KYC/AML/CFT Policy

2025

Division: Chennai

Document Control

Serial No	Type of Information	Document Data
1	Policy Title	KYC/AML/CFT Policy
2	Date of Approval	13.02.2025
3	Policy Superseded	-
4	Policy Version Number	4.0
5	Policy Owner	Chennai Branch
6	Policy Approval	Board of Directors

Disclaimer

The contents of this Policy document are subject to changes on subsequent amendments to existing legal provisions and new legal provisions that would be imposed by the Parliament of Sri Lanka and Parliament of India any rules, regulations and the guidelines that would be issued by the Central Bank of Sri Lanka and Reserve Bank of India from time to time.

Table of Contents

	Particulars	Page No
1.	Short Title	06
2.	Applicability	06
3.	Definitions	07
4.	General	12
5.	The KYC policy includes following four key elements	12
6.	Designated Director	13
7.	Principal Officer	13
8.	Compliance of KYC policy	14
9.	Customer Acceptance Policy	14
10.	Part – I – CDD Procedure in case of Individuals	16
11.	Part – II – CDD Measures for Sole Proprietary Firms	18
12.	Part – III – CDD Measures for Legal Entities	19
13.	Part – IV – Identification of Beneficial Owner	21
14.	Part – V – Trade Based Money Laundering	21
15.	Part – VI – On-going Due Diligence	24
16.	Part – VII – Enhanced and Simplified Due Diligence Procedure	26
17.	Record Management	28
18.	Reporting Requirements to Financial Intelligence Unit – India	29
19.	Requirements / Obligations under International Agreements	31
20.	Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems	
21.	(Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)	32
22.	Freezing of Assets under of Unlawful Activities (Prevention) Act, 1967	33
23.	Jurisdictions that do not or insufficiently apply the FATF Recommendations	33
24.	Other Instructions	34

Particulars	Page No
Annexure – I	42
Annexure – II	48
Annexure – III	56
Annexure – IV	59
Annexure – V	65
Annexure – VI	73
Annexure – VII	80
Annexure – VIII	82
Annexure – IX	84
Annexure – X	86
Annexure – XI	87
Annexure – XII	90
Annexure – XIII	92
Annexure – XIV	93

KYC/AML/CFT Policy, 2025

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India and Aadhaar and other Laws (amendment) Ordinance, 2019 as notified by the Government of India, Bank is required to follow certain customer identification procedure while undertaking a transaction either by establishing an account based relationship or otherwise and monitor their transactions.

This KYC Policy is prepared as per RBI's Master Directions on Know Your Customer (updated up to 17.10.2023) which incorporates the amendments made by Government of India, vide Gazette Notification G.S.R. 582(E) dated August 19, 2019 and Gazette Notification G.S.R. 840(E) dated November 13, 2019.

The Bank should take all necessary steps to implement this KYC/AML/CFT Policy and provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act ibid, Sections 45JA, 45K and 45L of the Reserve Bank of India Act, 1934, Section 10 (2) read with Section 18 of Payment and Settlement Systems Act 2007 (Act 51 of 2007), Section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

1. Short Title

Policy guidelines on Know Your Customer (KYC) Norms / Anti Money laundering (AML) Standards / Combating of Financing of terrorism (CFT) Measures / Obligation of the Bank under Prevention of Money Laundering Act (PMLA), 2002 shall be called as KYC/AML/CFT Policy, 2025

2. Applicability

a) The provisions of KYC Policy guidelines shall apply to Bank of Ceylon Chennai branch.

i. In case there is a variance in KYC / AML / CFT standards prescribed by the Reserve Bank of India and the host country regulators, Bank is required to adopt the more stringent regulation of the two.

Provided this rule shall not apply to 'small accounts'.

3. Definitions

In terms of RBI's Master Direction on KYC, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(A) Terms bearing meaning assigned in terms of Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005:

i. **"Aadhaar number"** as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

ii. **"Act" and "Rules"** means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

iii. **"Authentication"**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of Section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

iv. Beneficial Owner (BO)

a. **Where the customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has / have controlling ownership interests or who exercise control through other means

Explanation- For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of / entitlement to more than 10 per cent of the shares or capital or profits of the company.
(ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

b. **Where the customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has / have ownership of / entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation- For the purpose of this sub-clause, "control" shall include the right to control the management of policy decision.

c. **Where the customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has / have ownership of/ entitlement to more than 10 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. **Where the customer is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. **"Certified Copy of OVD"** - Obtaining a certified copy by the Bank shall mean comparing the copy of officially valid document so produced by the customer with the original where offline verifications cannot be carried out and recording the same on the copy by the Authorised Officer of the Branch will also attest the duly signed photograph of the customer.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

i. **"Central KYC Records Registry"** (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

ii. **"Designated Director"** means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

iii. **"Principal Officer"** means an officer nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules.

iv. **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

v. **"Non-profit Organizations"** (NPO) means any entity or organization constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

vi. **"Officially valid document"** (OVD) means the passport the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that,

a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -

i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. Property or Municipal tax receipt;

iii. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

Further, at the time of on-boarding of the customer, an undertaking should be obtained from the customer along with AOF/OVDs stating that Customer shall submit his OVD with updated current address within 3 months failing which operations in his account shall be restricted.

c. The customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above, failing which the operations in the account shall be restricted (Debit-freezed).

d. Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

vi. **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

vii. **"Person"** has the same meaning assigned in the Act and includes:

a. an individual,
b. a Hindu undivided family,
c. a company,
d. a firm,
e. an association of persons or a body of individuals, whether incorporated or not,
f. every artificial juridical person, not falling within any one of the above persons (a to e), and
g. any agency, office or branch owned or controlled by any of the above persons (a to f).

viii. "**Suspicious transaction**" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

(i) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
(ii) appears to be made in circumstances of unusual or unjustified complexity; or
(iii) appears to not have economic rationale or bona-fide purpose; or
(iv) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

ix. **A 'Small Account'** means a savings account which is opened in terms of sub- rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 18.

x. **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of an account;
b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. establishing or creating a legal person or legal arrangement.

xi. "**UCIC"** means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

(B) In RBI Master Directions on KYC, unless the context otherwise requires, shall bear the meanings assigned to them below: Terms bearing meaning assigned in this Policy, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. **"Common Reporting Standards"** (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

ii. **"Correspondent Banking"** is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

iii. **"Customer"** means a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iv. **"Walk-in Customer"** means a person who does not have an account-based relationship with the Bank, but undertakes transactions with the Bank.

v. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

vi. **"Customer identification"** means undertaking the process of CDD.

vii. **"FATCA"** means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest

viii. **"IGA"** means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

ix. **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

x. **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that **those** are consistent with the Bank's knowledge about the customers' business and risk profile and source of funds/wealth.

xi. **"Periodic Updation"** means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xii. **"Politically Exposed Persons"** (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

xiii. **"Shell bank"** means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xiv. **"Wire transfer"** related definitions means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

(C) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar.

(Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made there under, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. General

This KYC AML CFT policy is duly approved by the Board of Directors of bank. The policy will be reviewed by the Board and/or any committee of the Board to which power has been delegated, at yearly intervals or as and when considered necessary by the Board.

Purpose

The purpose of KYC policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.

For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

Objective

The KYC Policy has been framed to develop a strong mechanism for achieving the following objectives:

To prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently.

To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms / AML standards / CFT measures / Bank's Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.

5. The KYC policy includes following four key elements

(a) Customer Acceptance Policy (CAP);
(b) Risk Management;
(c) Customer Identification Procedures (CIP); and
(d) Monitoring of Transactions

5A. Money Laundering and Terrorist Financing Risk Assessment by Bank

(a) Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions, or delivery channels etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Bank from time to time.

(b) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. However, it should be reviewed at least annually.

(c) The outcome shall be reviewed by the Risk Management Committee of Chennai Branch and will be put up to the Management Committee of Chennai Branch also. Once the Management Committee of Chennai Branch reviews the outcome of the assessment, the report will be placed for the independent review of the Concurrent Auditor of the Bank after which the above will be placed in the Local Advisory Board (LAB).

(d) Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, the Bank shall monitor the implementation of the controls and enhance them if necessary.

6. Designated Director

(a) A "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and shall be nominated by the Board.

(b) The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

(c) Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

(d) In no case, the Principal Officer shall be nominated as the 'Designated Director'.

(e) The Country Manager shall act as the Designated Director for Chennai Branch.

7. Principal Officer

The Bank has appointed Chief Compliance Officer as the Principal Officer. The Principal Officer shall be independent and report directly to the Deputy General Manager Compliance at Head Office (Global CCO). Principal Officer is responsible for monitoring AML compliance at operational units, review of suspicious transactions reported by Bank through STRs and sharing of information as required under the law. The PO will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The role and responsibilities of the Principal Officer include overseeing and ensuring overall compliance with regulatory guidelines on AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time. The Principal Officer is responsible for timely submission of STR, CTR, CBWTR and reporting of counterfeit notes (CCR) and all transactions involving receipts by Non-Profit Organizations (NTR) of value more than Rupees Ten lakh or its equivalent in foreign currency to FIU-IND. The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information. The Principal Officer shall fix the thresholds for generation of AML alerts after review by the Management Committee of Chennai Branch and the periodicity of reviewing the alerts shall be once in a year or as and when required. The name, designation and address of the Principal Officer shall be communicated to FIU-IND as well as RBI. In no case, the Principal Officer shall be nominated as the 'Designated Director'.

8. Compliance of KYC policy

(a) Bank to ensure compliance with KYC Policy through:

i. A senior officer in the rank of Senior Vice President will be designated as 'Senior Management' for the purpose of KYC compliance.

ii. Allocation of responsibility through Office Order for effective implementation of policies and procedures at the Branch

iii. Concurrent / Internal Audit system to verify the compliance with KYC / AML policies and procedures and submit quarterly audit notes and compliance to the Local Advisory Board. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at Chennai branch would be reviewed for apprising Local Advisory Board.

iv. Concurrent / Internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports from CBS.

1. Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

2. PML Rules require Chennai Branch of the Bank to carry out Risk Assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels. The risk assessment should-

   i. be documented;

   ii. consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

   iii. be kept up to date; and

   iv. be available to competent authorities and self-regulating bodies.

Customer Acceptance Policy

9. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, the Bank shall ensure that

a. No account is opened in anonymous or fictitious / benami name.

b. No account is opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. The Bank shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

c. No transaction or account-based relationship is undertaken without following the CDD procedure.

d. The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.

e. 'Optional' / additional information, where such information requirement has not been specified in the internal KYC Policy of the Bank, is obtained with the explicit consent of the customer before / after the account is opened.

f. Bank will apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of Bank desires to open another account with the same Bank, there shall be no need for a fresh CDD exercise.
g. CDD Procedure is followed for all the joint account holders, while opening a joint account.
h. Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
i. No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
j. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
k. Where an equivalent e-document is obtained from the customer, Bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
l. Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
m. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank /other relevant authorities, on request.

10. Bank to ensure that the Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

Where the Bank forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

Risk Management

11. For Risk Management, Bank shall have a risk based approach which includes the following.

a. Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the Bank.
b. Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc.
c. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
d. The risk categorization of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

It is hereby specified that the various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.
Explanation: FATF Public Statement, the reports and guidance notes on KYC / AML issued by the Indian Banks Association (IBA), and other agencies etc. may also be used in risk assessment.

Customer Identification Procedure (CIP)

12. Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. Bank to undertake identification of customers in the following cases:

a. Commencement of an account-based relationship with the customer.
b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c. When Bank has reason to believe that a customer (account- based or walk- in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
d. Bank shall ensure that introduction is not to be sought while opening accounts.

Customer Due Diligence (CDD) Procedure

Part I -CDD Procedure in case of Individuals

13. For undertaking CDD, Bank shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

a) the Aadhaar number where,
   i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
   ii. he decides to submit his Aadhaar number voluntarily to the bank; or(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
   (ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
   iii. the KYC Identifier with an explicit consent to download records from CKYCR; and

b) Permanent account number (PAN) or Form 60 equivalent e-document thereof customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof, and
c) Two recent photograph; and
d) At least one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status, annual income, turnover (in case of business) such as salary slip, Registration certificate, Certificate / license issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST / VAT / GST certificates, Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, License / certificate of practice issued by any professional body incorporated under a statue,
Provided that where the customer has submitted,

i. Aadhaar number under clause (a) above, bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.
Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.

ii. Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank shall carry out offline verification.

While establishing an account-based relationship with individual customer, the Chennai branch official to ascertain as to whether the customer is already having a Cust ID with the Bank. In case the customer has an existing Cust ID, fresh Cust ID shall not be created and the new account shall be opened with the existing Cust ID.
Opening Form / Customer Master Form (marked as *) such as Name, Fathers" name, date of birth, address, Identity Proof, address proof, Identification number (Identity proof document number), Profession / activity (Nature of Business - specific), total annual income, total annual turnover (in case of business) etc. are completely and duly filled in by the customer and are also correctly captured in customer's database in CBS.
In order to verify the authenticity of the KYC document, the authorized official shall online verify Officially Valid Document (OVD) & PAN card details furnished by the customer from central authentic database, wherever available, in public domain.
PAN Card and Voter Identity Card, wherever obtained, be verified on-line through the following websites and a print of on-line verification of the said document be held on record with the relevant AOF:

Name of Documents	Website/Links
PAN Card	eportal.incometax.gov.in
Voter Identity Card	www.nvsp.in (National Voters Service Portal)
Aadhar Card	uidai.gov.in

14. Notwithstanding anything contained in Section 15 and as an alternative thereto, in case an individual who desires to open a bank account, banks shall open a 'Small Account', which entails the following limitations:

(i) the aggregate of all credits in a financial year does not exceed rupees one lakh;
(ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
(iii) the balance at any point of time does not exceed rupees fifty thousand.

Provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following conditions:

a) The bank shall obtain a self-attested photograph from the customer.
b) The Principal Officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
   Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
c) Ensure that foreign remittances are not credited to the account.
d) Banks shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
e) The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
f) The entire relaxation provisions shall be reviewed after twenty-four months.
g) Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.
h) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high-risk scenarios, the identity of the customer shall be established as per Section 15.
i) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 15.

Part II - CDD Measures for Sole Proprietary firms

15. For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

16. In addition to the above, any two of the following documents or the equivalent e- document thereof as a proof of business / activity in the name of the proprietary firm shall also be obtained:

(i) Registration certificate including Udyam Registration Certificate (URC) issued by the Government
(ii) Certificate / License issued by the municipal authorities under Shop and Establishment Act.
(iii) Sales and income tax returns.
(iv) GST certificate (provisional / final)
(v) Professional Tax authorities.
(vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
(vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities.
(viii) Utility bills such as electricity, water, and landline telephone bills.

In cases where the Bank is satisfied that it is not possible to furnish two such documents, Bank may, at their discretion, accept only one of those documents as proof of business / activity.

