction lists and local black list before processing any investment proposal. c) Implementation of BFIU instructions.
HOB/MOB/BAMLCO	<ul style="list-style-type: none"> a) Confirm the transaction monitoring process. b) Circulate and upgrade all employees of the branch regarding internal circular and BFIU circular of AML & CFT. c) Confirm sanction lists and local black list checking is done. d) Confirm AML & CFT training of all the employees of the branch. e) Confirm KYC/CDD/EDD of the customers of the branch.
International Division	<ul style="list-style-type: none"> a) Confirm that the respondent bank is not under sanction list. b) Confirm screening of customer information with sanction lists. c) Confirm the regulatory rules and regulation is maintained perfectly. d) Confirm that the applicant and beneficiary of foreign trade are not involved in financing on terrorism and financing in proliferation.
FRD Division	<ul style="list-style-type: none"> a) Confirm the source of fund of the remittance. b) Ensure the screening of the beneficiary or those who are involved in the transaction of the remittance.
IT Division	<ul style="list-style-type: none"> a) Confirm that system will generate report as per requirement of BFIU and CAMLCO's Office/AML & CFT Division. b) Update the system time to time in line with CAMLCO's Office/AML & CFT Division and BFIU requirement.

Bank officials/divisions/ departments/units	Role/Responsibilities
Credit/Investment Risk Management Division	a) Confirm that borrowers are not involve with terrorist financing and proliferation financing of weapons of mass destruction. b) Screening of customer information with sanction lists.
ICCD	a) Confirm the implementation status of combating terrorist financing and proliferation financing as per requirement of BFIU.
Card Division	a) Confirm screening of new customer and existing customer information with sanction lists and local black list. b) Confirm KYC/CDD of the customer before issuing cards.
Treasury Department	a) Release of remittance after checking confirmation of sanction list from the branch/department.
Central Compliance Committee(CCC)	a) Take appropriate initiative for combating terrorist financing and proliferation financing. b) Confirm of implementation of BFIU guidelines, circulars and internal circulars of the bank. c) Monitoring of all Branches.
CAMLCO	a) Take necessary initiative to comply the guidelines regarding terrorist financing and proliferation financing. b) Ensure that Bank has an effective system in place for combating terrorist financing and proliferation financing.
Managing Director & CEO	a) Provide all kinds of necessary support for implementation of guidelines, circulars for combating terrorist financing and proliferation financing.

All the employees of the Bank shall remain vigilant to ensure the bank is not used by terrorist financier and proliferation financier of weapons of mass destruction.

15.10 Role of Standard Bank in Preventing TF & PF Risk

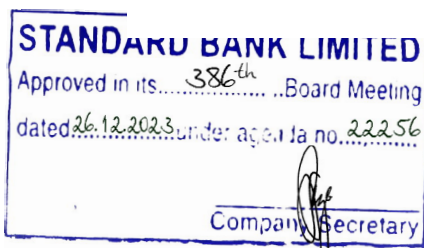
- ❖ Standard Bank discussed a procedure for detection and prevention of financing of terrorism and financing in proliferation of weapons of mass destruction, issued instructions about the duties of Bank officials and it will review those instruction time to time and ensure that they are complying with the instructions issued by BFIU.
- ❖ Bank shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions through which it is connected to any offence under ATA, 2009 (amendment 2012 & 2013) and if any suspicious transaction is

STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary




identified, the agency shall spontaneously report it to Bangladesh Bank without any delay.

- ❖ If any news of activities of financing of terrorism and financing of proliferation of weapons of mass destruction are published in any mass media, bank 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.
- ❖ The bank shall maintain and update the listed individuals and entities in electronic form and regularly run a check at the website of United Nations for updated list. 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.
- ❖ The bank shall run a check on the given parameters, including transactional review, to verify whether individuals or entities listed or scheduled under the ATA, 2009, (amendment 2012 & 2013); individuals or entities owned or controlled directly or indirectly by such persons or entities, as well as persons and entities acting on behalf of, or at the direction of, individuals or entities listed or scheduled under the Act are holding any funds, financial assets or economic resources or related services or having any form of relationship with them.



