BANK OF CEYLON

Bankers to the Nation

Know Your Customer and

Anti Money Laundering Policy

Division : Chennai

Next Review - August 2023

Document Control

Serial No	Type of Information	Document Data
1	Policy Title	Know Your Customer and Anti Money Laundering Policy
2	Date of Approval	15.11.2021
3	Policy Superseded	-
4	Policy Version Number	2.0
5	Policy Owner	Chennai Branch
6	Policy Approval	Board of Directors

Disclaimer

The contents of this Policy document is 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. Part – I – CDD Procedure in case of Individuals	15
3. Part – II – CDD Measures for Sole Proprietary Firms	18
4. Part – III – CDD Measures for Legal Entities	19
5. Part – IV – Identification of Beneficial Owner	20
6. Part – V – Trade Based Money Laundering	20
7. Part – VI – On-going Due Diligence	23
8. Part – VII – Enhanced and Simplified Due Diligence Procedure	25
9. Record Management	26
10. Reporting Requirements to Financial Intelligence Unit – India	27
11. Requirements / Obligations under International Agreements	29
12. Other Instructions	30
13. Annexure – I	33
14. Annexure – II	39
15. Annexure – III	46
16. Annexure – IV----- Ultimate Beneficial Owner	49
17. Annexure – V -----Risk Categorization of Customer Based on various parameters	57

Know Your Customer (KYC) Policy, 2022

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 issued as per RBI's Master Directions on Know Your Customer (updated upto 09.01.2020) 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 shall take all necessary steps to implement this KYC 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).

1. Short Title

Preliminary

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 Know Your Customer (KYC) Policy, 2022.

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 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 25 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 shareholders 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 15 per cent of capital or profits of the partnership.

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 15 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 15% 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 bank shall mean comparing the copy of officially valid document so produced by the customer with the original 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.

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

vii. **"Principal Officer"** 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.

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

ix. **"Non-profit Organisations"** (NPO) means any entity or organization 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.

x. **"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 licence 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.

xi. **"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).

xii. **"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).

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

xiv. **"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.

xv. **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.

xvi. **"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.

xvii. **"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:

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. **"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.

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

iv. **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the beneficial owner.

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

vi. **"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.

vii. **"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.

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

ix. **"On-going Due Diligence"** means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

x. **"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.

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

xii. **"Shell bank"** means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

xiii. **"Wire transfer"** 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.

xiv. **"Domestic and cross-border wire transfer":** When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

(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.

General

4. RBI has advised the Bank that a Know Your Customer (KYC) Policy, duly approved by the Board of Directors of the Bank, be formulated and put in place.

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, 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.

6. Principal Officer

a. Bank to nominate Chennai Branch CEO as "Principal Officer", as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules. Principal Officer shall be nominated by the Board.

b. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

7. 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.

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

(c) 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

8. Bank to frame a Customer Acceptance Policy.

9. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, 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.
   (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 is obtained with the explicit consent of the customer 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) 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.

Risk Management

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

    a. Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception of the Bank.
    b. Risk categorisation shall be undertaken based on parameters such as customer's identity, social / financial status, nature of business activity, and 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.

    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), guidance note circulated to all cooperative banks by the RBI 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, authorised 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; and

b) Permanent account number (PAN) or 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) one recent photograph; and

d) Atleast 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 / licence 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, Licence / 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

correctly 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 / Link
PAN Card	On line PAN verification
Voter Identity Card	www.nvsp.in (National Voters Service Portal)

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
(ii) Certificate / Licence 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 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

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 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

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 15, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

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 15, 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 15 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.

Part IV - Identification of Beneficial Owner

22. 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:

   (a) 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

23. 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.

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

24.1 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'.

24.2 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.

25. 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.

26. 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.

27. 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 identifythe 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 TBML/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

28. 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.

29. 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.

30. 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 categorisation 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.

31. Periodic Updation

Periodic updation shall be carried out at least once in six months for PEP's, every year for high risk customers, once in every five years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

a. Bank shall carry out

i. CDD, as specified in Section 15, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

ii. In case of Legal entities, Bank shall review the documents sought at the time of opening of account and obtain fresh certified copies.

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

b. 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.