Provided Bank undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III- CDD Measures for Legal Entities

17. **For opening an account of a company,** certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:
    - (i) Certificate of incorporation;
    - (ii) Memorandum and Articles of Association;
    - (iii) Permanent Account Number of the company;
    - (iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
    - (v) Documents, as specified in Section 13 relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
    - (vi) The names of the relevant persons holding senior management position; and
    - (vii) The registered office and the principal place of its business, if it is different.

18. **For opening an account of a partnership firm**, the certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:
    - (i) Registration certificate;
    - (ii) Partnership deed;
    - (iii) Permanent Account Number of the partnership firm; and
    - (iv) Documents, as specified in Section 13, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
    - (v) The names of all the partners and
    - (vi) Address of the registered office, and the principal place of its business, if it is different.

19. **For opening an account of a trust,** certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:
    - (i) Registration certificate;
    - (ii) Trust deed;
    - (iii) Permanent Account Number or Form No.60 of the trust; and
    - (iv) Documents, as specified in Section 13, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
    - (v) The names of the beneficiaries, trustees, settlor, **protector, if any** and authors of the trust
    - (vi) The address of the registered office of the trust; and
    - (vii) List of trustees and documents, as specified in Section **13**, for those discharging the role as trustee and authorized to transact on behalf of the trust.

20. **For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-document thereof shall be obtained:**

    (i) Resolution of the managing body of such association or body of individuals;
    (ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;
    (iii) Power of attorney granted to transact on its behalf;
    (iv) Documents, as specified in Section 13, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
    (v) Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

    Explanation: Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'.
    Explanation: Term 'body of individuals' includes societies.

21. **For opening an account of Hindu Undivided Family,** certified copies of each of the following documents shall be obtained:

    (i) Identification information as mentioned under Section 12 in respect of the Karta and Major Coparceners,
    (ii) Declaration of HUF and its Karta,
    (iii) Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses.
    (iv) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.

22. **Accounts of Non Profit Organizations**

    A Non Profit Organizations (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax At, 1961 (43 of 1961), that is registered as a Trust or a Society under the Societies Registration Act, 1860 (21 of 1860) or any similar State Legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

    All transactions involving receipts by these NPOs of value more than Rs. 10 Lakh or its equivalent in foreign currency is to be reported to FIU-IND by the Compliance Department at Chennai Branch. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 10 lakh, the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

    Registration of NPO (Non-profit Organization) on the DARPAN Portal of NITI Aayog
    Bank shall reach out to its customers who fall under the category of NPO to register the details of non-profit organisation on the DARPAN Portal of NITI Aayog, and shall maintain such registration records for a period of five years after the business relationship has ended or the account has been closed, whichever is later.

Part IV - Identification of Beneficial Owner

23. For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the Rules to verify his / her identity shall be undertaken keeping in view the following:

Where the customer or the owner of the controlling interest is

(i) an entity listed on a stock exchange in India, or

(ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or

(iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

i. In cases of company listed on a stock exchange, trust / nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

Part V – Trade Based Money Laundering

24. Background

In early stages trade finance was not considered as a major risk area for money laundering and terrorist financing. However, the perception has now been changed and international bodies and regulators increasingly consider trade activities as high-risk areas for money laundering, terrorist financing and proliferation of mass destruction. Therefore, the regulatory bodies have introduced more stringent rules and regulations for Financial Institutions based on the international best practices devised by the International Bodies acting on the prevention of ML and TF. The recent large fines imposed on Financial Institutions for breaches of international sanctions and financing and aiding ML and TF.

Because of these large fines imposed upon most of the global giants, they are in the process of de-risking which leads to the termination of correspondent relationships with Financial Institutions which poses high risk for ML and TF.

Hence, it is vital to effectively manage the ML and TF risks associated with trade activities.

25. Risks Associated with Trade Finance Activities related ML and TF

25.1 Money Laundering and Financing of Terrorism

As the controls implemented by the Financial Institutions on traditional techniques of ML and TF have become more robust, the other methods of transmitting funds including trade activities have become more attractive to the criminals.

The use of trade finance to obscure illegal movements of funds includes methods to misrepresent price, quantity and quality of goods traded. The transfer of value may be accomplished in a variety of ways as described below.

I. Over invoicing

By misrepresentation of price of the goods in the invoice and other documents (stating above the true value), the seller gains excess value when the payment is made,

II. Under invoicing

By misrepresentation of price of the goods in the invoice and other documents (stating below the true value), the buyer gains excess value when the payment is made.

III. Multiple invoicing

By issuing more than one invoice for the same goods, a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one Financial Institution to facilitate the payments.

IV. Short shipping

The seller ships less than the invoiced quantity or quality of goods thereby misrepresenting the value of goods in the documents. The effect is similar to over invoicing.

V. Over shipping

The seller ships more than the invoiced quantity or quality of goods thereby misrepresenting the value of goods in the documents. The effect is similar to under invoicing.

VI. Deliberate obfuscation of the type of goods

Parties may structure a transaction in a way to avoid alerting any suspicion to Financial Institutions or other third parties which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it. This activity may or may not involve a degree of collusion between the parties involved and may be for a variety reasons or purposes.

VII. Phantom shipping

No goods are shipped and all documentations are completely falsified.

VIII. Acquisition and sale of Intangibles

Global trade in services provides greater opportunities for money laundering than trade in merchandise because fraud is more difficult to detect and prove. The intangible nature of services makes supply difficult to determine. Unlike merchandise, services are less likely to be standard, so anomalies in value and price are less apparent and more difficult to substantiate.

IX. Shell and Front Companies

Both shell and front companies can be used to facilitate TBML but in different ways. A shell company has no real operating activities and is used to hide money laundering activity and the identities of individuals involved to obscure the money trail.

Free Trade Zones (FTZ)

FTZs are also emerging as being especially vulnerable to TBML. FATF defines FTZs as 'designated areas within countries that offer a free trade environment with a minimum level of regulation'

25.2 Sanctions

There are a variety of United Nations and national or regional sanctions in place. These include the following.

Country based financial sanctions that target specific individuals and entities.

Trade based sanctions i.e. embargoes on the provision of certain goods, services or expertise to certain countries.

26. The Role of the Bank in preventing Trade Based money laundering

On the basis of the International Chamber of Commerce (ICC) rules, banks deal with documents, not with goods. This principle is the basis for defining the degree of scrutiny and understanding a Financial Institution should have in identification of unusual activities involving trade finance transactions.

27. Risk Assessment

I. As per the Risk Based Approach, the Bank shall apply the Risk Based Approach to assess and manage the ML and TF risk in relation to Trade Finance activities.

II. As trade transactions may involve a number Financial Institutions, there is a responsibility lying upon these institutions to conduct due diligence on their respective customers. Therefore, the Bank will exercise due diligence on the correspondent Financial Institutions as per the Bank's Board approved AML policy in order to assess the ML/ TF risk associated with them.

III. In recent years there has been a series of UN Security Council Resolutions which have been issued targeting financial sanctions and/or activity based financial prohibitions in respect of certain countries and territories. Therefore, the Bank shall ensure that all transactions are monitored to verify that no UN, other

IV. International or local sanctions are breached. For this the Bank shall assess the ML/ TF risks associated with the countries before establishing trade transactions.

28. Application of Controls

The Bank shall exercise a higher level of control to prevent the banking system being abused by the criminals.

I. Due Diligence

The Bank shall not only perform Know Your Customer/ Due Diligence to identify the customers but also on all parties involved in the transactions who are not customers mentioned in the section 4 of this policy. This will be extended up to the correspondent banks as well.

II. Reviewing

All customer information shall be reviewed periodically or as and when necessary as mentioned in the section 8.1 of this policy. All correspondent bank information also shall be reviewed annually based on the Wolfsburg questionnaire in order to assess their ML/ TF risks.

III. Screening

All parties involved in the transactions including customers and Financial Institutions shall be screened prior to executing the transactions using the tool provided by the Bank, as mentioned in the section 2.1 of this policy. Further, all transactions are screened real-time using SWIFT screening tool for any breaches of international and local sanctions.

IV. Monitoring

All trade transactions are monitored using the automated financial crime detection system, in order to identify suspicious activities or potential unusual activities as mentioned in the section 9 of this policy.

V. Training and Awareness

The Bank provides training for specific staff to have a stronger awareness among the staff about the TB ML/ TF to have a robust AML/ CFT programme within the Bank related to trade finance transactions as mentioned in the section 15 of this policy.

Part VI - On-going Due Diligence

29. Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

30. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:

    a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
    b. Transactions which exceed the thresholds prescribed for specific categories of accounts.
    c. High account turnover inconsistent with the size of the balance maintained.
    d. Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

31. The extent of monitoring shall be aligned with the risk category of the customer.
Explanation: High risk accounts have to be subjected to more intensified monitoring.

    a. A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place. The system provides risk categorization on half-yearly basis, which will be verified by the officers.

32. Periodic Updation

Periodic updation shall be carried out annually for PEPs and high risk customers, once in every five years for medium risk customers and once in every seven years for low-risk customers as per prevailing norms at Head Office by adopting the most stringent regulation as per RBI norms.

a. Bank shall carry out

    i. In case of no change in the KYC information, with respect to their identities and addresses, a self-certification to that effect shall be obtained through customer's email-id registered with the Bank, customer's mobile number registered with the Bank.
    ii. In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Bank, customer's mobile number registered with the Bank, and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.
    iii. Further, the Bank has to obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation or within three months whichever is earlier.
    iv. In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Bank. Wherever required, Banks may carry out fresh KYC of such customers i.e., customers for whom account was opened when they were minor, on their becoming a major.

v. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Banks shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

vi. In case of Legal entities, Bank shall review the documents sought at the time of opening of account and obtain fresh certified copies. In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the Bank, letter from an official authorized by the LE in this regard, board resolution, etc. Further, the Bank shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

vii. In case of change in KYC information, bank shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

Provided, Bank shall ensure that KYC documents, as per extant requirements of the Master Direction on KYC issued by RBI, are available with them.

a. Bank may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

b. Bank shall ensure to provide acknowledgment with date of having performed KYC updation.

c. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

d. In case of existing business relationship which is not KYC compliant or KYC has not been updated as per prescribed periodicity, Bank shall temporarily cease operations in the account. However, before temporarily ceasing operations for an account, the Bank shall give the client two notices of 10 days each and within 30 days period the account should be made KYC compliant otherwise operations in the account shall be frozen. The account holders shall have the option, to revive their accounts by submitting the KYC documents.

The Bank shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the bank has expired at the time of periodic updation of KYC, The Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

The Bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the Bank.

33. In case of existing customers, Bank shall obtain the Permanent Account Number (PAN) or the equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or the equivalent e-document thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank shall give the client an accessible notice and a reasonable opportunity to be heard.

However, operations in accounts of customers who are unable to provide PAN or the equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes, may allowed to be continued. The Country Manager shall allow such relaxation for continuation of operations in such accounts till the time PAN or the equivalent e-document thereof or Form 60 is obtained from the customer for which an officer from the Chennai branch will be deputed to personally visit the customer for obtaining the PAN or the equivalent e-document thereof or Form 60. However, the Country Manager shall ensure that such accounts are subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a Bank gives in writing to the Bank that he does not want to submit his Permanent Account Number or the equivalent e-document thereof or Form No.60, Bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

Part VII - Enhanced and Simplified Due Diligence Procedure Enhanced Due Diligence

34. Any additional due diligence measures undertaken over and above the standard level of due diligence is termed as Enhanced Due Diligence. EDD can be applied at the product level or customer type level where the suspicion of money laundering or terrorist financing is high. Some of the parameters which can be used for enhanced due diligence are:

a) Customer location
b) Nature of business /occupation;
c) Transactions in line with the business activity / occupation;
d) Number and value of transaction;
e) Public domain checks for adverse media news on customer.

Indicative examples of what can constitute Enhanced Due Diligence

i. Obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment.

ii. Carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment.

iii. Verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime. Seeking additional information from the customer about the purpose and intended nature of the business relationship.

iv. Seeking additional information from the customer about the purpose and intended nature of the business relationship.

35. High Risk Customers

a. Politically Exposed Persons (PEPs)
b. Persons from countries that have inadequate measures for prevention of money laundering and financing of terrorism (High risk countries)
c. Customers not physically present for establishing business relationships and transactions
d. Customers who provide unsatisfactory information relating to CDD
e. Non-Governmental Organizations (NGOs) and Not-for-Profit Organizations or Charities
f. Any other customer and transaction that may be stipulated by the FIU.

36. Accounts of Politically Exposed Persons (PEPs)

Politically Exposed Persons are individuals who have been entrusted with prominent public functions by a foreign country, including the Heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. Bank shall gather sufficient information on any person / customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Bank shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members or close relatives of PEPs. The decision to open an account of a PEP as well as the decision to continue the business relationship in the event of an existing customer or relatives of an existing customer subsequently becoming Politically Exposed Person (PEP), shall be obtained from the Senior Management. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to PEPs including enhanced monitoring on an ongoing basis. PEPs, customers who are close relatives of PEPs and accounts where a PEP is the ultimate beneficial owner shall be categorized as 'High Risk' so that appropriate transaction alerts are generated, and the accounts are subjected to enhanced CDD on an ongoing basis. Bank shall have appropriate ongoing risk management systems for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner. The Risk and Compliance Department of Chennai Branch shall closely monitor PEP accounts on ongoing basis for identifying and applying enhanced CDD to PEPs.

The Bank shall have the option of establishing a relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

a. Bank have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;
b. Reasonable measures are taken by the bank for establishing the source of funds / wealth;
c. the approval to open an account for a PEP shall be obtained from the senior management;
d. all such accounts are subjected to enhanced monitoring on an on-going basis;

e. in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

B. These instructions shall also be applicable to family members or close associates of PEPs.

37. Procedure to be followed by banks while opening accounts of foreign students

a. Banks shall, at their option, open a Non-Resident Ordinary (NRO) bank account of a foreign student on the basis of his / her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

   (i) Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

   (ii) Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

b. The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA. 1999.

c. Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

Record Management

38. The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Bank shall,

a. Section 36 (b) of Record keeping requirement up to at least 06 years as per the section 4(1) a of Sri Lankan Transaction Reporting Act No 06 of 2026 as per Customer Due Diligence (CDD) Rule No 20 of the CDD Gazette No 1951/13 issued by CBSL on 27.01.2016 stated that "Every Financial Institutions shall ensure that foreign branches and majority-owned subsidiaries apply anti-money laundering and suspension of terrorist financing measures consistent with the domestic law requirements, where the relevant written laws of the relevant foreign country provide less stringent requirements than those provided for in the domestic law.

b. Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least six years after the business relationship is ended;

c. Make available swiftly the identification records and transaction data to the competent authorities upon request;

d. Maintain all necessary information in respect of transactions so as to permit reconstruction of individual transaction, including the following:

   (i) the nature of the transactions;

   (ii) the amount of the transaction and the currency in which it was denominated;

   (iii) the date on which the transaction was conducted; and

   (iv) the parties to the transaction.

e. Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
f. Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.
g. The Bank shall ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Bank shall register the details on the DARPAN Portal. Banks shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

Reporting Requirements to Financial Intelligence Unit – India

39. Bank shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof. Bank shall report Suspicious Transaction Report / Cash Transaction Report, using the formats published by FIU-IND.

40. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation.

41. Bank shall not put any restriction on operations in the accounts where an STR has been filed. Bank shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

42. Reports to be furnished to Financial Intelligence Unit – India

(1) Cash Transaction Report (CTR)

(i) Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- will not be reported in the Cash Transaction Report.

(ii) The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.

(2) Suspicious Transaction Reports (STR)

(i) While determining suspicious transactions, bank will be guided by the definition of "suspicious transaction" as contained in PMLA Rules as amended from time to time.

"Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

(ii) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. Bank will report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.

(iii) Bank to submit STRs if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iv) Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

(3) Transaction Monitoring

(i) For effective monitoring of transactions of the customers, Bank has implemented an AML system for generation of AML alerts on day to day basis based on the pre-defined scenarios, as advised by Indian Banks Association (IBA) / Financial Intelligence Unit – India (FIU-IND) from time to time. These scenarios will be periodically reviewed to make them more effective based on the feedback received and experience gained. In case any suspicious transaction is detected, the same be reported to Chief Compliance Officer for onward submission of Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) through FINnet Gateway after getting the approval of Principal Officer of the Bank.

Indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring, high & medium risk: customers/ products & services/ geographies/ locations/alerts for Chennai branch, are attached at Annexure-I.

(4) Counterfeit Currency Report (CCR)

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format by 15th of the succeeding month.

(5) Non-Profit Organizations Transaction report [NTR]

Bank will report all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

(6) **Cross-border Wire Transfer Report [CWTR]**

Bank will file Cross-Border Wire Transfer Report (CWTR) to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in

During analysis of alerts, special attention shall be given to alerts pertaining to Trade Based Money Laundering High Risk Customers, Politically Exposed Persons and High Value Transactions.

i. Any changes in KYC Policy may be implemented after approval of the Board.

Requirements / Obligations under International Agreements

Sanction Compliance

43. Bank shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, do not have any account in the name of individuals / entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:
The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida.

44. The "Taliban Sanctions List", established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban
The Bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Bank for meticulous compliance.
Details of accounts resembling any of the individuals / entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

45. In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions / entities from time to time shall also be taken note of.

46. The Bank has to screen customer names with UN List of terrorist individuals / entities from the AML system before creation of new CIF / opening of accounts. The Bank has to ensure that the name (s) of the proposed customer does not match with that of the UN list of Terrorist individuals / organization / entities, before opening any new account. The Compliance Department, Chennai Branch will also cross check the details of all existing accounts with the updated list. The Bank also has to verify transaction and ensure that no account is held by or linked to any of the entities or individuals included in the list maintained for this purpose. If the particulars of any of the account(s) have resemblance with those appearing in the list, bank has to verify transactions carried out in such accounts and report those accounts to RBI / Financial Intelligence Unit-INDIA apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

47. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)

a. Bank's shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

b. In accordance with paragraph 3 of the aforementioned Order, Bank shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

c. Further, Bank shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

d. In case of match in the above cases, bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. The Bank shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.
It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

e. Bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

f. In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, The Bank shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

g. In case an order to freeze assets under Section 12A is received by the REs from the CNO, Bank shall, without delay, take necessary action to comply with the Order.

h. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by bank along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

48. The Bank shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

48A. 108 In addition to the above, Bank shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

49. Freezing of Assets under of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated March 14, 2019 shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

i. The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

ii. Bank shall strictly follow the procedure laid down in the UAPA revised order dated February 2, 2021, in supersession of the earlier order dated March 14, 2019 (Annexure II of this policy) and ensure meticulous compliance with the Order issued by the Government.

iii. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

50. Jurisdictions that do not or insufficiently apply the FATF Recommendations

1. FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

2. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

   Explanation: The process referred to a & b do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

3. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank / other relevant authorities, on request.

Other Instructions

51. Secrecy Obligations and Sharing of Information

1. Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
2. While considering the requests for data / information from Government and other agencies, bank shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.
3. The exceptions to the said rule shall be as under:
   a. Where disclosure is under compulsion of law,
   b. Where there is a duty to the public to disclose,
   c. the interest of bank requires disclosure and
   d. Where the disclosure is made with the express or implied consent of the customer.
4. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

51A. Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010

Banks shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, banks shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

52. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

b) In terms of provision of Rule 9(1A) of the PML Rules, the Bank shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

c) Operational Guidelines for uploading the KYC data have been released by CERSAI.

d) Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

e) Once KYC Identifier is generated by CKYCR, Bank shall ensure that the same is communicated to the individual/LE as the case may be.

f) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

g) Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

h) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the bank, with an explicit consent to download records from CKYCR, then such bank shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –

i. there is a change in the information of the customer as existing in the records of CKYCR;
ii. the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
iii. the current address of the customer is required to be verified;
iv. the Banks considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.
v. the validity period of documents downloaded from CKYCR has lapsed.

Also, whenever the Bank obtains additional or updated information from any customer as per clause (i) to (v) above or Rule 9 (1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Bank regarding an update in the KYC record of an existing customer, the Bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Bank.

Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

53. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

i. Under FATCA and CRS, Bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:
   (a) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same.
   (b) Constitute a "Management Committee" under the Principal Officer or any other equivalent functionary to ensure compliance.

   (c) Ensure compliance with updated instructions / rules / guidance notes / Press releases / issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. Bank may take note of the following:
      (i) updated Guidance Note on F A T C A and CRS
      (ii) a press release on 'Closure of Financial Accounts' under Rule 114H (8).

ii. A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by bank.

The Operations Department, Chennai Branch shall be responsible for responsible for submission of report to Income Tax Department as per following directions:-

a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login

- -> My Account

--> Register as Reporting Financial Institution,

(b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) shall be referred to.

Explanation: Bank shall refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

54. Operation of Bank Accounts & Money Mules

The Bank shall strictly adhere to the Standard Operating Procedure (SOP) on opening of accounts and monitoring of transactions, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." The Bank shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed by the Bank, it shall then be deemed that the Bank has not complied with these directions. If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions. The SOP for identification of Money Mule Accounts is enclosed in Annexure XI.

55. Introduction of New Technologies Net Banking / RTGS / NEFT / ECS etc.

Adequate attention shall be paid by Bank to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products / services / technologies.

56. Correspondent Banking

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving cross-border correspondent banking and other similar relationships. In addition to performing normal CDD measures, such relationships shall be subject to the following conditions:

a. Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.

b. The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information.
c. Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.
d. Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved.
e. In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts of the correspondent bank and is undertaking on-going 'due diligence' on them.
f. The correspondent bank shall ensure that the respondent bank is able to provide the relevant CDD information immediately on request.
g. Correspondent relationship shall not be entered into or continued with a shell bank.
h. It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.
i. Banks shall be cautious of correspondent banking relationships with institutions located in jurisdictions, which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
j. Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

57. Wire transfer

Bank shall ensure the following while effecting wire transfer:

A. Information requirements for wire transfers for the purpose of this Master Direction

i. All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:

a. name of the originator;
b. the originator account number where such an account is used to process the transaction;
c. the originator's address, or national identity number, or customer identification number, or date and place of birth;
d. name of the beneficiary; and
e. the beneficiary account number where such an account is used to process the transaction.

In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

ii. In case of batch transfer, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate

originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

iii. Domestic wire transfer, where the originator is an account holder of the ordering bank, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.

iv. Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering bank, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering Bank and where the information accompanying the wire transfer can be made available to the beneficiary Bank and appropriate authorities by other means, it is sufficient for the ordering Bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

The ordering Bank shall make the information available within three working/business days of receiving the request from the intermediary Bank, beneficiary Bank, or from appropriate competent authorities.

v. Bank's shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement authorities, prosecuting / competent authorities as well as FIU-IND on receiving such requests with appropriate legal provisions.

vi. The wire transfer instructions are not intended to cover the following types of payments:

a. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated, financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact the obligation of the bank to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

B. Responsibilities of ordering bank, intermediary bank and beneficiary bank, effecting wire transfer, are as under

i. Ordering Bank

a. The ordering bank shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, contain required and accurate originator information and required beneficiary information, as indicated above.

b. Customer Identification shall be made if a customer, who is not an account holder of the ordering bank intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.

c. Ordering bank shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this section.

ii. Intermediary Bank

a. Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.

b. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary bank.

c. Intermediary bank shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

d. Intermediary bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iii. Beneficiary Bank

a. Beneficiary bank shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.

b. Beneficiary bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

C. Other Obligations

i. Obligations in respect of banks' engagement or involvement with unregulated entities in the process of wire transfer

Bank's shall be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the Bank's shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that,

i. there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;

ii. the agreement / arrangement, if any, with such unregulated entities by bank clearly stipulates the obligations under wire transfer instructions; and

iii. a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

ii. Banks' responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities)

Banks' are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, Bank shall ensure that they do not process cross-border transactions of designated persons and entities.

iii. Banks' responsibility to fulfil record management requirements

Complete originator and beneficiary information relating to wire transfers shall be preserved by the bank involved in the wire transfer, in accordance with Section 46 of the Master Direction.

The Legal Entity Identifier (LEI) will be applicable for domestic, cross border transactions undertaken by entities (non-individuals) for single payment exceeding INR 50 Crores. (Including both remitter and beneficiary)

58. Issue and Payment of Demand Drafts, etc.,

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/RTGS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.
Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank.

59. Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

60. Hiring of Employees and Employee training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/ hiring process shall be put in place.

(b) The Bank shall endeavor to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. Banks shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(c) On-going in house employee training programme on quarterly basis, shall be put in place so that the members of staff are adequately trained in KYC/ AML / CFT policy. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML / CFT policies of the Bank, regulation and related issues shall be ensured.

61. Accounts under Foreign Contribution Regulation Act, 2010 (FCRA)

RBI vide letter no: DOR.AML. No.1783/14.08.001/2020-21 dated December 09, 2020.RBI has informed that Ministry of Home Affairs (MHA), Government of India has issued gazette notification regarding the Foreign Contribution (Regulation) Amendment Act, 2020, The said amendment Act has been notified on September 28, 2020 and has been enforced from September 29, 2020 through notification of date.

In terms of the amended Section 17 of the above-mentioned amendment act, every person/ NGO/ association who have been granted FCRA certificate of registration under FCRA 2010 and prior permission to receive foreign contribution shall henceforth receive such contribution only in an account designated as "FCRA Account" in the specified branch (Main Branch) of State Bank of India (SBI) at New Delhi. No person/ NGO/ association shall receive foreign contributions received in accordance with the FCRA 2010 in any account other than the one designated as "FCRA Account" as per section 17(1) of the FCRA Act, 2010 in the specified branch, i.e., New Delhi Main Branch of the SBI, Sansad Marg, New Delhi, post opening of such an account.

In terms of section 46 of the Foreign Contribution (Regulation) Act, 2010, the MHA has advised to instruct all the scheduled banks to stop receiving/ crediting with effect from April 01, 2021 any foreign contributions in any account other than the "designated FCRA Account" in the aforesaid branch of the SBI at New Delhi, which has been opened by the person who has been granted certificate or prior permission under the FCRA, 2010. The period from September 29, 2020 till March 31, 2021 will be treated as transition period to facilitate opening of the designated "FCRA Account". However, Chennai Branch does not have any FCRA accounts as at date.

MHA has also clarified that the person/ NGO/ association would be free to retain their present account as "other FCRA Account" in any branch of a scheduled bank of their choice which they can link with the "designated FCRA Account" opened in the SBI, New Delhi Main Branch as specified by the Central Government. All foreign contributions shall be received only in the "designated FCRA Account" with the SBI from the date of opening of such account or April 01, 2021, whichever is earlier. All branches and offices to strict adherence to above guidelines of RBI.

The standard operating procedure for opening FCRA Account at the SBI, New Delhi Main Branch is available in Annexure XIV.

Annexure – I

Indicative List of Various Types of Indicators I.E. Customer Behavior and Risk Based Transaction Monitoring, High & Medium Risk: Customers/ Products & Services/ Geographies/ Locations/Alerts for Chennai Branch

1. Indicative List of Customer Behavior & Risk BasedTransaction Monitoring

i. Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.
ii. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
iii. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
iv. Customer giving confusing details about a transaction.
v. Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.
vi. Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits are unremarkable, but the total of all credits / debits is significant.
vii. Customer's representatives avoiding contact with the branch.
viii. Customers who repay the problem loans unexpectedly.
ix. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
x. Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
xi. Customer regularly issues large value cheques without balance and then deposits cash.

A. Transactions Involving Large Amounts of Cash

Exchanging an unusually large amount of small denomination notes for those of higher denomination;

i. Frequent withdrawal of large amounts by means of cheques,
ii. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
iii. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
iv. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;
v. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

B. Transactions that do not make Economic Sense

i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
ii. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

C. Activities not consistent with the Customer's Business

i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
ii. Corporate accounts where deposits & withdrawals by cheque / telegraphic transfers/foreign inward remittances any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.
iii. Unusual applications for DD/TT/PO against cash.
iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
v. Retail deposit of many cheques but rare withdrawals for daily operations.

D. Attempts to avoid Reporting/Record-keeping Requirements

i. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
ii. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
iii. An account where there are several cash deposits/withdrawals below a specified threshold level to an avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E. Unusual Activities

i. An account of a customer who does not reside/have office near the branch even though there are other bank branches near his residence/office.
ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
iii. Funds coming from the list of countries/centers, which are known for money laundering.

F. Customer who provides Insufficient or Suspicious Information

i. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
ii. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
iii. A customer who has no record of past or present employment but makes frequent large transactions.

G. Certain Suspicious Funds Transfer Activities

i. Sending or receiving frequent or large volumes of remittances to/from countries outside India.
ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

H. Certain Bank Employees arousing Suspicion

i. An employee whose lavish lifestyle cannot be supported by his or her salary.
ii. Negligence of employees/willful blindness is reported repeatedly.