List of Abbreviations

AML, CFT & CPF	: Anti -Money Laundering, Combating Financing on Terrorism & Combating Proliferation Financing.
AOF	: Account Opening Form
APG	: Asia Pacific Group on Money Laundering
ATA	: Anti-Terrorism Act
BAMLCO	: Branch Anti Money Laundering Compliance Officer
BB	: Bangladesh Bank
BDT	: Bangladesh Taka
BFIU	: Bangladesh Financial Intelligence Unit
BMPE	: Black Market Peso Exchange
BO	: Beneficial Owner
CAMLCO	: Chief Anti Money Laundering Compliance Officer
CCC	: Central Compliance Committee
CDD	: Customer Due Diligence
CTC	: Counter Terrorism Committee
CTR	: Cash Transaction Report
CBML	: Credit Back/Backed Money Laundering
DCAMLCO	: Deputy Chief Anti Money Laundering Compliance Officer
DAMLCO	: Divisional/ Departmental Anti Money Laundering Compliance Officer
EU	: European Union
FATF	: Financial Actions Task Force
FERA	: Foreign Exchange Regulation Act
FI	: Financial Institution
FIU	: Financial Intelligence Unit
FPWM	: Financing of Proliferation of Weapons of Mass Destruction
FSRB	: FATF Style Regional Body
GPML	: Global program against Money Laundering
IBML	: Investment Backed/Back Money Laundering
ICRG	: International Cooperation and Review Group
IOSCO	: International Organization of Securities Commissions
IAIS	: International Association of Insurance Supervisors
IP	: Influential Person
ITP	: Independent Testing Procedure
KYC	: Know Your Customer
KYCC	: Know Your Customer's Customer
KYE	: Know Your Employee

KPF	: KYC Profile Form
LC	: Letter of Credit
ML	: Money Laundering
MLPA	: Money Laundering Prevention Act
NCC	: National Coordination Committee
NCCT	: Non-cooperating Countries and Territories
OBU	: Offshore Banking Unit
OECD	: Organization for Economic Co-operation and Development
OFAC	: Office of Foreign Assets Control
PEP	: Politically Exposed Persons
PF	: Proliferation Financing
PTA	: Payable Through Account
RBA	: Risk Based Approach
SAR	: Suspicious Activity Report
STR	: Suspicious Transaction Report
SDD	: Simplified Due Diligence
TF	: Terrorist Financing
TP	: Transaction Profile
TFS	: Targeted Financial Sanction
UBO	: Ultimate Beneficial Owner
UN	: United Nations
UNODC	: UN Office of Drugs and Crime
UNSCR	: United Nations Security Council Resolution
UCIC	: Unique Customer Identification Code
UTRN	: Unique Transaction Reference Number
TBML	: Trade Based Money Laundering
TL	: Transaction Laundering



Conventional Banking Vs Islamic Banking Terms

Serial No	Conventional Banking Terms	Islamic Banking Terms
1	Term loan	Murabaha Term Investment
2.	SOD	Bai Muajjel
3.	Loan General	Investment General
4.	Lease finance	Corporate HPSM Lease Finance
5.	Packing Credit	IHP Corporate Bai - Salam Pre-Shipment
6.	L/C Subsequent term loan	L/C Subsequent term investment
7.	SOD (Earnest Money)	Bai Muajjal (Earnest Money)
8.	L/C Subsequent term loan	L/C Subsequent Murabaha term investment
9.	Savings account	Mudaraba savings deposit account
10.	Current Account	Al-Wadiah Current Deposit account
11.	Fixed deposit Scheme	Retail Mudaraba Fixed Term Deposit
12.	Deposit Pension Scheme(DPS)	Mudaraba Deposit Pension Scheme
13.	Credit backed Money Laundering	Investment backed Money Laundering
14.	Loan backed Money Laundering	Investment backed Money Laundering
15.	Interest	Profit
16	Bank Loan	Bank Investment

ANNEXURE-A

KYC DOCUMENTATION


STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary



KYC documentation

Annexure A

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Individual	<ul style="list-style-type: none"> • Photograph of applicant (attested by the introducer) and nominee (attested by the applicant) • Passport/ National Id Card/ Birth Certificate + other photo ID (acceptable by the Bank) • Valid driving license (if any) • Credit Card (if any) • Any other documents that satisfy the bank. <p><i>NB: But in case of submitting the birth registration certificate, any other photo id (issued by a Government department or agency) of the person has to be supplied with it. If he does not have a photo id, then a certificate of identity by any renowned people has to be submitted according to the bank's requirement. That certificate must include a photo which is duly attested by the signing renowned person. The person should sign the certificate (printing his/her name clearly underneath) and clearly indicate his/her position or capacity on it together with a contact address and phone number.</i></p>	<ul style="list-style-type: none"> • Salary Certificate (for salaried person). • Employed ID (For ascertaining level of employment). • Self-declaration acceptable to the bank.(commensurate with declared occupation) • Documents in support of beneficial owner's income (income of house wife, students etc.) • Trade License if the customer declared to be a business person • E-TIN (if any) • Documents of property sale. (subject to necessity) • Other Bank statement (if any) • Document of MTDR encashment (if any) • Document of foreign remittance (if any fund comes from outside the country) • Document of retirement benefit. • Bank investment. 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier. • Physical verification report of bank official • Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). • Residential address appearing on an official document prepared by a Government Agency
Minor Account	<ul style="list-style-type: none"> • Photograph of applicant & guardian (attested by the introducer) and nominee (attested by the applicant) • Birth Certificate/Passport 	<ul style="list-style-type: none"> • Supporting documents of profession of guardian. 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department.


STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary





Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Minor Account	<ul style="list-style-type: none"> Any Other certificate attaching the photo ID like ID card/registration card (educational), etc. which is acceptable. Nominee & Guardian information Nominee & Guardian identity certificate. Information of beneficial owner (if any) 	<ul style="list-style-type: none"> Supporting documents of profession of beneficial owner. 	<ul style="list-style-type: none"> Proof of delivery of thanks letter through courier. Third party verification report. Physical verification report of bank official Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old).
Joint Account	<ul style="list-style-type: none"> Photograph of applicants (attested by the introducer) and nominee (attested by the applicant) Passport/National Id Card/ Birth Certificate + other photo id (acceptable by the Bank) Valid driving license (if any) Credit Card (if any) 	<ul style="list-style-type: none"> Salary Certificate (for salaried person). Employed ID (For ascertaining level of employment). Self-declaration acceptable to the bank.(commensurate with declared occupation) Documents in support of beneficial owner's income (income of house wife, students etc.) Trade License if the customer declared to be a business person E-TIN (if any) Documents of property sale.(if any) Other Bank statement (if any) Document of MTRD encashment (if any) Document of foreign remittance (if any fund comes from outside the country) 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier. Third party verification report. Physical verification report of bank official Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). Residential address appearing on an official document prepared by a Government Agency


Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Joint Account		<ul style="list-style-type: none"> Document of retirement benefit. Bank investment. 	
Sole Proprietorships or Individuals doing business	<ul style="list-style-type: none"> Photograph of the account holder duly attested by the introducer. Passport/National Id Card/ Birth Certificate + other photo id (acceptable by the Bank) Valid driving license (if any) Credit Card (if any) Rent receipt of the shop (if the shop is rental) Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents) Membership certificate of any association. (Chamber of commerce, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association etc. Any other documents that satisfy to the bank. 	<ul style="list-style-type: none"> Trade License (update) E-TIN Self-declaration acceptable to the bank. (commensurate with nature and volume of business) Documents of property sale. (if injected any fund by selling personal property) Other Bank statement (if any) Document of MTDR encashment (if any fund injected by en-cashing personal MTDR) Document of foreign remittance (if any fund comes from outside the country) Bank investment (if any) Personal borrowing (if any) 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier. Third party verification report. Physical verification report of bank official Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). Residential address appearing on an official document prepared by a Government Agency
Partnerships	<ul style="list-style-type: none"> Photograph of the partners (attested by the introducer). Partnership deed Registered partnership deed (if registered) Resolution of the partners, specifying operational guidelines/ instruction of the partnership account. Passport of partners/ National Id Card of partners/ Birth Certificate + other photo id (acceptable by the Bank) 	<ul style="list-style-type: none"> Trade License (update) E-TIN Documents of property sale. (if injected any fund by selling personal property of a partner) Other Bank statement (if any) Document of MTDR encashment (if any partner injected capital by en-cashing Personal MTDR) 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier. Third party verification report. Physical verification report of bank official

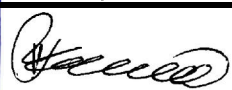
STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary






Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Partnerships	<ul style="list-style-type: none"> Valid driving license of partners (if any) Credit Card of partners (if any) Rent receipt of the shop (if the shop is rental) Ownership documents of the shop (i.e. purchase documents of the shop or inheritance documents) Membership certificate of any association. (Chamber of commerce, market association, trade association i.e.; Hardware association, cloth merchant association, hawker's association etc. Any other documents that satisfy to the bank. 	<ul style="list-style-type: none"> Document of foreign remittance (if any fund comes from outside the country) Bank investment Personal Borrowing (if any) 	<ul style="list-style-type: none"> Copy of utility bill/utility card on satisfaction of the dealing officer (not beyond 3 months old). Residential address appearing on an official document prepared by a Government Agency
Private Limited Companies	<ul style="list-style-type: none"> Photograph of the all Directors (attested by the introducer) Passport of all the directors/National Id Card of all the directors/ Birth Certificate + other photo id (acceptable by the Bank) Certificate of incorporation Memorandum and Articles of Association List of directors Resolution of the board of directors to open an account and identification of those who have authority to operate the account. Power of attorney granted to its Managers, Officials, or Employees to transact business on its behalf. Nature of the company's business. Expected monthly turnover 	<ul style="list-style-type: none"> A copy of last available financial statements duly authenticated by competent authority Other Bank statement Trade License E-TIN VAT registration Bank investment 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier. Physical verification, if necessary.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary






Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Private Limited Companies	<ul style="list-style-type: none"> Identity of beneficial owners, holding 20% profitor more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company. 		
Public Limited Companies	<ul style="list-style-type: none"> Photograph of the signatories/directors Passport of all the directors/National Id Card of all the directors/ Birth Certificate + other photo id (acceptable by the Bank) Certificate of incorporation Memorandum and Articles of Association Certificate of commencement of business List of directors in form -XII Resolution of the board of directors to open an account and identification of those who have authority to operate the account. Power of attorney granted to its Managers, Officials, or Employees to transact business on its behalf. Nature of the company's business Expected monthly turnover Identity of beneficial owners, holding 20% profitor more of having control over the company's 	<ul style="list-style-type: none"> A copy of last available financial statements duly authenticated by competent authority Other Bank statement Trade License E-TIN Cash flow statement VAT registration Bank investment Any other genuine source 	N/A

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary






Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Public Limited Companies	<ul style="list-style-type: none"> Identity of beneficial owners, holding 20% profitor more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee , officer or director of the company. 		
Government-Owned entities	<ul style="list-style-type: none"> Photograph of the signatories. Statue of formation of the entity Resolution of the board to open an account and identification of those who have authority to operate the account. Passport of the operator (s)/National Id Card of the operator (s)/ Birth Certificate + other photo id (acceptable by the Bank) 	N/A	N/A
NGO	<ul style="list-style-type: none"> Photograph of the signatory (s) (attested by the introducer) National Id Card of the operator (s)/ Passport of the operator (s)/ Birth Certificate + other photo id (acceptable by the Bank) Resolution of the board of directors to open an account and identification of those who have authority to operate the account. Documents of nature of the NGO Certificate of registration issued by competent authority Bye-laws (certified) 	<ul style="list-style-type: none"> A copy of last available financial statements duly authenticated by competent authority Other Bank statement Trade License E-TIN Certificate of Grand/ Aid 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier.

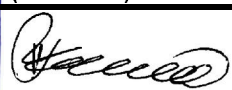
STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary





Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
NGO	<ul style="list-style-type: none"> List of Management Committee/ Directors 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">
Charities or Religious Organizations	<ul style="list-style-type: none"> Photograph of the signatory (s) (attested by the introducer) National Id Card of the operator (s)/ Passport of the operator (s)/ Birth Certificate + other photo id (acceptable by the Bank) Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. Documents of nature of the Organizations Certificate of registration issued by competent authority (if any) Bye-laws (certified) List of Management Committee/ Directors 	<ul style="list-style-type: none"> A copy of last available financial statements duly authenticated by competent authority Other Bank statement Certificate of Grand/ Aid/ donation Any other legal source 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier.
Clubs or Societies	<ul style="list-style-type: none"> Photograph of the signatory(s) (attested by the introducer) National Id Card of the operator (s)/ Passport of the operator (s)/ Birth Certificate + other photo id (acceptable by the Bank) Resolution of the Executive Committee to open an account and identification of those who have authority to operate the account. Documents of nature of the Organizations Certificate of registration issued by competent authority (if any) Bye-laws (certified) 	<ul style="list-style-type: none"> A copy of last available financial statements duly certified by a professional (if registered) Other Bank statement Certificate of Grand/ Aid Subscription If unregistered declaration of authorized person/ body 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier. Physical verification, if necessary.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary





Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Clubs or Societies	<ul style="list-style-type: none"> List of Management Committee/ Directors 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">
Trusts, Foundations or similar entities	<ul style="list-style-type: none"> Photograph of the signatory(s) (attested by the introducer) National Id Card of the trustee (s)/ Passport of the trustee (s)/ Birth Certificate + other photo id (acceptable by the Bank) Resolution of the Managing Body of the foundation/ association to open an account and identification of those who have authority to operate the account. Certified true copy of the Trust Deed Bye-laws (certified) Power of attorney allowing transaction in the account. 	<ul style="list-style-type: none"> A copy of last available financial statements duly certified by a professional (if registered) Other Bank statement Donation 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier. Physical verification, if necessary.
Financial Institutions (NBFi)	<ul style="list-style-type: none"> Photograph of all the directors(attested by the introducer) Passport of all the directors/ National Id Card of all the directors/ Birth Certificate + other photo id (acceptable by the Bank) Certificate of incorporation Memorandum and Articles of Association Certificate of commencement of business List of directors in form -XII Resolution of the board of directors to open an account and identification of those who have authority to operate the account. 	<ul style="list-style-type: none"> A copy of last available financial statements duly certified by professional accountant. Other Bank statement Trade License E-TIN Cash flow statement VAT registration 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier.