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

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

e. 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.

32. In case of existing customers, Bank shall obtain the Permanent Account Number 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 Permanent Account Number 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

33. 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.

34. Accounts of Politically Exposed Persons (PEPs)

a. Bank shall have the option of establishing a relationship with PEPs provided that:
   (i) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
   (ii) the identity of the person shall have been verified before accepting the PEP as a customer;
   (iii) the decision to open an account for a PEP is taken at a senior level, i.e. at the level of Country Manager , in accordance with the Bank' Customer Acceptance Policy;
   (iv) all such accounts are subjected to enhanced monitoring on an on-going basis;
   (v) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

b. These instructions shall also be applicable to accounts where PEP is the beneficial owner.
c. Account to be reviewed bi-annually.

35. 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

36. 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. maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction as per Section 12 of Prevention of Money Laundering Act, 2002;
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 five years after the business relationship is ended;
c. make available the identification records and transaction data to the competent authorities upon request;
d. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
e. maintain all necessary information in respect of transactions prescribed under PML Rule 3 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.

f. 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;

g. 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.

Reporting Requirements to Financial Intelligence Unit - India

37. 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.

38. 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.

39. 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.

40. 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 Senior vic President Compliance 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 Organisations 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.

<u>Requirements / Obligations under International Agreements</u>

Sanction Compliance

41. 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:

    a. The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List.
    b. The"1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban.

42. 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 March 14, 2019.

43. 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.

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

The procedure laid down in the UAPA Order dated March 14, 2019 (Annexure- II of this KYC Policy) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

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

a. 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.

b. 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.

c. 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.

<u>Other Instructions</u>

46. Secrecy Obligations and Sharing of Information:

a. Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

b. 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.

c. The exceptions to the said rule shall be as under :
    1. Where disclosure is under compulsion of law,
    2. Where there is a duty to the public to disclose,
    3. the interest of bank requires disclosure and
    4. Where the disclosure is made with the express or implied consent of the customer.

d. 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.

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

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 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.

The KYC data / documents pertaining to all new individual accounts opened on or after January 1, 2017 have to be invariably uploaded with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 within ten days of opening the accounts, uploaded of Legacy records on CKYCR at the time of ReKYC – update as per CKYC registry circular dated 06.01.2021.

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

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 FATCA and CRS
ii. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

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

50. 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.

51. **Wire transfer**

Bank shall ensure the following while effecting wire transfer:

a. All cross-border wire transfers shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account.

b. Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.

c. Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

d. Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.

e. Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

f. A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

g. The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

h. All the information on the originator of wire transfers shall be immediately made available to appropriate law enforcement and / or prosecutorial authorities on receiving such requests.

i. Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.

j. Beneficiary bank shall report transaction lacking complete originator information to FIU-IND as a suspicious transaction.

k. The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

52. 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. 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 AML / CFT policy. Proper staffing of the audit function with persons adequately trained and well-versed in AML / CFT policies of the Bank, regulation and related issues shall be ensured.

Annexure – I

INDICATIVE LIST OF VARIOUS TYPES OF INDICATORS I.E. CUSTOMER BEHAVIOUR AND RISK BASED TRANSACTION MONITORING, HIGH & MEDIUM RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/ LOCATIONS/ALERTS FOR CHENNAI BRANCH

1. INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION 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 is 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

i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
ii. Frequent withdrawal of large amounts by means of cheques,
iii. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
iv. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;

v. 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.;

vi. 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 a 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

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.

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.

File No.14014/01/2019/CFT **Annexure-II**

Government of India Ministry of Home Affairs CTCR Division

New Delhi, dated 14 March 2019

ORDER

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

The Unlawful Activities (Prevention) Act, 1967 (UAPA) was amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51 A, 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. In order to expeditiously and effectively implement the provisions of Section 51A, a procedure was outlined vide this Ministry Order No. 17015/10/2002-IS-VI dated 27.08.2009. After the reorganization of the Divisions in Ministry of Home Affairs, the administration of Unlawful Activities (Prevention) Act, 1967 and the work relating to countering of terror financing has been allocated to the CTCR Division. The order dated 27.8.2009 is accordingly modified as under:

Appointment and communication of details of UAPA Nodal Officers

2. As regards appointment and communication of details of UAPA Nodal Officers-

(i) The UAPA Nodal Officer for CTCR Division would be the Joint Secretary (CTCR), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsctcr-mha@gov.in (e-mail id).