I. Bank no longer knows the true identity

i. When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

J. Some examples of suspicious activities/transactions to be monitored by the operating staff-

i. Large Cash Transactions
ii. Multiple accounts under the same name
iii. Frequently converting large amounts of currency from small to large denomination notes
iv. Placing funds in term Deposits and using them as security for more loans.
v. Large deposits immediately followed by wire transfers.
vi. Sudden surge in activity level.
vii. Same funds being moved repeatedly among several accounts.
viii. Multiple deposits of money orders, Banker's cheques, drafts of third Parties
ix. Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
x. Cheques of third parties into the account followed by immediate cash withdrawals.
xi. Transactions inconsistent with the purpose of the account.
xii. Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

i. A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
ii. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
iii. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

iv. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
v. A customer experiences increased wire activity when previously there has been no regular wire activity.
vi. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
vii. A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
viii. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
ix. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
x. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
xi. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
xii. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
xiii. Periodic wire transfers from a person's account/s to Bank haven countries.
xiv. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
xv. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques.
xvi. A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when
xvii. The amount is very large (say over Rs. 10 Lakh)
- The amount is just under a specified threshold.
- The funds come from a foreign country or
- Such transactions occur repeatedly.

xviii. A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)
xix. A non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

2. Indicative List of High-Risk Customers

i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.
ii. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities
iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations
iv. Customers with dubious reputation as per public information locally available or commercially available.
v. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
vi. 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 etc.
vii. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.
viii. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
ix. Non-resident customers and foreign nationals
x. Accounts of Embassies / Consulates;
xi. Off-shore (foreign) corporation/business
xii. Non face-to-face customers
xiii. High net worth individuals [HNIs]
xiv. Firms with 'sleeping partners'
xv. Companies having close family shareholding or beneficial ownership
xvi. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale

3. Indicative List of Medium Risk Customers

i. Non-Bank Financial Institution
ii. Import / Export
iii. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
iv. Sole Practitioners or Law Firms (small, little known)
v. Notaries (small, little known)
vi. Secretarial Firms (small, little known)
vii. Accountants (small, little known firms)
viii. Venture capital companies

4. List of High / Medium Risk Products & Services

i. Foreign correspondent accounts
ii. Trade finance (such as letters of credit)
iii. Lending activities, particularly loans secured by cash collateral and marketable securities
iv. Provision of safe custody and safety deposit boxes
v. Trade finance services and transactions involving high-risk jurisdictions

Indicative List of High / Medium Risk Geographies/ Locations/ Countries
Countries/Jurisdictions

i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions ("UNSCR").
ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf- gafi.org)
iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
v. Countries identified by credible sources 1 as lacking appropriate AML/CFT laws, regulations and other measures.
vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
vii. Countries identified by credible sources as having significant levels of criminal activity.
viii. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

5. Indicative List of High Risk Countries

The countries identified by Financial Action Task Force [FATF] as high-risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.

Annexure II

File No. 14014/01/2019/CFT
Government of India
Ministry of Home Affairs
CTCR Division
North Block, New Delhi.
Dated: the 2nd February, 2021
(Amended vide corrigendum dated March 15, 2023)
(Amended vide corrigendum dated August 29, 2023)

ORDER

Subject: - Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) reads as under: -

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to —

a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

c) prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism". The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under: - "Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

2. In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:

3. Appointment and communication details of the UAPA Nodal Officers:

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA [Telephone Number: 011- 23093124, 011- 230923465 (Fax), email address: jsctcr-mha@gov.in]

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.3 All the States and UTs shall appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.4 The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.

3.5The Financial Regulators shall forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies. 3.7 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the consolidated list of UAPA Nodal Officers to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs.

4. Communication of the list of designated individuals/entities

4.1 The Ministry of External Affairs shall update the list of individuals and entities subject to the UN sanction measures whenever changes are made in the lists by the UNSC 1267 Committee pertaining to Al Qaida and Da'esh and the UNSC 1988 Committee pertaining to Taliban. On such revisions, the Ministry of External Affairs would electronically forward the changes without delay to the designated Nodal Officers in the Ministry of Corporate Affairs, CBIC, Financial Regulators, FIU–IND, CTCR Division and Foreigners Division in MHA.

4.2 The Financial Regulators shall forward the list of designated persons as mentioned in Para 4(i) above, without delay to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies.

4.3 The Central [designated] Nodal Officer for the UAPA shall forward the designated list as mentioned in Para 4(i) above, to all the UAPA Nodal Officers of States/UTs without delay.

4.4 The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 4(i) above, to the immigration authorities and security agencies without delay.

4.5 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the list of designated persons as mentioned in Para 4(i) above, to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs without delay.

5. Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc.

5.1 The Financial Regulators will issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by the SEBI and insurance companies requiring them –

(i) To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks, Insurance policies etc., with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., held by such customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

(iii) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in 5.1 (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and to Regulators and FIU-IND, as the case may be, without delay.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall prevent such designated persons from conducting financial transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No.011-23092551 and also convey over telephone No.011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI, and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts, covered under Paragraph 5.1(ii) above, carried through or attempted as per the prescribed format.

5.2 On receipt of the particulars, as referred to in Paragraph 5 (i) above, the Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks, stock exchanges/ depositories, intermediaries and insurance companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars

5.3 In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an orders to freeze these assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer for the UAPA without delay and conveyed electronically to the concerned bank branch, depository and insurance company under intimation to respective Regulators and FIU-IND. The Central [designated] nodal officer for the UAPA shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and all UAPA nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The Central [designated] Nodal Officer for the UAPA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967. The order shall be issued without prior notice to the designated individual/entity.

6. Regarding financial assets or economic resources of the nature of immovable properties

6.1 The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction, without delay.

6.2 In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Central [designated] Nodal Officer for the UAPA without delay at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post would necessarily be conveyed on email id: jsctcr-mha@gov.in.

6.3 The UAPA Nodal Officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.

6.4 The Central [designated] Nodal Officer for the UAPA may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

6.5 In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be issued by the Central [designated] Nodal Officer for the UAPA without delay and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT. The order shall be issued without prior notice to the designated individual/entity.

6.6 Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The UAPA Nodal Officer of the State/UT shall, upon becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

7. Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and other Designated Non-Financial Businesses and Professions (DNFBPs) and any other person

(i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.
(a) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above. Further, if the dealers hold any assets or funds of the designated individual/entity, either directly or indirectly, they shall freeze the same without delay and inform the UAPA Nodal officer of the State/UT.

(ii) The CBIC shall advise the dealers of precious metals/stones (DPMS) that if any designated individual/entity approaches them for sale/purchase of precious metals/stones or attempts to undertake such transactions the dealer should not carry out such transaction and without delay inform the CBIC, who in turn follow the similar procedure as laid down in the paragraphs 6.2 to 6.5 above.

(iii) The UAPA Nodal Officer of the State/UT shall advise the Registrar of Societies/ Firms/ non-profit organizations that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar should inform the UAPA Nodal Officer of the State/UT without delay, who will, in turn, follow the procedure as laid down in the paragraphs 6.2 to 6.5 above. The Registrar should also be advised that no societies/ firms/ non-profit organizations should be allowed to be registered, if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and in case such request is received, then the Registrar shall inform the UAPA Nodal Officer of the concerned State/UT without delay, who will, in turn, follow the procedure laid down in the paragraphs 6.2 to 6.5 above.

(iv) The UAPA Nodal Officer of the State/UT shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino and/ or if any assets of such designated individual/ entity is with the Casino operator, and of the particulars of any client matches with the particulars of designated individuals/ entities, the

Casino owner shall inform the UAPA Nodal Officer of the State/UT without delay, who shall in turn follow the procedure laid down in paragraph 6.2 to 6.5 above.

(v) The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) requesting them to sensitize their respective members to the provisions of Section 51A of UAPA, so that if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of Designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(vi) The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited liability firm, partnership firm, society, trust, association where any of designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(vii) In addition, the member of the ICSI be sensitized that if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person then the member should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(viii) The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraph 8 to 10 above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms.

Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

(ix) Any person, either directly or indirectly, holding any funds or other assets of designated individuals or entities, shall, without delay and without prior notice, cause to freeze any transaction in relation to such funds or assets, by immediately informing the nearest Police Station, which shall, in turn, inform the concerned UAPA Nodal Officer of the State/UT along with the details of the funds/assets held. The concerned UAPA Nodal Officer of the State/UT, would follow the same procedure as in para 6.2 to 6.6 above.

8. Regarding implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001

8.1 The U.N. Security Council Resolution No.1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; 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 and entities, including funds or other assets derived or generated from property owned

or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

8.2 To give effect to the requests of foreign countries under the U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.

8.3 The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officers in Regulators, FIU-IND and to the Nodal Officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

9. Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs 5 and 6 above shall be followed. The freezing orders shall be issued without prior notice to the designated persons involved.

10. Regarding exemption, to be granted to the above orders in accordance with UNSCR 1452.
10.1 The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the Central [designated] nodal officer of the UAPA to be:- (a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification; (b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA;

10.2. The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 10 of: (a) interest or other earnings due on those accounts, or (b) payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of resolutions 1267 (1999), 1333 (2000), or 1390 (2002), Provided that any such interest, other earnings and payments continue to be subject to those provisions;
10.3 (a): The designated individual or organization may submit a request to the Central [Designated] Nodal Officer for UAPA under the provisions of Para 10.1 above. The Central [Designated] Nodal Officer for UAPA may be approached by post at "Additional Secretary (CTCR), North Block, New Delhi – 110001" or through email to jsctcr-mha@gov.in"
(b): The Central [Designated] Nodal Officer for UAPA shall examine such requests, in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and, if accepted, communicate the same, if applicable, to the Ministry of External Affairs, Government of India for notifying the committee established pursuant to UNSC Resolution 1267 (1999) of the intention to authorize, access to such funds, assets or resources in terms of Para 10.1 above.

11. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person:

11.1 Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets

or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officers of State/UT.

11.2 The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the State/ UT Nodal Officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Central [designated] Nodal Officer for the UAPA as per the contact details given in Paragraph 3.1 above, within two working days.

11.3 The Central [designated] Nodal Officer for the UAPA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he/she shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officer of State/UT. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Central [designated] Nodal Officer for the UAPA shall inform the applicant expeditiously.

11A. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals / organisations in the event of delisting by the UNSCR 1267 (1999), 1988 (2011) and 1989 (2011) Committee Upon making an application in writing by the concerned individual / organization, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs., who in turn shall forward the application along with the full details of the assets frozen to the Central [Designated] Nodal Officer for UAPA within two working days. The Central [Designated] Nodal Officer for UAPA shall examine the request in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and cause such verification as may be required and if satisfied, shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services owned or held by the applicant under intimation to concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs.

12. Regarding prevention of entry into or transit through India:

12.1 As regards prevention of entry into or transit through India of the designated individuals, the UAPA Nodal Officer in the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

12.2 The immigration authorities shall ensure strict compliance of the order and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the UAPA Nodal Officer in Foreigners Division of MHA.

13. Procedure for communication of compliance of action taken under Section 51A: The Central [designated] Nodal Officer for the UAPA and the Nodal Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

14. Communication of the Order issued under Section 51A of Unlawful Activities (Prevention) Act, 1967: The order issued under Section 51A of the Unlawful Activities (Prevention) Act, 1967 by the Central [designated] Nodal Officer for the UAPA relating to funds, financial assets or economic resources or related services, shall be communicated to all the UAPA nodal officers in the country, the Regulators of Financial Services, FIU-IND and DNFBPs, banks, depositories/stock exchanges, intermediaries regulated by SEBI, Registrars performing the work of registering immovable properties through the UAPA Nodal Officer of the State/UT.

15. All concerned are requested to ensure strict compliance of this order.

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

To,

1) Governor, Reserve Bank of India, Mumbai

2) Chairman, Securities & Exchange Board of India, Mumbai

3) Chairman, Insurance Regulatory and Development Authority, Hyderabad.

4) Foreign Secretary, Ministry of External Affairs, New Delhi.

5) Finance Secretary, Ministry of Finance, New Delhi.

6) Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.

7) Secretary, Ministry of Corporate Affairs, New Delhi

8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.

9) Director, Intelligence Bureau, New Delhi.

10) Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi. 11) Chief Secretaries of all States/Union Territories

12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories

13) Directors General of Police of all States & Union Territories

14) Director General of Police, National Investigation Agency, New Delhi.

15) Commissioner of Police, Delhi. 16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi

16) Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.

18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi. 19) Director (FIU-IND), New Delhi. Copy for information to: - 1. Sr. PPS to HS 2. PS to SS (IS)

Annexure - III

Money Laundering and Terrorist Financing Risk Assessment

Sl. No.	Parameters	Particulars
1.	**Risk Assessment**	A risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which bank business is exposed. Based on the assessment, ML/TF risks should be classified as low, medium and high impact risks. **While assessing the risks, following factors should be considered:** The nature, scale, diversity and complexity of their business; Target markets; The number of customers already identified as high risk; The jurisdictions the entity is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organized crime, and/or deficient AML/CFT controls and listed by RBI or FATF; The distribution channels, including the extent to which the entity deals directly with the customer or relies third parties to conduct CDD; The internal audit and regulatory findings; The volume and size of its transaction. The risk assessment should be approved by senior management.
2.	**Analysis of ML/TF threats and vulnerabilities**	In the context of money laundering/terrorist financing (ML/TF), risk means: **At the National level:** threats and vulnerabilities presented by ML/TF that put at risk the integrity of India's financial system. **At the Reporting Entity level:** threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF. Threats: this could be a person (or group), object that could cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups. **Vulnerabilities:** elements of a business that could be exploited by the identified threat. In the ML/TF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.
3.	**Risk Mitigation**	To develop and implement policies and procedures to mitigate the ML/TF risks should be identified through individual risk assessment: Customer due diligence (CDD) processes should be designed to understand the customers; Gather information on what they do and why they require financial services; To assess the ML/TF risk associated with a proposed business relationship; Determine the level of CDD to be applied and deter persons from establishing a business relationship to conduct illicit activity.
4.	**CDD Procedures**	Identifying the customer and, where applicable, the customer's beneficial owner; Verifying the customer's identity on the basis of reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework; Understanding the purpose and intended nature of the business

		relationship; To take measures to comply with national and international sanctions legislation by screening the customer's and beneficial owner's names against the UN and other relevant sanctions lists; The CDD procedures and policies should suitably include checkpoints with respect to ML and TF.
5.	Risk Categorization	The risk classification of the customer should also be done based on the CDD carried out. In case of medium or high-risk customers, or unusual transactions, the entities should also carry out transaction due diligence to identify source and application of funds, beneficiary of the transaction, purpose etc. Bank should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers.
6.	Monitoring of Transactions	**Monitoring in high risk situations:** daily transaction monitoring, manual transaction monitoring, frequent analysis of information, considering the destination of funds, establishment of red flags based on typologies reports, reporting of monitoring results to senior management etc. **Monitoring in lower risk situations:** thresholds, low frequency, automated systems
7.	Reporting	The Banks have the ability to flag unusual movement of funds or transactions for further analysis. Funds or transactions that are suspicious should be reported promptly to the Financial Intelligence Unit (FIU) and in the manner specified by the authorities.
8.	Internal Control	Adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated and there are controls to test the overall effectiveness of the BANK's policies and processes to identify, assess and monitor risk.
9.	Governance	The successful implementation and effective operation of a Risk Based Approach to AML/CFT depends on strong senior management leadership and oversight of the development and implementation of the RBA across the functions. **Senior Management should consider various ways to support AML/CFT initiatives:** To promote compliance as a core value of the Bank by sending a clear message that the Bank will not enter into, or maintain, business relationships that are associated with excessive ML/TF risks which cannot be mitigated effectively. Senior management, together with the board, are responsible for setting up robust risk management and controls adapted to the Bank stated, sound risk-taking policy; Implement adequate mechanisms of internal communication related to the actual or potential ML/TF risks faced by the Bank; Decide on the measures needed to mitigate the ML/TF risks identified. **Steps taken by Senior Management to promote compliance:** To carry out product development and commercial campaigns in

		strict compliance with national AML/CFT legislation. To involve senior management in AML/CFT training of staff.
10.	**Training and Awareness**	The effective application of AML/CFT policies and procedures depends on staff within Bank understanding not only the processes they are required to follow but also the risks these processes are designed to mitigate, as well as the possible consequences of those risks. It is therefore important that Banks staff receive AML/CFT training, which should be: **Of high quality**, relevant to the Banks ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls; **Obligatory** for all relevant staff; **Tailored** to particular lines of business within the Bank equipping staff with a sound understanding of specialized ML/TF risks they are likely to face and their obligations in relation to those risks; **Effective:** training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the Bank AML/CFT controls; **Ongoing:** AML/CFT training should be regular, relevant, and not be a one-off exercise when staff are hired; **Complemented** by AML/CFT information and updates that are disseminated to relevant staff as appropriate. Overall, the training should also seek to build up a working behavior where compliance is embedded in the activities and decisions of all Bank staff.
11.	**Assessment of Controls**	Bank should take steps to be satisfied that their AML/CFT policies and controls are adhered to and effective. **INTERNAL CONTROLS TO ENCOURAGE COMPLIANCE:** **1) Facilitate the reporting of suspicious transactions:** Set up staff training on mechanisms to adequately detect unusual transactions; Establish adequate channels to allow staff to report unusual transactions to the Compliance Officer; Ensure confidentiality to staff reporting suspicious transactions **2)Allow staff to report areas of policy or controls they find unclear/unhelpful/ineffective:** Establish ongoing consultation channels for staff concerning AML/CFT issues; Ensure consistency of the answers given to staff questions concerning AML/CFT issues; Conduct AML/CFT activities in such a way that they are perceived by all staff as a support to the quality of the Bank services provided to clients and the integrity of the Bank.
12.	**Reporting to Board of Directors**	Chennai Branch should report through the Country Manager to the Assistant General Manager(Overseas Manager), Deputy General Manager (International, Treasury and Investment), Chief Risk Officer, General Manager and Board of Directors.