STANDARD BANK LIMITED
Approved in its...386th...Board Meeting
dated 26.12.2023 under agenda no. 22256
Company Secretary





Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Financial Institutions (NBF)	<ul style="list-style-type: none"> • Power of attorney granted to its Managers, Officials, or Employees to transact business on its behalf. • Nature of the company's business • Expected monthly turnover • Identity of beneficial owners, holding 20% profit or more of having control over the company's assets and any person (or persons) on whose instructions the signatories of the account act where such persons may not be a full time employee, officer or director of the company 		<ul style="list-style-type: none"> •
Embassies	<ul style="list-style-type: none"> • Photograph of the signatory(s) (attested by the introducer) • Valid Passport with visa of the authorized official • Clearance of the foreign ministry • Other relevant documents in support of opening account 		<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.
Foreign National (Individual)	<ul style="list-style-type: none"> • Passport along with visa page. • Identity of nominee(s), beneficial owner(if any) • Photograph of applicant (attested by the introducer) and nominee(s) (attested by the applicant) • Valid driving license (if any) • Credit card (if any) • Any other documents that satisfy the bank • Documents in support to stay in Bangladesh 	<ul style="list-style-type: none"> • Work permit • Employment certificate • Documents of foreign remittance • Other bank statement (if any) 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.

STANDARD BANK LIMITED
Approved in its...^{386th}...Board Meeting
dated 26.12.2023 under agenda no. 22256

Company Secretary





Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Foreign National (Individual)	<ul style="list-style-type: none"> Documents in support to source of fund or profession. 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none">
Foreign National Firm/Company/ Joint Venture Contracting	<ul style="list-style-type: none"> Copy of registration in Bangladesh with Board of investment/ Bangladesh Bank for Foreign/ Joint Venture Firm/Company Memorandum and Article of Association duly certified by RJSC. Copy of partnership deed Copy of Bye-laws Copy of service contact/ appointment letter/ work permit if any for operation of the account Resolution of governing body to open account and authorization of operation. List of authorized signatories and members of the governing body. Copies of the relevant pages of passport In case of foreign signatory(s) passport with visa page and work permit. In case of Bangladesh signatory(s) NID/ Passport/ Birth Certificate + other photo id (acceptable by the Bank) E-TIN (if any) Supporting documents of sources of fund of the signatory(s). Photographs of the signatories duly attested by the introducer. 	<ul style="list-style-type: none"> A copy of last available financial statements duly certified by professional accountant. Other Bank statement Certificate of grant/aid Any other documents of legal source. 	<ul style="list-style-type: none"> Acknowledgement receipt of thanks letter through postal department. Proof of delivery of thanks letter through courier.

Customer type	Standard Identification document	Document for verification of source of funds	Document or strategy for verification of address
Non Resident Bangladeshi (NRB) Account	<ul style="list-style-type: none"> • Photocopy of relevant pages of the passport duly attested by the competent authority. • Work/resident permit • Supporting documents of the nominee (NID/ Passport/ Birth Certificate + any other photo ID acceptable by the bank officials) • Documents of beneficial owner (if any) • Photograph of applicant (attested by the introducer) and nominee(s) (attested by the applicant) • Supporting document of source of fund/profession. 	<ul style="list-style-type: none"> • Employee ID • Documents for foreign remittance • Employee certificate 	<ul style="list-style-type: none"> • Acknowledgement receipt of thanks letter through postal department. • Proof of delivery of thanks letter through courier.

Note:

- If any customer want to authorize any person to operate an account on behalf of his/her then duly signed the mandate form to be obtained by the branch official. Mandate Form should be filled up mentioning the purpose of mandate and duration of this mandate. Branch official must be obtain accurate and complete information of mandatee.
- If there is one or more beneficial owners have been found then branch official must obtain supporting document of profession and identity.
- AML declaration form must be signed by the customer.
- SBS form must filled up and duly signed by the branch officials.
- If a person is US person as per FATCA, branch officials must obtain declaration and supporting documents as per requirement.