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the CTCR Division in MHA.

(iii) The States and UTs should 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 CTCR Division in MHA.

(iv) The CTCR Division in MHA would maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA Noda! Officers should be circulated by the Nodal Officer of CTCR Division of MHA in July every year and on every change. Joint Secretary (CTCR) being the Nodal Officer of CTCR Division of MHA, shall cause the amended list of UAPA Noda! Officers to be circulated to the Nodal Officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, CTCR Division and Foreigners Division in MHA,

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The CTCR Division of MHA would forward the designated lists to the UAPA Nodal Officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

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

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies requiring them to-

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order, herein after, 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 or 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 and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, 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 Joint. Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone or 011-23092736. The particulars apart from being sent by post, should necessarily be conveyed on e-mail 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 (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and Regulators and FIU-IND, as the case maybe.

(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 would prevent designated persons from conducting financial transactions, under intimation to the Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in.

(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 by paragraph (ii) above, carried through or attempted as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 4(ii) above, CTCR Division of MHA 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 regulated by SEBI 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 within a period not exceeding 5 working days from the date of receipt of such particulars.

6. 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 order to freeze these assets under Section 51A of the UAPA would be issued by the UAPA Nodal Officer of CTCR Division of MHA and conveyed electronically/to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA Nodal Officer of CTCR Division

of MHA shall also forward a copy thereof to ail the Principal Secretary/Secretary, Home Department of the States or UTs, 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 UAPA Nodal Officer of CTCR Division of MHA 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.

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

7. CTCR Division of MHA would electronically forward the designated lists to the UAPA Nodal Officer of all States and UTs with the 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.

8. 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 Joint Secretary (CTCR), Ministry of Home Affairs, immediately within 24 hours at Fax No.011- 23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id jsctcr- mha@gov.in.

9. 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 would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary (CTCR), Ministry of Home Affairs at the Fax, telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also conveyed over telephone on 01123092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: jsctcr-mha@gov.in. MHA may also have the verification conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under section 51A of the UAPA would be issued, by the UAPA Nodal Officer of CTCR Division of MHA 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.

12. 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 coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State / UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act 1967.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

13. U.N. Security Council Resolution 1373 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.

14. To give effect to the requests of foreign countries under 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 UAPA Nodal Officer for CTCR Division for freezing of funds or other assets.

15. The UAPA Nodal Officer of CTCR Division of MHA, shall cause the request to be examined, within 5 working days, 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.

16. Upon receipt of the requests by these Nodal Officers from the UAPA nodal officer of CTCR Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

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

17. 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 and the State/UT Nodal Officers.

18. The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties 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 Nodal Officer of CTCR Division of MHA as per the contact details given in paragraph 4 (ii) above, within two working days.

19. The Joint Secretary (CTCR), MHA being the UAPA Nodal Officer for CTCR Division of MHA shall cause such verification, as may be required on the basis of

the evidence furnished by the individual/entity, and, if satisfied, he shall Pass an order, within 15 working days, 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 and the Nodal Officers of States/UTs. However, if it is not possible for any reason to pass an Order unfreezing the assets within 15 working days, the UAPA Nodal Officer of CTCR Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act, 1967.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, 1967 relating to funds, financial assets or economic resources or related services, would be communicated to all the banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all Registrars performing the work of registering immovable properties, through the State/UT Nodal Officer by CTCR Division of MHA.

Regarding prevention of entry into or transit through India

21. As regards prevention of entry into or transit through India of the designated individuals. 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.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under section 51A

23. The Nodal Officers of CTCR Division and Foreigners Division of 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.

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

(Piyush Goyal)

Joint Secretary to the Government of India

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.