Annexure IV – Ultimate Beneficial Owner

Beneficial owner

A natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a person or a legal arrangement

Beneficiary

The person to whom or for whose benefit the funds are sent, in relation to wire transfers or value transfers.

1. Ultimate Beneficial Owner of a Natural person

a. When a customer acts on behalf of another person, that another person is the Beneficial Owner of a natural person Ex. Mr. X is conducting transactions on behalf of Mr. B. Then Mr. B is the beneficial owner of Mr.X

b. When there are persons who receive benefits from the properties of a customer, that persons are the beneficial owners of a natural person Ex. Mr. X is the registered owner of 'A' factory. But his son Mr. Y is the person who started and carrying on the business. Then, Mr. Y is the beneficial owner of Mr. X's business

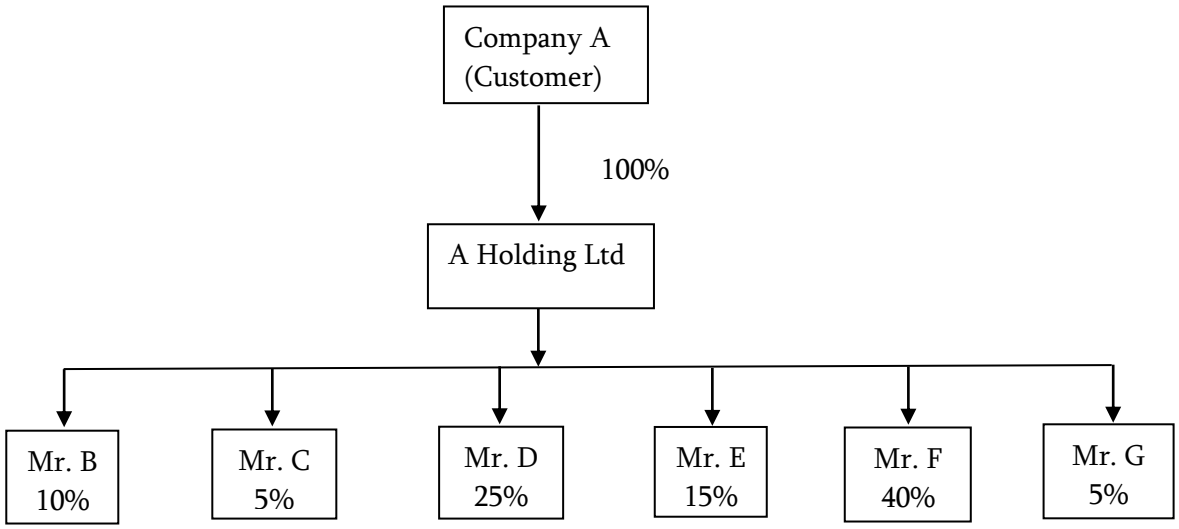
2. Ultimate Beneficial Owner of a Legal Person Legal Person Any entity other than a natural person which able to establish a permanent customer relationship with the Bank: a company, a body corporate, a foundation, a partnership, an association etc.

Steps of Identification of Ultimate Beneficial Owners of a Legal person

1. Natural person/s who owns or controls equal or more than ten percent (10%) of the customer's equity (Ownership)
2. Natural person who has effective control (Effective Control) identify through the understanding the governing structure of the legal person.
3. On behalf of which natural person/s the transactions are being conducted

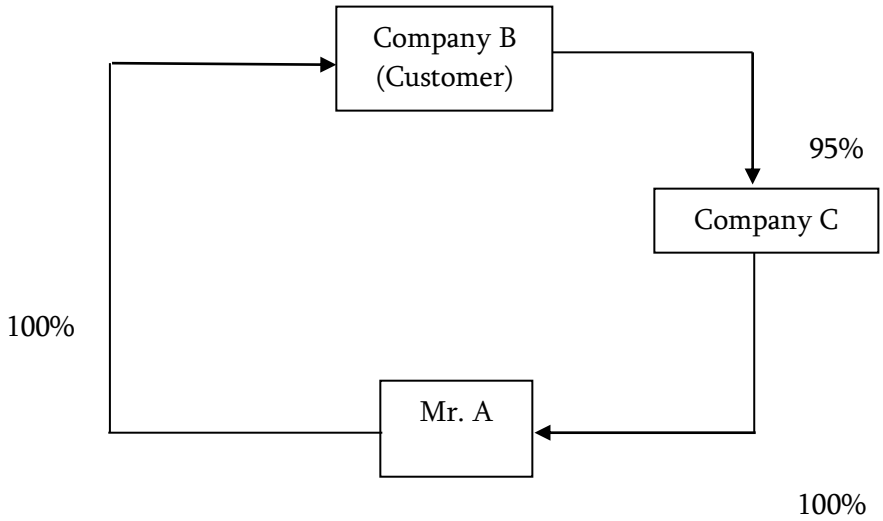
IDENTIFICATION OF BENEFICIAL OWNERSHIP

1. **Figure I – Simple Indirect Shareholding**



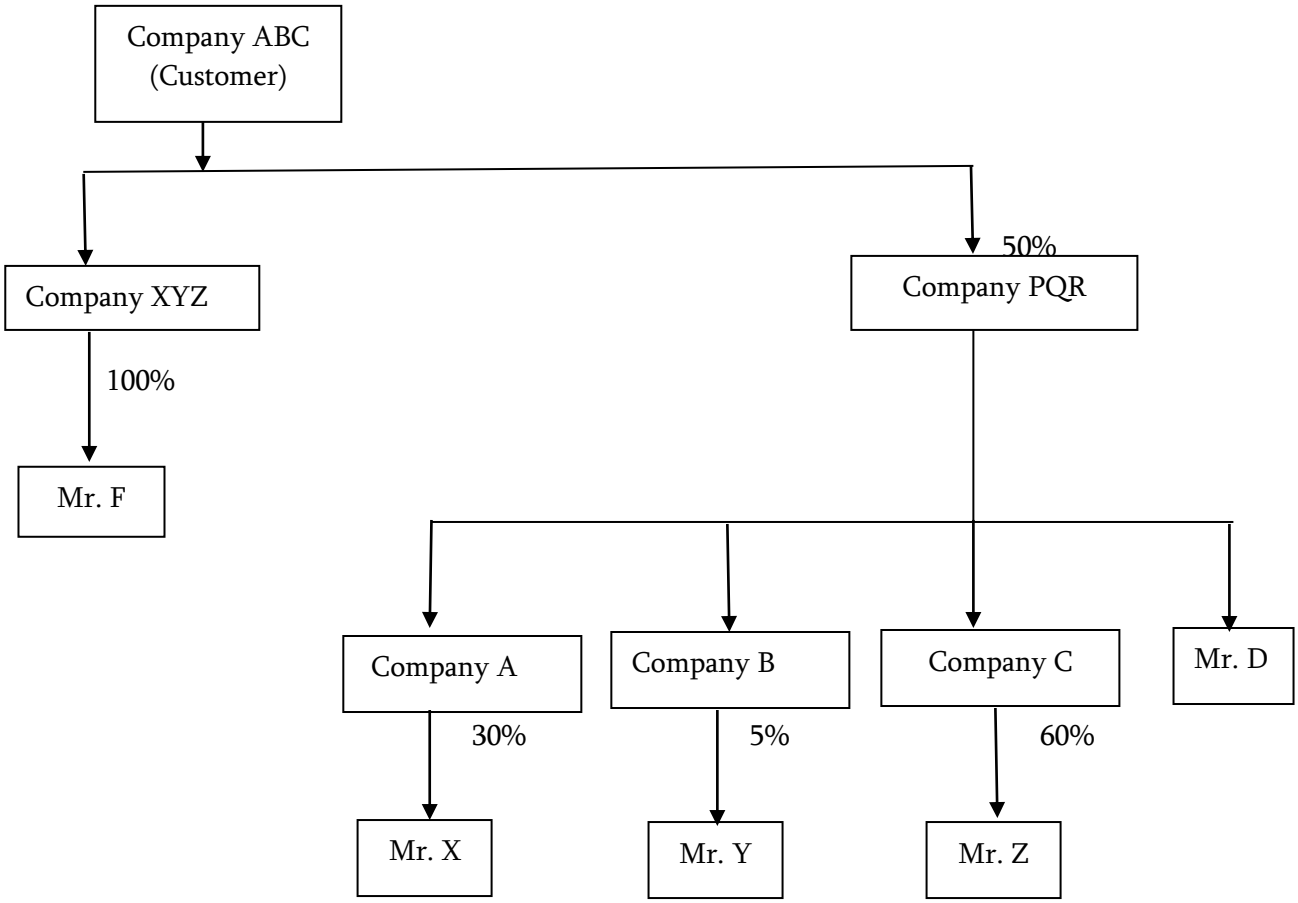
Mr. B, Mr. D, Mr. E and Mr. F are beneficial owners of the Company A.

Figure II – Direct and Indirect Share Holdings



Mr. A is the sole beneficial owner of Company B (Direct 5% + Indirect 95%).

Figure III – Multi-level Indirect Share Holdings



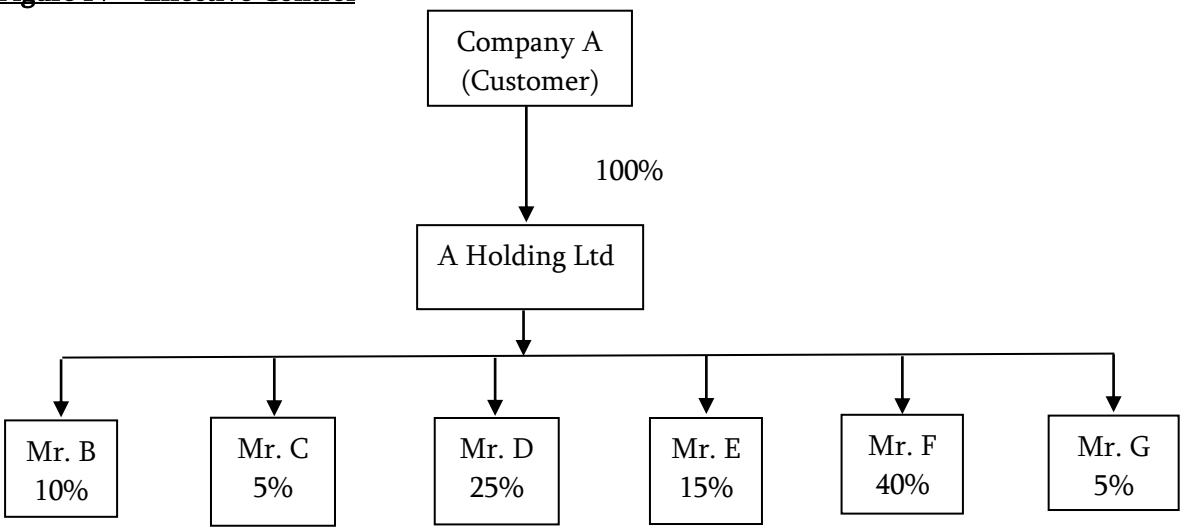
Mr. F, Mr. X and Mr. Z are beneficial owners of Company ABC through indirect shareholding.

2. Effective Control

1. For some customers, ownership may be spread over a large number of individuals with all individual owing less than ten percent (10%). In such instance, the effective control would be more appropriate to determine the beneficial ownership.
2. Effective control can be direct or indirect, formal or informal. At the direct and formal level, it is essential to understand the customer's governance structure in identifying the natural persons that exercise effective control over the customer.
3. In deciding effective control of a customer, following should be considered
   a. natural person who can hire or terminate a member of senior level management,
   b. natural person who can appoint or dismiss Directors,
   c. senior managers who have control over daily/regular operations of the legal person/arrangement (e.g., a CEO, CFO or a Managing Director).

d. A natural person who can control the legal person by;
   i. Personal connections to persons such as Chief Executive Officer / Chief Financial Officer/Managing Director or that possess ownership.
   ii. Significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person.
   iii. Control without ownership participating in the financial of the enterprise, or by the way of close family relationships, historical or contractual associations, or if a company/legal person defaults on certain payments.
   iv. Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised.

Figure IV – Effective Control



Mr. G is the managing director of the ABC Bank, which is the main financing source of the company A. In such situation, even if Mr. G hold less than ten percent (10%) of company A, he has effective control over the company A, through ABC Bank and should be considered as a beneficial owner through effective control.

3. Ways in which beneficial ownership information can be hidden / obscured

a. Use of shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,
b. Complex ownership and control structures involving many layers of ownership
c. Sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions,
d. Bearer shares and bearer share warrants.
e. use of legal persons as directors,
f. formal nominee shareholders and directors where the identity of the nominator is undisclosed,
g. informal nominee shareholders and directors, such as close associates and family,
h. trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,
i. use of intermediaries in forming legal person, including professional intermediaries such as accountants, lawyers, notaries, trust and company service providers.