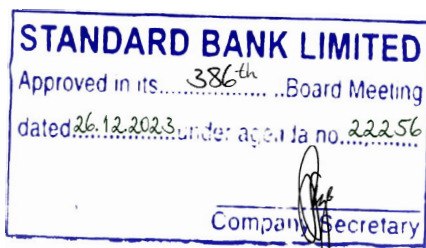






ANNEXURE-B

RED FLAGS - INDICATOR TO IDENTIFY STR/SAR



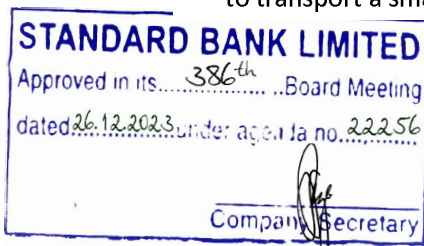
Red Flags pointing to STRs/SARs regarding Money Laundering

The following are examples of common indicators that may point to a suspicious transaction/ Suspicious Activity regarding Money Laundering:

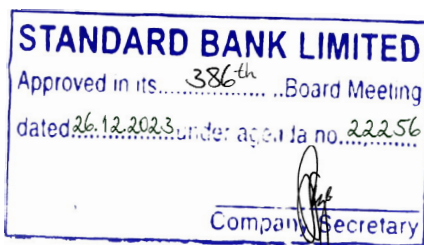
1. The client cannot provide satisfactory evidence of identity.
2. The client doesn't want correspondence sent to home address.
3. Situations where it is very difficult to verify customer information.
4. Situations where the source of funds cannot be easily verified.
5. Transactions in countries in which the parties are non-residents and their only purpose is a capital investment (they are not interested in living at the property they are buying).
6. Frequent change of ownership of same property in unusually short time periods with no apparent business, economic or other legitimate reason and between related persons.
7. Client wants to re-sell Property shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area.
8. Client wishes to form or purchase a company whose corporate objective is irrelevant to the client's normal profession or activities, without a reasonable explanation.
9. The client sets up shell companies with nominee shareholders and/or directors.
10. Client repeatedly changes Attorneys within a short period of time without any reasonable explanation.
11. Client purchases property in names of other persons or uses different names on offers to purchase, closing documents and deposit receipts.
12. Client deposits a large amount of cash with you to make payments which are outside of the client's profile.
13. Client negotiates a purchase but wants to record a lower value on documents, paying the difference "under the table", (inadequate consideration).
14. Client's documents such as identification, statement of income or employment details are provided by an intermediary who has no apparent reason to be involved, (the intermediary may be the real client).



15. Transaction involves legal entities and there is no relationship seen between the transaction and the business activity of the buying company, or the company has no business activity.
16. Client requests the firm to act as his agent in obtaining high sum bankers' drafts, cashiers' cheques and other cash equivalent or near cash monetary instruments or in making wire transfers to and from other banks or financial institutions, (anonymity).
17. Divergence from the type, volume or frequency of transactions expected in the course of the business relationship.
18. Client gives power of attorney to a non-relative to conduct large transactions (same as above).
19. Letter of credit is received from countries with a high risk for money laundering.
20. Over invoicing and under invoicing of goods and services at price.
21. Payments to a vendor by unrelated third parties
22. False reporting, such as commodity misclassification, commodity over- or under-valuation
23. Repeated importation and exportation of the same high-value commodity, known as carousel transactions
24. Commodities being traded that do not match the business involved
25. Unusual shipping routes or transshipment points
26. Packaging inconsistent with the commodity or shipping method
27. Double-invoicing
28. Whether the size of the shipment appears inconsistent with the scale of the Importer's regular business activities
29. Whether shipment is made prior to the LC issuing date;
30. Whether bill of exchange value differs with the commercial invoice;
31. Whether documents contain so many corrections;
32. Whether the transaction involves the use of repeatedly amended or frequently extended LC without reasonable justification;
33. Whether significant discrepancies appear between the descriptions of the goods on the transport document (i.e., bill of lading) and the invoice, or other documents (i.e., certificate of origin, packing list, etc.);
34. Whether Shipment locations or description of goods is inconsistent with the letter of credit;
35. Whether Packaging is inconsistent with commodity or shipping method;
36. Whether the shipment does not make economic senses e.g. the use of a forty-foot container to transport a small amount of relatively low value merchandise;



37. Whether the transaction involves the use of front or shell companies;
38. Whether unusual shipping routes or trans-shipment points are used;
39. Whether Port of Loading, transit or transshipment points, Port of Discharge, vessel name, carrier, master and/or any other party appearing in the BL or any other new name appearing in any other document are properly checked in the sanction list of UNSCR, EU, OFAC & local list;
40. Whether phantom/less shipment is made against LC;
41. Whether any duplication of payment has been identified/ received.
42. Use of letters of credit to move money between those countries, where such trade would not normally occur and / or is not consistent with the customer's usual business activity.
43. A Letter of credit is generally resorted to so as to accord more legitimacy to the transaction in order to conceal the real facts.
44. 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.
45. 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.
46. Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity are indicators for Trade Based Money Laundering. In this regard the study of foreign exchange remittances may help detect the offence.
47. The commodity is shipped to or from a jurisdiction designated as 'high risk' for ML activities or sensitive/non co-operative jurisdictions.
48. The commodity is transshipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
49. Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction i.e. trade in goods other than goods which are normally exported/imported by a jurisdiction or which does not make any economic sense.
50. Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
51. Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or



the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.