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

Customer Due Diligence (CDD)

Customer Due Diligence is obtaining and using information about a customer over and above the basic identification information before enter in to any agreement and ongoing scrutiny of any transaction undertaken throughout the course of the business relationship with a customer to ensure that any transaction that is being conducted is consistent with the Institution's knowledge of the customer, the customer's business and risk profile, the sources of earning, purpose of the account, expected monthly turn over, expected mode of transactions, including, where necessary, the expected type of counterparties

Freezing

Prohibiting the transfer, conversion, disposition or movement of funds or other property on the basis of, and for the duration of the validity of, an order issued by a court of law or other competent authority

Inter-Mingling

Mixing profits or funds earned from legal activities with profits or funds earned from illegal activities

Immediate Family Member

Spouse, children and their spouses or partners, parents, siblings and their spouses and grandchildren and their spouses

Legal person

Any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association.

Money Laundering (M/L)

The involvement in any one transaction or series of transactions that assists a criminal in keeping, concealing or disposing of proceeds derived from illegal activities. Having reasons to believe that such funds are derived from unlawful activity he/she / any party shall be guilty of the offence of money laundering.

Smurfing

Breaking down a transaction into smaller transactions to avoid regulatory requirements or an investigation by the authorities

Terrorist Financing (T/F)

Provision or collection of funds by any means, directly or indirectly, to be used in full or in part to carry out terrorist acts or support terrorist groups which encompass both legitimate and criminal funds. Any person shall be guilty of the offence of financing of terrorists, if committed the above and be punished with imprisonment for a term not less than fifteen years and liable to a fine.

Third Party Customer

A person who transacts with the bank through a third party account in respect of which the third party is the customer of the Bank

Occasional Transactions

Any transaction, in relation to cash and electronic fund transfer, that is conducted by any person other than through an account in respect of which the person is the customer.

Occasional Customer

Any person who engages in an occasional transaction

One-off Customers

Who do not access their accounts maintained at the Bank on a regular basis for financial transactions, either physically or from an online account platform, the access to which, is provided by the Bank

Originator

The party who initiated the transfer of funds

Politically Exposed Person

An individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals.

Walk-in Customer

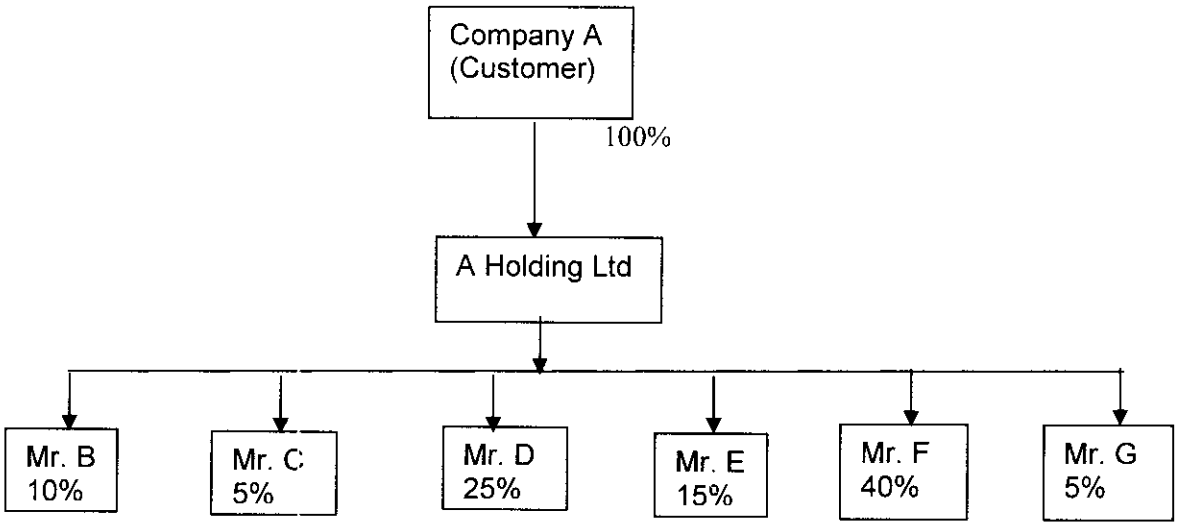
A person who is not a customer of the Bank to which he has presented himself, although the purpose of his visit is to obtain a financial service or to conduct a financial transaction with the Bank.