4. Periodic review of beneficial ownership

Any material/significant change in customer circumstances may necessitate a review of beneficial ownership. Material/significant changes can be include following among other changes;

a. public company is taken private
b. a shareholder or group of shareholders takes effective control of voting shares
c. a new partner is added, of an existing partner is removed
d. change in management positions;
e. new trustees are appointed;
f. a trust is dissolved
g. a new account is opened for the same customer
h. transactions are attempted that are inconsistent with the customer's profile.

DECLARATION OF BENEFICIAL OWNERSHIP

This form has been issued under the Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 issued in terms of the Section 2(3) of the Financial Transactions Reporting Act No 6 of 2006. This form, or an approved equivalent, is required to be completed by customers of financial institutions designated under the Act to the best of their knowledge. The original completed and signed and witnessed version of this form must be retained by the financial institution and available to the competent authorities upon request.

Details of the natural person/ legal person/ legal arrangement, to whom account opened

Name	
Address	
Account No.	
Identification/ Registration No.	
In case of a natural person: Designation	
In case of a Trust: Name of Trustee & Trust Deed No.	

Details of declarant (natural person authorized to act on behalf of the above mentioned natural person/ legal person/ legal arrangement)

Name	
Identification No. (NIC, Passport, etc.)	
Date of birth	
Designation	

I declare that I am:

☐ The/a ultimate beneficial owner[1] of the afore said account,

☐ Not the ultimate beneficial owner of the afore said account,

and details of all ultimate beneficial owners,

That own or control 10% or more of the entity's equity,

On whose behalf the account is being operated,

Who exercises effective control are specified below.

UBO 1

Name :…….

Current address :……..

Identification document No :…… Country of issue: ……

Citizenship :…… PEP[2] status: Yes / No

Date of birth :……..

Source of Beneficial Ownership: ☐ Equity (……. %)
☐ Person on whose behalf the account is being operated
☐ Effective control

UBO 2
Name :……
Current address :……
Identification document No :…… Country of issue :……
Citizenship :…… PEP status : Yes / No
Date of birth :……..
Source of Beneficial Ownership: ☐ Equity (……. %)
☐ Person on whose behalf the account is being operated
☐ Effective control

UBO 3
Name :……
Current address :……
Identification document No :…… Country of issue :……...
Citizenship :…… PEP status: Yes / No
Date of birth:……..
Source of Beneficial Ownership: ☐ Equity (……. %)
☐ Person on whose behalf the account is being operated
☐ Effective control

UBO 4
Name :……
Current address :……
Identification document No :…… Country of issue :……
Citizenship :…… PEP status : Yes / No
Date of birth :……..
Source of Beneficial Ownership: ☐ Equity (……. %)
☐ Person on whose behalf the account is being operated
☐ Effective control

UBO 5
Name :……...
Current address :……..
Identification document No :…… Country of issue :……
Citizenship :…… PEP status : Yes / No
Date of birth :……..
Source of Beneficial Ownership: ☐ Equity (……. %)
☐ Person on whose behalf the account is being operated
☐ Effective control

UBO 6
Name :……...
Current address :……
Identification document No :…… Country of issue :……
Citizenship :…… PEP status : Yes / No
Date of birth :……..
Source of Beneficial Ownership: ☐ Equity (……. %)

☐ Person on whose behalf the account is being operated ☐ Effective control	
I attest the veracity of all information herein. …… Date	…….. Signature and the seal of the Declarant
For Office Use Only	
I have carefully examined the above information together with the relevant documents submitted by the customer and satisfied myself that the said information and documents are in conformity with the Internal Policies &circulars of the Bank. Further I attest that I have identified the Customer whose signature is on this form and have witnessed the same.	
Name	
PF No.	
Date	
Signature & Seal	

1 A natural person who ultimately owns or control a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a person or a legal arrangement.

2 An individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and their immediate family members/ close associates.

Annexure V

Risk Categorization of customers based on various parameters

Basis	High Risk	Medium Risk	Low Risk
Type of Customer	(i) Private Ltd., Company (ii) Public Ltd Company (Closely held) (iii) Trusts (iv) Charities (v) NRIs having aggregate deposit of Rs.50 lakhs & above (vi) Politically Exposed Persons (vii) Non-Face to face customers with aggregate deposit of Rs.10 lakhs and above. (viii) Customers having adverse publicity. NRIs of Indian Origin. (ix) Firms with operative transactions authorized by sleeping partner.	(i) Public Ltd companies (widely held) (ii) NRIs with balance of Rs.25 lakhs and above, but < Rs.50 lakhs. (iii) Firms with sleeping partners.	(i) Salaried persons. (ii) Pensioners (iii) Professional & Self-employed persons. (iv) Agriculturist (v) Self Help Groups (vi)Government companies. (vii) Public Sector companies. (viii) Government Departments. (ix) NRIs with balance of less than Rs.25 lakhs and below.
Source (Nationality) of funds	Foreign Remittances from national of Gulf, Pakistan, Afghanistan, Libya and Syria	Foreign Remittance from national of Eastern Block Countries, Indonesia, Burma, Malaysia, Singapore and Thailand	Foreign Remittance nationals of United States and European Countries. Foreign Remittances from NRIs & persons of Indian origin.

	One-time transaction Rs. 1 lac and above (cash.) Rs.5 lac and above (non cash)	One-time transaction Rs. 20,000 and above but below 1 lac cash Rs.1 lac and above but less than Rs.5 lacs non cash	One time transaction Less than Rs. 20,000/- Cash Less than Rs.1 lacs non cash
Location of Customer	Developing Countries, African Countries, South American Countries	Asian Countries, Russia and China	United States and European Countries

Business Activity	(1) Jewellery (2) Chit Funds (3) Finance Companies (4) Foreign Exchange, Money Market Brokers (5) Travel Agencies (6) Export / Import Trade (7) SMEs with annual turnover exceeding Rs. 25 Crores and above	(i)Commodity Trade (ii) SMEs with annual turnover Rs. 10 Crores and above, but < Rs.25 Crores	(i) Industry (ii) Hotel (iii) Plantations (iv) SMEs with turnover less than Rs. 10 Crores. (v) Retail Trade
Composition of partners directors	Entirely Foreign nationality	A mix of Indian and Foreign nationals	Exclusively Indian nationals
Quantum of Transaction	Cash transaction of Rs. 5 lac and above Non cash transactions of Rs.10 lacs and above	Cash transaction of Rs. 1 lac & above but less than 5 lacs. Non cash transactions of Rs.2 lacs & above but below Rs.10 lac	Cash transactions less than Rs. 1 lac Non cash transactions Less than Rs.2.00 lacs

The following parameters are some of the indicative parameters of risk categorization

1. Customer Constitution: Individual, proprietorship, partnership, private limited etc.
2. Business segment: Retail, Corporate etc.
3. Country of residence/Nationality: Whether India or any overseas location/Indian or foreign national
4. Product subscription: Salary account, NRI products etc.
5. Economic Profile: HNI, public ltd company etc.
6. Account Status: Active, inoperative, dormant etc.
7. Account vintage: Less than six months old etc.
8. Presence in regulatory negative/PEP/defaulter/fraudster lists
9. Suspicious Transaction Report (STR) filed for the customer
10. AML Alerts

Customer Risk Categorization

For categorizing a customer as Low Risk, Medium Risk and High Risk, the parameters considered are customer 's identity, social/financial status, nature of business activity, mode of payments, volume of turnover, information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Low Risk Customers

Individuals (other than High Net worth) and entities whose identities and sources of income can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as

Low Risk customers, such as:

a. Salaried employees
b. People belonging to lower economic strata of the society
c. Government Departments
d. Government owned companies
e. Regulatory and Statutory bodies, etc.
f. Senior Citizens and Self Help Groups
g. Illiterate individuals
h. For the above category, the KYC requirements of proper identification and verification of proof of address would suffice.

Updating KYC of Low Risk Customers: Every 7 years. (as per Host Country Regulation)

Medium Risk Customers

Customers who are likely to pose a higher-than-average risk to the Bank should be categorized as medium or high risk. For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his/her client profile, etc. besides proper identification.

The following customers are classified as Medium Risk Customers:

1. Gas Dealers
2. Car/boat/plane dealers
3. Electronics (wholesale)
4. Travel agency, Telemarketers, Telecommunication service providers

5. Pawnshops, Auctioneers, Restaurants, Retail shops, Movie theatres
6. Sole practitioners
7. Notaries
8. Accountants – Blind
9. Purdanashin

Updating KYC of Medium Risk Customers: Every 5 years. (as per Host Country Regulations)

High Risk Customers

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Bank shall subject such accounts to enhanced monitoring on an ongoing basis.

1. Trusts, charities, NGOs and organizations receiving donations.
2. Associations/Clubs
3. Companies having close family shareholding or beneficial ownership - Firms with sleeping partners '.
4. Accounts under Foreign Contribution Regulation Act.
5. Politically Exposed Persons (PEPs).
6. Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
7. Those with dubious reputation as per public information available. - Accounts of non-face-to-face customers.
8. High Net worth Individuals*
9. Non-Resident customers.
10. Foreign Nationals
11. Embassies/Consulates
12. Complex business ownership
13. United Nations or its agencies
14. Import & Export
15. Hindu Undivided Family (HUF)
16. Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) & jewellers.

Updating KYC of High Risk Customers: Once a year (As per Host Country Regulations)

* Parameters defining High Net worth Individuals (HNIs)

Customers with any of the following shall be treated as High Net worth Individuals; Average balance exceeding Rs. 25 lakh in SB.

Average Balance exceeding Rs. 50 lakh in CA.

Term deposits exceeding Rs. 100 lakh in aggregate.

Annual turnover exceeding Rs. 25 lakh in the SB account, and exceeding Rs. 100 MIO in the CA account.

For arriving at average balance in Savings and Current account, average balance during the immediately preceding last half financial year shall be considered.

For term deposits, aggregate term deposits of the customer at any point of time during the current financial year shall be considered.

Parameters for defining High Net worth Individuals:

Customers with any of the following:

Average balance of Rs. 1 Cr and above in all deposit accounts (SB+CA+TD).

Enjoying Fund based limits/term loans exceeding Rs. 1 Cr.

As per IBA Working Group guidelines, Bank may choose to carry out either manual classification or automatic classification or a combination of both. Similarly, for selecting parameters, Bank may select the parameters based on the available data from system. Once the parameters are finalized, Bank may choose the appropriate risk rating/scoring models by giving due weightage to each parameter as discussed above.

Bank has adopted combination of manual and automatic classification. Based on system generated risk categorization on the basis of data fields, bank shall finalize parameters which are available in the system and the same shall be reviewed half yearly basis. System shall assign provisional risk categorization based on the system provided parameters. Branches shall review the same and make suitable modification/revision, if need be, based on remaining indicators as covered in the policy (Annexure I).

The Bank shall prepare a Risk profile of each customer and apply enhanced due diligence measures on High-Risk customers. IBA has provided an indicative list of High/Medium Risk Products, Services, Geographies, Locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure I in this Policy).

For illustrative examples of Low, Medium and High-Risk customers refer Annexure V. The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while taking into account the above aspects. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Bank.

Risk Parameters

The first step in process of risk categorization is selection of parameters, which would determine customer risk. IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used, to determine the profile and risk category of Customers:

1. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd. etc.
2. Business Segment: Retail, Corporate etc.
3. Country of residence / Nationality: Whether India or any overseas location / Indian or foreign national.
4. Product Subscription: Salary account, NRI products etc.
5. Economic Profile: HNI, Public Ltd. Company etc.
6. Account Status: Active, inoperative, dormant.
7. Account Vintage: Less than six months old etc.
8. Presence in regulatory negative / PEP / Defaulters / Fraudster lists.
9. Suspicious Transaction Report (STR) filed for the customer.
10. AML alerts

Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating etc. can also be used in addition of the above parameters. Bank shall adopt all or majority of these parameters based on availability of data.

Periodical review of risk categorization of customers shall be undertaken once in every six months. Such review for the first half of the financial year i.e. April to September shall be undertaken in succeeding November and for second half of the financial year i.e. October to March in succeeding May in every Financial Year.

Risk rating of Customers

Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending on background, nature and location of activity, country of origin, sources of funds and client profile etc.

A. Risk rating based on the Deposits/account balance:

Account Types High Medium Low All deposit accounts (SB+ CA+ TD) Rs. 100 lakh & above Rs. 25 lakh & above but less than Rs. 100 lakh Less than Rs. 25 lakh

Above categorization of the Customer shall be based on all accounts linked to Customer Information File (CIF) irrespective of constitution of account like Joint account, Partnership account etc. However, accounts linked to (CIF) where customers do not have any stake in Business/activity need not be clubbed for the above purpose.

B. Risk Categorization of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:

Unusual transaction / behavior (given as Annexure I – Monitoring of Customer Risk Categorization (CRC).

1. Submitted Suspicious Transaction Reports (STR) for Customer.
2. Submitted Cash Transaction Report (CTR).
3. Frequent Cheque returns.
4. Minors

C. Risk Categorization of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer. Example: **a Travel Agent (Medium risk) with Proprietorship account (low risk) and having Savings account with average balance of Rs. 1,50,000/-(medium risk) and Term Deposit of Rs. 4,00,000/- (low risk),** shall be assigned with overall rating of "Medium Risk", provided all other conditions mentioned under C above does not necessitate for assigning "High Risk". (Annexure VIII)

Risk categorization of Customers undertaken by the Bank Based on the policy/guidance notes of RBI/IBA and also the methodology of Customer Risk Categorization (as detailed under points A, B & C above), risk rating has been assigned taking into account the following parameters available in CBS system:

1. Customer type
2. Customer profession
3. Type of business
4. Product code
5. Account status

Average balance in deposits in SB/Current/Term Deposit accounts.

All customer profiles/accounts of NRIs, HNIs, PEPs, NGOs, Trusts, Co-operative Societies, HUF, Exporters, Importers and Accounts having Beneficial Owners shall be invariably categorized as High Risk, irrespective of the lower risk category (low/medium) allotted under other parameters in the Matrix like customer profession, type of business, product code, account status, account vintage and balance in the account. As per RBI directions, the parameters used for categorizing the risk profile of customers should include those named in complaints (from legal enforcement authorities) / frauds. As the system will not identify the customers/accounts named in complaints (from legal

enforcement authorities) / frauds, this parameter has not been included in the Risk Categorization Matrix. The Department undertaking the risk categorization is advised to categorize such customers / accounts under – "High Risk" category as and when complaints (from legal enforcement authorities) are received or fraud is reported against the customer/account holder. Blocked Accounts and Unclaimed deposits shall be categorized as High Risk. As per RBI directions, blocked account status should be part of the initial categorization of an account at the branch level rather than being part of the review of risk categorization at the central level. Hence, branches are advised to categorize such accounts as High Risk at the time of blocking the account. Accounts of dealers in Jewellery, Gold/Silver/Bullions, Diamonds and other precious metals/stones shall be categorized under "High Risk". However, if the accounts under the above categories are rated as High/Medium risk under any of the other 6 parameters under the risk categorization matrix, such accounts are to be categorized basing on the highest risk category allotted under those parameters.