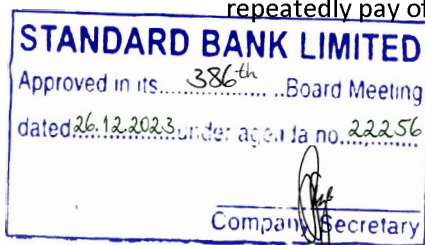
52. Trade transaction reveals links between representatives of companies exchanging goods i.e. same owners or management.

Red Flags regarding Credit/ Investment Backed or Based Money Laundering

These indicators are not intended to represent an exhaustive list of all the possible types of transactions that might be linked to money laundering/ terrorist financing/proliferation financing. Nor should it in any way be implied that the transactions listed here are necessarily linked to such activities. It should be remembered that activities related to money laundering or terrorist financing or proliferation financing are always carried out with the aim of appearing to be "normal". The criminal nature of the activity derives from the origin of the funds and the aim of the participants.

Natural persons:

- Transactions involving persons residing in tax havens or risk territories, when the characteristics of the transactions match any of those included in the list of indicators.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
- Transactions involving persons who are being tried or have been sentenced for crimes or who are publicly known to be linked to criminal activities involving illegal enrichment, or there are suspicions of involvement in such activities and that these activities may be considered to underlie money laundering.
- Transactions involving persons who are in some way associated with the foregoing (for example, through family or business ties, common origins, where they share an address or have the same representatives or attorneys, etc.).
- Transactions involving an individual whose address is unknown or is merely a correspondence address (for example, a PO Box, shared office or shared business address, etc.), or where the details are believed or likely to be false.
- Several transactions involving the same party or those undertaken by groups of persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Individuals who unexpectedly repay problematic investments or mortgages or who repeatedly pay off large investments or mortgages early, particularly if they do so in cash.

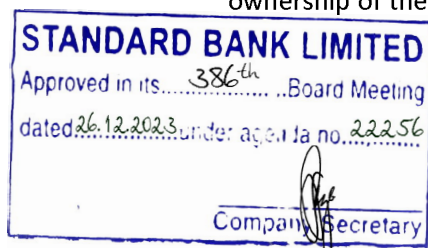


Legal persons:

- Transactions involving legal persons or legal arrangements domiciled in tax havens or risk territories, when the characteristics of the transaction match any of those included in the list of indicators.
- Transactions involving recently created legal persons, when the amount is large compared to their assets.
- Transactions involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
- Transactions involving foundations, cultural or leisure associations, or non-profit-making entities in general, when the characteristics of the transaction do not match the goals of the entity.
- Transactions involving legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Transactions involving legal persons whose addresses are unknown or are merely correspondence addresses (for example, a PO Box number, shared office or shared business address, etc.), or where the details are believed false or likely to be false.
- Various transactions involving the same party. Similarly, transactions carried out by groups of legal persons that may be related (for example, through family ties between owners or representatives, business links, sharing the same nationality as the legal person or its owners or representatives, sharing an address, in the case of legal persons or their owners or representatives, having a common owner, representative or attorney, entities with similar names, etc.).
- Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.
- Formation of legal persons to hold properties with the sole purpose of placing a front man or straw man between the property and the true owner.
- Contribution of real estate to the share capital of a company which has no registered address or permanent establishment which is open to the public in the country.
- Transactions in which unusual or unnecessarily complex legal structures are used without any economic logic.

Natural and legal persons:

- Transactions in which there are signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real customer.
- Transactions which are begun in one individual's name and finally completed in another's without a logical explanation for the name change. (For example, the sale or change of ownership of the purchase or option to purchase a property which has not yet been handed



over to the owner, reservation of properties under construction with a subsequent transfer of the rights to a third party, etc.).