Wire Transfers

Any transaction carried out on behalf of an originator through an instruction by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary institution, irrespective of whether the originator and the beneficiary are the same person.

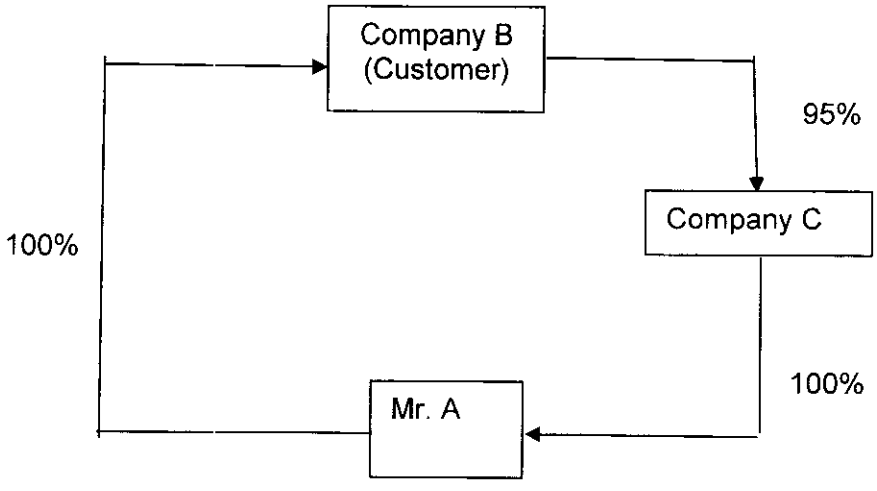
IDENTIFICATION OF BENEFICIAL OWNERSHIP

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



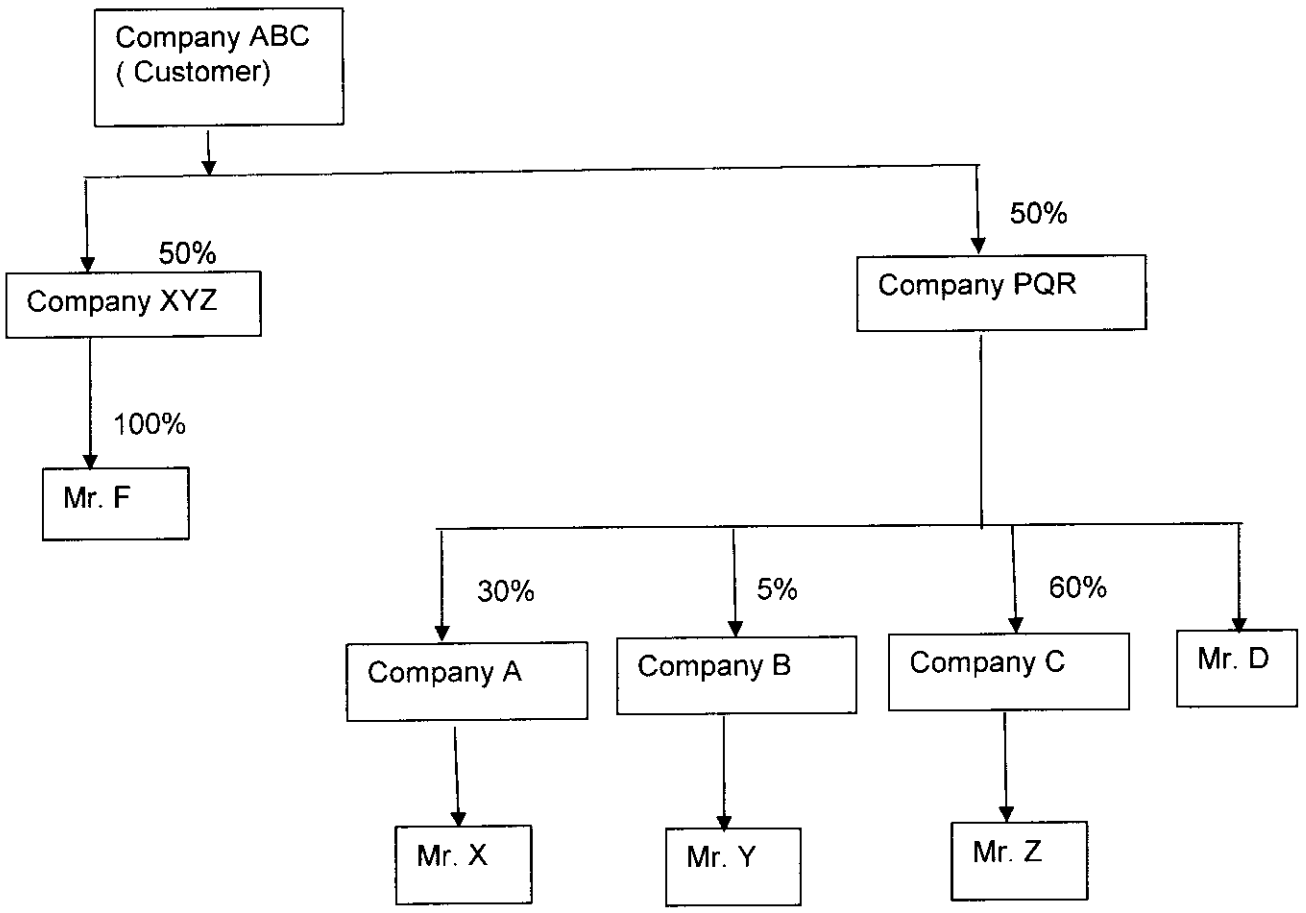
Mr B, Mr D, Mr E and Mr F are beneficial owners of the Company A.