Customer Identification Procedure-Features to be verified and Documents that may be obtained from Customers:

Feature	Documents
Accounts of individuals	
Proof of Identity and Address	Where the client is an individual, he shall submit: - a. Any Certified copy which contains proof of Identity / address b. The Permanent Account Number (PAN) of form 60/61 as defined in the Income Tax Rules,1962, And such other documents including in respect of the nature of business and financial status of the client as may be required by the Bank. Officially Valid Documents (OVD) are as under: a. Proof of Possession of Aadhaar Number b. Passport c. Driving License d. Voter's Identity Card issued by Election Commission of India e. Job Card issued by NREGA duly signed by an officer of the State Government f. Letter issued by the National Population Register containing details of name and address g. Any other document as notified by the Central Government in consultation with the Regulator. **Banks can use physical copy of the Aadhaar card as well as e-Aadhaar, masked Aadhaar and offline electronic Aadhaar xml provided by UIDAI, which are various forms of Aadhaar, as Officially Valid Documents (OVD) for the KYC purpose but without e- KYC based authentication for those customers who do not give a declaration that s/he is desirous of receiving her/his entitled benefits for subsidies welfare schemes funded from the Consolidated Fund of India in her/his account directly.**

	(As per UIDAI circular dated 23-10-2018 based on the opinion received from the Ld. Attorney General for India after the Aadhaar Judgment of the Hon. Supreme Court of India, delivered on 26-09-2018).
Accounts of Proprietorship Concerns	
Proof of name, address and activity of the concern	For Proprietary concerns, in addition to the PAN No and certified copy of documents applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern should be submitted: a. Registration certificate (in the case of a registered concern). b. Certificate / license issued by the municipal authorities under Shop and Establishment Act. c. Sales and income tax returns. d. CST/VAT/ GST certificate (provisional / final). e. Certificate / registration document issued by Sales Tax / Service Tax/Professional Tax authorities. f. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by Income Tax authorities e.g. Utility bills such as electricity, water, landline telephone bills etc. h. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License/certificate of practiceissued in the name of the proprietary concern by any professional body incorporated under a statute. Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, however, would have to undertake contact point verification, collect such

	information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern. RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not enjoyingany credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s). Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or unsecured.
Accounts of partnership firms	
Proof of name, address and activity of the concern	Where the client is a partnership firm,certified copies of following documents or the equivalent e-documents of all the following documents are to be submitted: a. Registration Certificate b. Partnership Deed c. Permanent Account Number of the Partnership Firm d. Any Officially Valid Document which contains proof of identity / address in respects of managers, officers and employees holding an attorney to transacts on its behalf. And e. PANs or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the partnership firm. RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not

	enjoyingany credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s). Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or unsecured.
Accounts of companies	
Proof of name, address and activity of the concern	Where the client is a company, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: a. Certificate of incorporation b. Memorandum and Articles of Association c. Permanent Account Number of the Company d. A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf. e. Any Certified Officially Valid Document, which contains proof of identity / address in respects of managers, officers and employees holding an attorney to transact on its behalf. and f. PANs or Form 60/61 as defined in the Income Tax Rules, 1962 issued to managers, officers or employees holding an attorney to transact on the company‘s behalf. RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer

	with any other bank(s). Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or Unsecured.
Accounts of trusts	
Proof of name, address and activity of the concern	Where the client is a Trust, certified copies of documents or the equivalent e- documents of all the following documents are to be submitted: a. Registration Certificate b. Trust Deed c. Permanent Account Number or Form 60/61 of the Trust d. Any Certified Officially Valid Document which contains proof of identity / address in respects of managers, officers and employees holding an attorney to transact on its behalf. e. PANs or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the Trust.
Accounts of Unincorporated Association or body of individuals	
Proof of name, address and activity of the concern	Where the client is an unincorporated association or a body of individuals, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: a. Resolution of the managing body of such association or body of individuals b. Permanent Account Number or Form 60/61 of the Unincorporated association or a body of individuals c. Power of Attorney granted to the person who will transact on its behalf. d. Any Certified Officially Valid Document, which contains

	proof of identity / address in respects of managers, officers and employees holding an attorney to transact on its behalf. And e. PAN or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the unincorporated association or a body of individuals.
Accounts of Governments or its Departments, Societies, Universities and Local Bodies like village panchayats	
Proof of name, address and activity of the concern	i. Document showing name of the person authorized to act on behalf of the entity; a. Any Certified Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf. And b. PAN or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the entity.
Accounts of Limited Liability Partnerships	
Proof of name, address and activity of the concern	a. Certified copy of incorporation documents filed with registrar of Companies b. Certificate issued by the registrar of Companies c. Copy of LLP Agreement signed by all the partners. In case, there is no LLP Agreement, Schedule I of the LLP Act signed by all the partners will prevail. d. (i) Any Certified Officially Valid Document which contains proof of identity / address in respects of person holding an attorney to transacts on its behalf and (ii) PAN or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding a power of attorney to transact on its behalf
Relaxation for Accounts of low risk customers	
'Simplified measures' may be applied in the case of 'Low risk' customers taking into	Additional documents deemed to be certified OVDs for the purpose of proof of identity

consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.	where simplified measures are applied: a. Identity card with applicant's photograph issued by Central /State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; b. Letter issued by a gazetted officer, with a duly attested photograph of the person. For the limited purpose of proof of address, the following additional documents are deemed to be OVDs where simplified measures are applied: a. Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill); b. Property or Municipal Tax receipt; c. Bank account or Post Office saving bank account statement; d. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; e. Letter of allotment of accommodation from employer issued by Central / State Government departments, Statutory or Regulatory bodies, Public Sector Undertakings, Scheduled Commercial Banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting officialsaccommodation; and f. Documents issued by Government departments of foreign jurisdiction and letter issued by Foreign Embassy or Mission in India.
Bank has to obtain only the documents as mentioned above and not to accept any other document for KYC purpose.	

ANNEXURE – VII

KYC documents for eligible FPIs under PIS

		FPI Type		
Document Type		Category I	Category II	Category III
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN148	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution@@	Exempted *	Mandatory	Mandatory
Senior Management (Whole Time Directors/ Partners/ Trustees/ etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head
	Photographs	Exempted	Exempted	Exempted *
Authorized Signatories	List and Signatures	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter
	Photographs	Exempted	Exempted	Exempted *

Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.

@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution'

Category	Eligible Foreign Investors
I.	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies.
II.	a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc. b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc. c) Broad based funds whose investment manager is appropriately regulated. d) University Funds and Pension Funds. e) University related Endowments already registered with SEBI as FII/Sub Account.
III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

ANNEXURE – VIII

Indicative Alert Indicators for the Bank to report suspicioustransactions / attempted transactions

Alert indicator		Indicative rule / scenario
CV– Customer Verification		
CV1.1	Customer left without opening the account	Customer did not open the account after being informed about KYC
CV2.1	Customer offered forged or false documents	Customer gives false documents or documents that appear to be forged / inaccurate / altered
CV2.2	Documents are not verifiable	Documents for identification are not verifiable i.e. Foreign documents
CV 3.1	Address found to be non-existent	Address provided by customer found to be non-existent
CV 3.2	Address found to be wrong	Customer not staying at the address provided at the time of account opening
CV 4.1	Difficult to identify the beneficial owner	Customer uses complex legal structures
LQ- Law Enforcement Agency Query		
LQ 1.1	Customer being investigatedfor criminal offences	Customer has been the subject of inquiry from Any law enforcement agency relating to criminal offences
LQ 2.1	Customer being investigatedfor TF offences	Customer has been the subject of inquiry fromAny law enforcement agency relating to criminal offences or TF offences
MR– Media Reports		
MR 1.1	Adverse media report about criminal activities customer	Match of customer details with persons reported in local media/ open source for criminal offences
MR 02.1	Adverse media report about terrorism finance activities customer	Match of customer details with persons reported in local media/ open source for criminal offences and TF activities
EI – Employee Initiated		
EI 1.1	Customer did not complete transaction	Customer did not complete transaction after queries such as source of funds
EI 2.1	Customer is nervous	Customer is hurried or nervous
EI 2.2	Customer is over cautious	Customer over cautious in explaining genuineness of transaction
EI 2.3	Customer provides inconsistent information	Customer provides information that seems false/minimal or inconsistent
EI 3.1	Customer acting on behalf of a third party	Customer has vague knowledge about amount of money involved in the transaction

EI 3.2	Multiple customers working as group	Multiple customers arrive together but pretend to ignore each other
EI4.1	Customer avoiding nearer	Customer travels unexplained distances to conduct transactions
EI 4.2	Customer offers different identification on different occasions	Customer offers different identification on different occasions with an apparent attempt to avoid linkage of transactions.
E14.3	Customer wants to avoid reporting	Customer wants to avoid reporting by convincing staff.
E14.4	Customer could not explain source of funds	Customer could not explain source of funds satisfactorily
E15.1	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.
E15.2	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense
E15.3	Transaction inconsistent with business	Movement of transaction inconsistent with customer's business
E15.4	Unapproved inward remittance in NPO	Foreign remittance received by NPO not approved by FCRA
E17.1	Complaint received from public	Complaint received from public for abuse of account for committing fraud etc.
E18.1	Alert raised by agent	Alert raised by agents about suspicion.
E19.1	Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross-border referrals.

ANNEXURE – IX

Examples of STRs received at FIU-IND

Examples of STRs received at FIU-IND		
	Type of Suspicion	**Summary of Detection and Report**
1	False Identity	Identification documents found to be forged during customer verification process. The account holder not traceable.
2	Wrong Address	Welcome pack received back since the person was notstaying at the given address. In some cases, the address details given by the account holder found to be false. The account holder not traceable.
3	Use of similar sounding corporate names	Account was opened with names very close to other established business entities.
4	Doubt over the real beneficiary of the account	Customer not aware of transactions in the account. Transactions inconsistent with customer's profile.
5	Account of persons underinvestigation	The customer reported in media for being under investigation/ Account of a customer frozen by the bank
6	Account of wanted criminal	Name of the account holder and additional criteria(Date of birth / Father's name / Nationality) matched with details on a Watch List of UN, Interpol etc.
7	Account used for cyber crime	Complaints of cybercrime received against a customer. The transactions in the account have no valid explanation.
8	Doubtful activity of accountholder	Cash deposited in a bank account at multiple cities on the same day. The account holder a citizen of country with high rate of drug trafficking.
09	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter-account transactions without any economicrationale.
10	Unexplained activity in dormant accounts	The customer could not provide satisfactory explanation to Transactions in a dormant account.
11	Suspicious cash withdrawals in bank account	Large value cheques deposited followed by immediate cash withdrawals
12	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.

13	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list
14	Doubtful utilization of Foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation
15	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization
16	Unexplained activity in Account inconsistent With what would be expected from declared business	Transactions in account inconsistent with declared business. The Customer could not provide satisfactory explanation.
17	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
18	Doubtful use of safe deposit Locker	Safe deposit locker operated frequently though the financial status of client does not warrant such frequency. Large suitcase brought by customer.
19	Doubtful source of cash deposited in bank account	Cash transactions of value just under the reporting threshold. Cash transactions spilt across accounts to avoid reporting. No valid explanation

ANNEXURE –X

Additional Alert Scenarios for Identifying Suspicious Transactions Related toTrade Based Money Laundering

S. No.	ADDITIONAL ALERT SCENARIOS FOR IDENTIFYING SUSPICIOUS TRANSACTIONS RELATED TO TRADE BASED MONEY LAUNDERING
1	Scenarios for verifying the actual date of import and the date of remittance
2	Many proprietorship firms importing from the same exporter from a foreign land
3	Advance waivers provided or pre-accepted discrepancy by the applicant and/or the applicant is over keen to waive discrepancy
4	Representation of an official document immediately after a turn-down for discrepancy
5	Submission/payment of round figure bills
6	Transaction limits for the first time import active customer
7	Outward remittance to same overseas party (with internal thresholds for the number of days and number of transactions)
8	Outward remittance of same value from single customer. Mot\re than x transactions on last y days.
9	Cumulative transaction amount (frequency and the amount thresholds according to the bank's experience) in outward remittance.

Standard Operating Procedure for Identification of Money Mules

Objective

The purpose of this Standard Operating Procedure (SOP) is designed to assist the bank in complying with the Reserve Bank of India (RBI) guidelines on Know Your Customer (KYC), Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and obligations under the Prevention of Money Laundering Act, 2002. The SOP aims to identify and prevent money mule activities, including money laundering, terrorist financing, and other illicit activities, by detecting and reporting and reporting suspicious transactions involving money mules. Money mule networks pose a global threat, facilitating the movement of large sums of illegal money for criminal and terrorist purposes.

Definitions

i. Money Mule
   Also known as "smurfers", money mules are individuals recruited, knowingly or unknowingly, to participate in money laundering schemes. They typically assist in opening and managing bank accounts to facilitate the deposit, transfer and withdrawal of illegal funds.

ii. Suspicious Transaction
   Any transaction that appears to be unusual, lacks a clear economic rationale, or may be related to money laundering or terrorist financing.

iii. Know Your Customer (KYC)
   The process of verifying customer identity and assessing potential risks of illegal intentions in a business relationship.

iv. Shell Companies
   Business entities are often used by money launderers to conceal illegal funds and the identity of beneficial owners.

Responsibilities

i. The Deputy Manager shall have overall responsibility for implementing and monitoring the SOP within the branch.
ii. The Officer in charge for account opening and Senior Vice President (Risk) shall be responsible for conducting customer due diligence and ensuring compliance during account opening, and assisting in the verification and documentation process for customer accounts.
iii. Compliance Officer shall be responsible for monitoring transactions, detecting suspicious activities, and reporting them to the appropriate authorities.

Customer Onboarding

The process of establishing and verifying a customer's identity and the nature of their business is a cornerstone of risk-based AML. Robust customer due diligence (CDD) is vital to the detection of money mules that are opening accounts on behalf of third parties.

i. The Bank shall obtain all necessary customer information and documents during the account opening process, adhering to KYC guidelines issued by the RBI.
ii. Conduct enhanced due diligence for high-risk customers, including politically exposed persons (PEPs) and those from high-risk jurisdictions.

iii. Verify the authenticity of documents submitted by the customer using reliable sources and digital verification methods, if available.
iv. Perform sanction screening of customers using Compass AML before onboarding.

Monitoring Transactions

The Bank should monitor customer accounts for suspicious transaction patterns. Money mule accounts may be used to facilitate an unusual volume or frequency of transactions or may engage in unusual transaction patterns.

i. Implement a robust system for monitoring transactions and account activities including beneficiaries and destination.
ii. Set thresholds for suspicious transaction monitoring based on Indian Banks' Association (IBA)/RBI guidelines and customer risk profiles.
iii. Analyze transaction patterns to detect significant deviations from customer's profile or known business activities.
iv. Money mules may be acting on behalf of PEPs or other high-risk individuals. In such a scenario, Bank to implement Politically Exposed Person and sanction screening measures identify connections to high-risk individuals.
v. Monitoring accounts engaged in multiple transactions without clear purposes or involving transfers to and from higher-risk jurisdictions.
vi. The Bank should also pay special attention to transaction involving potential money mule accounts, particularly those related to jurisdictions with weak AML systems and controls.
vii. Investigate and report suspicious shell companies to the authorities to prevent money laundering attempts.