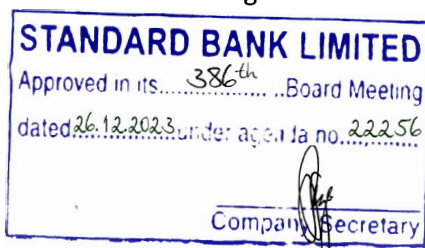
- Transactions in which the parties:
 - Do not show particular profit/income in the characteristics of the property (e.g. quality of construction, location, date on which it will be handed over, etc.) which is the object of the transaction.
 - Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms.
 - Show a strong profit/income in completing the transaction quickly, without there being good cause.
 - Show considerable profit/income in transactions relating to buildings in particular areas, without caring about the price they have to pay.
- Transactions in which the parties are foreign or non-resident for tax purposes and:
 - Their only purpose is a capital investment (that is, they do not show any profit/income in living at the property they are buying, even temporarily, etc.).
 - They are interested in large-scale operations (for example, to buy large plots on which to build homes, buying complete buildings or setting up businesses relating to leisure activities, etc.).
- Transactions in which any of the payments are made by a third party, other than the parties involved. Cases where the payment is made by a credit institution registered in the country at the time of signing the property transfer, due to the granting of a mortgage investment, may be excluded.

Intermediaries:

- Transactions performed through intermediaries, when they act on behalf of groups of potentially associated individuals (for example, through family or business ties, shared nationality, persons living at the same address, etc.).
- Transactions carried out through intermediaries acting on behalf of groups of potentially affiliated legal persons (for example, through family ties between their owners or representatives, business links, the fact that the legal entity or its owners or representatives are of the same nationality, that the legal entities or their owners or representatives use the same address, that the entities have a common owner, representative or attorney, or in the case of entities with similar names, etc.).
- Transactions taking place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.

Means of payment:

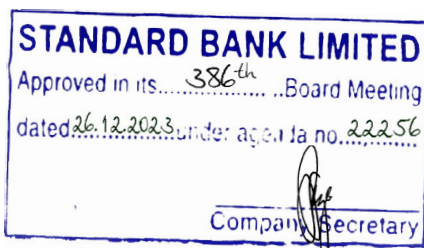
- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction.



- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them.
- Transactions where there are doubts as to the validity of the documents submitted with investment applications.
- Transactions in which a investment granted, or an attempt was made to obtain a investment, using cash collateral or where this collateral is deposited abroad.
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments, or where payment is made by endorsing a third-party's cheque.
- Transactions with funds from countries considered to be tax havens or risk territories, according to anti-money laundering legislation, regardless of whether the customer is resident in the country or territory concerned or not.
- Transactions in which the buyer takes on debt which is considered significant in relation to the value of the property. Transactions involving the subrogation of mortgages granted through institutions registered in the country may be excluded.

Nature of the Transaction:

- Transactions in the form of a private contract, where there is no intention to notarize the contract, or where this intention is expressed, it does not finally take place.
- Transactions which are not completed in seeming disregard of a contract clause penalizing the buyer with loss of the deposit if the sale does not go ahead.
- Transactions relating to the same property or rights that follow in rapid succession (for example, purchase and immediate sale of property) and which entail a significant increase or decrease in the price compared with the purchase price.
- Transactions entered into at a value significantly different (much higher or much lower) from the real value of the property or differing markedly from market values.
- Transactions relating to property development in high-risk urban areas, in the judgment of the company (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics.
- Recording of the declaration of a completed new building by a non-resident legal person having no permanent domicile indicating that the construction work was completed at its own expense without any subcontracting or supply of materials.
- Transactions relating to property development in high-risk urban areas based on other variables determined by the institution (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).



Red Flags pointing to STRs/SARs regarding Terrorist Financing

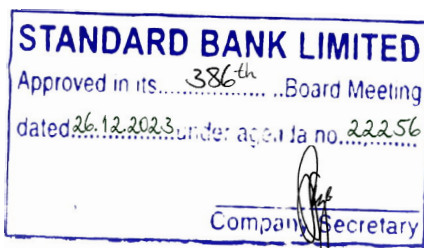
The following are examples of common indicators that may point to a suspicious transaction/ Suspicious Activity regarding financing of terrorism:

Behavioral Indicators:

1. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
2. Use of false corporations, including shell-companies.
3. Inclusion of the individual or entity in the United Nations 1267 Sanctions list.
4. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
5. Beneficial owner of the account not properly identified.
6. Use of nominees, trusts, family members or third party accounts.
7. Use of false identification.
8. Abuse of non-profit organization. Indicators linked to the financial transactions:

Indicators linked to financial transactions:

1. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
2. The transaction is not economically justified considering the account holder's business or profession.
3. A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
4. Transactions which are inconsistent with the account's normal activity.
5. Deposits were structured below the reporting requirements to avoid detection.
6. Multiple cash deposits and withdrawals with suspicious references.
7. Frequent domestic and international ATM activity.
8. No business rationale or economic justification for the transaction.
9. Unusual cash activity in foreign bank accounts.



10. Multiple cash deposits in small amounts of an account followed by a large wire transfer to another country.
11. Use of multiple, foreign bank accounts.