Identifying Money Mules

i. The Bank staff should be capable of recognizing potential signs of money mule activities, such as frequent large cash deposits or withdrawals, rapid fund transfers, or involvement in suspicious businesses.
ii. Staff should be vigilant with customers who receive funds from multiple unrelated sources or sending funds to high-risk jurisdictions without valid reason.
iii. Monitor accounts showing multiple transactions involving unrelated third parties, especially shortly after the account is opened.

Reporting Suspicious Transactions

The Bank should consider "red flag" behaviors or characteristics of money muling as part of their AML response.

i. If any suspicious transaction is identified or suspected to be related to money mule activities, it should be reported immediately through the AML system to the Bank's Chief Compliance Officer.
ii. The Chief Compliance Officer shall conduct a thorough investigation and gather additional information if necessary.
iii. If the suspicion is substantiated, a Suspicious Transaction Report (STR) with the Financial Intelligence Unit-India (FIU-IND) as per RBI guidelines.

Communication and Training

i. The Bank will regularly communicate the importance of identifying money mules and adhering to the SOP to all bank staff members.
ii. Conduct training sessions and workshops to educate staff about the latest money laundering and money mule trends and techniques.
iii. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment websites, social networking sites, instant messaging and advertisements in newspapers. The Bank shall take steps to ensure that the customers do not fall prey to such scamsters.

Record Keeping

Maintain comprehensive records of customer due diligence documentation, transaction details, and all related communications as per the Bank's Record Retention Policy.

Review and Update

i. The Bank will periodically review and update the SOP to align with changes in RBI regulations or emerging money mule risks.
ii. Conduct internal audits to assess the effectiveness of the SOP's implementation and make necessary improvements.

Non-Compliance

Non-compliance with this SOP or failure to report suspicious transactions may subject the Bank to regulatory penalties or supervisory action.

This SOP should be followed diligently by all bank staff involved in customer onboarding, transactions, and compliance-related activities. By adhering to these guidelines, the bank contributes to the collective effort of combating money mule activities and ensuring a safer financial ecosystem.

Annexure – XII

Standard Operating Procedure for handling of AML alerts

This document provides the basic understanding of alerts handling process that is to be followed at the Bank for effective transaction monitoring at all levels. The document covers the operational processes to be followed by AML users to review the alerts and attain the objective of proactive vigilance. It is to be noted that the verification process described below is not exhaustive or exclusive in nature and the verifying officers may use their own diligence during the verification.

Generation of alerts

The AML alerts are automated and generated through the system. The Bank has implemented the COMPASS AML hosted by M/s Quantum Data Engines Pvt Ltd. The alerts are auto generated and pushed to AML system from the CBS and SWIFT at the start of the day. The alerts are generated based predefined criteria issued by IBA, FIU, and based on the business model of the Bank may adopt their own scenarios.

AML system Users

AML User - First Level Verification. An Officer who is in the cadre of Junior Executive II and above will be eligible to be assigned as AML User. The Bank should have atleast 03 AML Users having adequate knowledge on KYC/AML/CFT guidelines. The AML Users are Officers who are not involved in the day to day operations in the Bank. All transactions from the AML system will be directly assigned to the AML Users who will verify the same and in case if the transaction is in accordance with the normal course of the customer profile, the same may be closed by the AML User with the valid reason for closure.

In case of any suspicion, the same will be escalated to the AMLRO with the ground of suspicion. All transactions by the AML users should be closed within the next working day. The Risk Department will monitor the same on a daily basis and in case no action has been taken within 02 working days from the date of alert, the same may be reported to Principal Officer for further action.

AMLO (Anti Money Laundering Officer)-Second Level Verification. An AMLRO will be a Senior Management Officer with adequate experience and updated knowledge in KYC/AML/CFT guidelines. The Officer will verify all transactions escalated to them by the AML Users and in case, the alert is found to be non-suspicious can close the same with proper reasons. The AMLRO in case finds the transaction to be suspicious in nature, has to escalate the same, MLRO by assigning reasons for escalating the same. The Bank should have at least 02 AMLROs.

The AMLO should either close the alert or escalate the same within 03 working days. The AMLO should also randomly verify closures made by AML Users and ensure that proper reasons have been assigned for closure and found to be satisfactory.

MLRO (Money Laundering Reporting Officer)-Principal Officer or Chief Compliance Officer who has been assigned by the Regulator to carry out the compliance functions. The alerts escalated by the AMLRO will be verified and in case found to be suspicious, the Officer will refer the same to Designated Director and generate the STR report in the AML system. The Principal Officer has to provide the GOS as per the FIU format and it is the duty of the PO to report the STR to FIU-IND within the stipulated timeframe. In case, MLRO based on the history and profile of the customer may carry out a due diligence and close the alert with proper justification.

AML System

The alerts and the risk categorisation has to be reviewed on a periodical basis and in case of any scenarios to be included in the system, it has to be immediately updated in the system. The PO is responsible for updating and reviewing the system on a regular basis.

Updation of Sanction Lists

The Bank has currently subscribed to the following sanction lists

1.UNSC

2.OFAC

3.Dow Jones

The updation of lists should be carried out on a daily basis. The IT Department will be responsible for daily updation. The Senior Vice President (Risk) shall ensure compliance to the above. The Vice President (Compliance) shall verify the updation of names published in the sanction lists to the AML system as and when an updated list is issued by the RBI/FIU/Government Agencies etc.

Risk Categorisation

Based on the KYC/AML/ CFT Policy of the Bank, the system carry out risk categorisation on a half-yearly basis which will be verified by the Operations in-charge and the Risk Officer. The movement in risk categorisation has to be discussed in the Management Committee of Chennai Branch and if any enhanced due diligence has to be initiated which has to be immediately carried out.

Review of AML alerts

The Risk Management Department will submit a report in the Risk Management Committee on the number of alerts generated, number of alerts closed and number of STRs escalated if any

Tip off

Any Officers dealing with AML system should not provide any tip-off to the customers and all transactions are to be reviewed cautiously and in the interest of the Bank.

Accountability

The AML Officers are accountable for the actions taken on the closure of alerts in the AML system.

MIS

The PO has to ensure that the system is capable of generating alerts for all specified scenarios and a report has to be placed before the Management Committee of Chennai Branch on a regular basis. The system should generate a report of all randomly verified alerts by AMLO and MLRO.

Annexure – XIII

Prohibition of Opening SB Account

The Bank is prohibited from opening a savings deposit account in the name of Government departments / bodies depending upon budgetary allocations for performance of their functions / Municipal Corporations or Municipal Committees / Panchayat Samitis / State Housing Boards / Water and Sewerage / Drainage Boards / State Text Book Publishing Corporations / Societies / Metropolitan Development Authority / State / District Level Housing Co-operative Societies, etc. or any political party or any trading/business or professional concern, whether such concern is a proprietary or a partnership firm or a company or an association and entities other than individuals, Karta of HUF and organisations/agencies listed in Schedule -I.

Explanation

For the purposes of this clause, 'political party' means an association or body of individual citizens of India, which is, or is deemed to be registered with the Election Commission of India as a political party under the Election Symbols (Reservation and Allotment) Order, 1968 as in force for the time being.

SCHEDULE- I

1. Primary Co-operative Credit Society which is being financed by the bank.
2. Khadi and Village Industries Boards.
3. Agriculture Produce Market Committees.
4. Societies registered under the Societies Registration Act, 1860 or any other corresponding law in force in a State or a Union Territory except societies registered under the State Co-operative Societies Acts and specific state enactment creating Land Mortgage Banks.
5. Companies licensed by the Central Government under Section 8 of Companies Act, 2013 or Section 25 of Companies Act, 1956 or under the corresponding provision in the Indian Companies Act, 1913 and permitted, not to add to their names the words 'Limited' or the words 'Private Limited'.
6. Institutions other than those mentioned in Section 28(h) and whose entire income is exempt from payment of Income-tax under the Income-Tax Act, 1961.
7. Government departments / bodies / agencies in respect of grants/ subsidies released for implementation of various programmes / Schemes sponsored by Central Government / State Governments subject to production of an authorization from the respective Central / State Government departments to open savings bank account.
8. Development of Women and Children in Rural Areas (DWCRA).
9. Self-help Groups (SHGs), registered or unregistered, which are engaged in promoting savings habits among their members.
10. Farmers' Clubs – Vikas Volunteer Vahini – VVV.

Standard Operating Procedure (SOP) to open and operate the "FCRA Account" as provided under Section 17(1) of the amended Foreign Contribution (Regulation) Act, 2010 with SBI, New Delhi Main Branch in terms of FCRA (Amendment), 2020

1. The amended Foreign Contribution (Regulation) Act, 2010 mandates that every person/NGO/ Association (hereinafter referred to as an "entity") that have been granted FCRA certificate of registration or prior permission u/s 12 of the Act shall open an "FCRA Account" at specified branch of State Bank of India in New Delhi. The Central Government vide notification dated 07.10.2020 has notified New Delhi Main Branch (henceforth NDMB) of SBI, 11, Sansad Marg, New Delhi-110001 as specified branch.
2. Presently, there are approximately 23,000 entities which have got a Certificate of Registration or prior permission to receive foreign contribution. They now have to open a "FCRA Account" for inward remittance of any foreign contribution at the aforementioned specified branch (i.e. NDMB) on or before 31.03.2021. From the date of opening of "FCRA Account" in NDMB or from 31.03.2021, whichever is earlier, no inward remittance will be allowed in any account other than that opened in NDMB.
3. The following steps and procedure will be followed so as to ensure hassle-free opening and operation of "FCRA Account" by entities making requests for fresh FCRA registration/prior permission as well as existing FCRA registration/prior permission holders having FCRA accounts in any Branch or Bank other than NDMB Branch of SBI.

A. SOP FOR ACCOUNT OPENING

i. Any entity which seeks to receive foreign contribution may approach either the nearest SBI Branch or any other SBI Branch of their choice for submitting the completed Account Opening Form (AOF) for KYC/photo/signature verification, scanning and forwarding through mail as well as sending hard copy of their AOF for opening of "FCRA Account" at NDMB.

ii. The applicant shall collect the Account Opening Form (AOF) physically or download the same from the website of SBI and submit the duly up form along with mandatory KYC documents, for scrutiny / verification. Mandatory documents should include KYCs of signatories and KYCs of Controlling Person / Beneficial Owner (in terms of guidelines issued by RBI).

iii. The applicant shall receive an acknowledgement in this regard from the AOF accepting Branch.

iv. The AOF accepting branch of SBI would scrutinize AOF and KYC documents and email the verified documents to SBI, NDMB within 3 working days from the date of receipt of completed documents. SBI, NDMB shall confirm to the applicant entity through an email regarding receipt of AOF and other documents within 1 working day of its receipt.

v. The NDMB will intimate to the applicant entity the details of "FCRA Account" so opened within 3 working days from the date of receipt of duly verified scanned copies of complete set of AOF and KYC documents from e-mail ID of the receiving branch. The intimation will be sent by registered email ID as well as through SMS.

vi. "Entity" can maintain their existing FCRA Accounts for Keeping or Utilization purposes.

vii. The complete details of the specified branch i.e. SBI NDMB are as under:

Name of the Branch	State Bank of India, New Delhi Main Branch (NDMB)
Address of the FCRA Cell at NDMB	FCRA Cell, 1st Floor, 11, Sansad Marg, New Delhi-110001
Branch Code	00691
IFSC Code	SBIN0000691
SWIFT CODE	SBININBB104
E-Mail ID	fcra.00691@sbi.co.in
Telephone No	011-23374392, 23374390, 23374143, 23374213

B. Process flow after opening of "FCRA Account" in case of persons entities already in possession of a Registration Certificate or prior permission of Central Govt. to receive foreign contribution through SWIFT mode.

i. The NDMB will allow receipt of foreign contribution only in the "FCRA Account" opened in NDMB after confirming that the MHA has already granted a certificate or prior permission under section 12 of FCRA, 2010. The foreign inward remittance received should invariably contain following details:
   - "FCRA Account" Number of the Beneficiary in the NDMB of SBI
   - SWIFT Code of NDMB (SBININBB104)
   - Name of the Beneficiary
   - Name of the Donor/ Remitter
   - Account number of the Donor/Remitter
   - Donor/Remitter's Address
   - Donor/Remitter's Country of Residence

ii. In case of fresh applicant / entity, the NDMB shall open the "FCRA Account" and then wait for MHA's decision on the application of the entities / persons for grant of prior permission or registration certificate. As soon as the MHA approval for such registration or prior permission is conveyed to NDMB through an e-mail, NDMB shall allow inflow of foreign contribution into the relevant account from that date.

iii. SBI, NDMB shall intimate the customers, through an e-mail and SMS regarding receipt of foreign contribution.

iv. The customers will be required to submit an undertaking detailing the purpose of the receipt of funds as per FEMA declaration and RBI guidelines to the SBI Branch, where it had initially submitted the AOF. The Branch shall then forward duly scrutinized copies to New Delhi Main Branch on the designated email id (fcra.00691@sbi.co.in).

v. Standard Forex conversion rate as permitted under the FEMA guidelines and RBI instructions to be applied on the inflow of foreign currency. It shall be duly intimated to the account holder through an e-mail.

vi. The "FCRA Account" holder shall have complete freedom to transfer the foreign contribution (FC) received in "FCRA Account" opened in NDMB to another "FCRA Account", if any, of his choice opened in any branch of any Scheduled Commercial Bank as per its convenience for keeping or utilization. It may also avail Internet Banking facility (with full transaction rights) with the NDMB.

vii. NDMB will not levy any charges / fee etc on any transfer of foreign contribution from the "FCRA Account" to "another FCRA Account", if any, and to Utilization Account, if any, of the

entity. For each such transfer, the "FCRA Account" holder to be informed through an e-mail as well as SMS immediately.

B. GRIEVANCE REDRESSAL MECHANISM

If the "FCRA Account" holder raises any grievance while opening of "FCRA Account" or while operating it, the following redressal mechanism shall be available:

i. The "FCRA Account" holder or the applicant entity may send e-mail on fcracomplaints.00691@sbi.co.in. The NDMB shall create an "FCRA Cell" to handle all such e-mails.
ii. The applicant person / entity or the "FCRA Account" holder may also register their complaints / grievances/ suggestion on 011-23374392, 23374143, 23374213.
iii. If grievance is not redressed after accessing the aforementioned mechanism, it may be escalated through an e-mail to sbi.00691@sbi.co.in. The DGM of NDMB will handle this matter.
iv. The escalation matrix for grievance redressal is given in the paragraph C(i), C(ii) and C(iii) above. However, if the applicant person / entity is not satisfied with the grievance redressal provided, then the grievance may be escalated to DGM (IBD-II) [e-Mail: dgmibd2.ibg@sbi.co.in] who is the apex grievance redressal authority.