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 share holding.

2. Effective Control

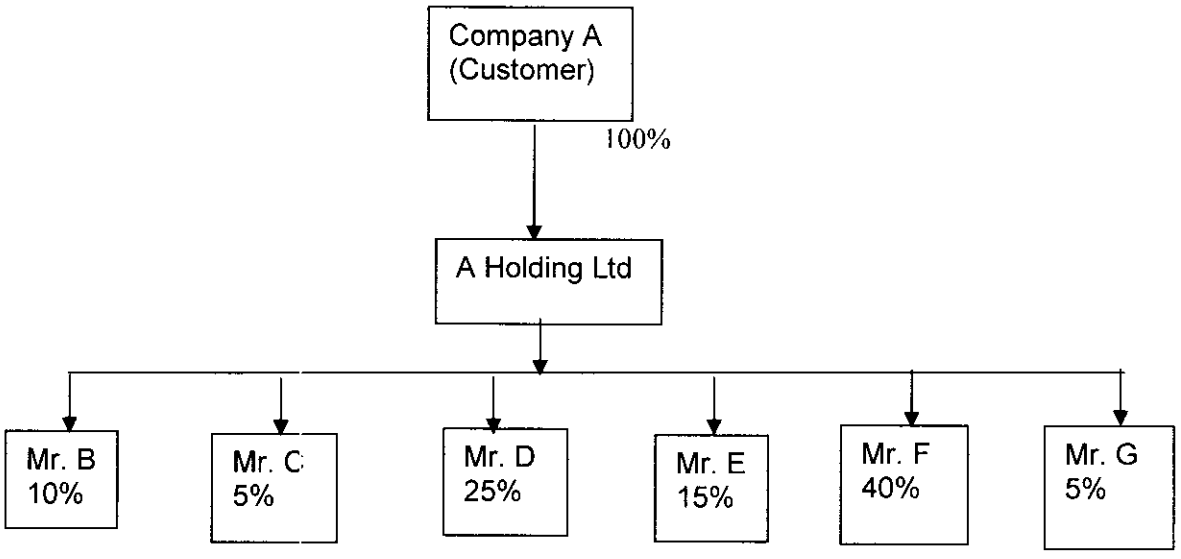
1. For some customers, ownership may be spread over a large number of individuals with all individual owing less than ten percent (10%). In such instance, the effective control would be more appropriate to determine the beneficial ownership.
2. Effective control can be direct or indirect, formal or informal. 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

Customer Identification	
Name and designation of natural person opening account	
Name, reg. no. and address of legal person for which the account is being opened	
Name, deed no., trustee and address of legal arrangement for which the account is being opened	

I declare that I:

☐ am the beneficial owner of the customer for this account

☐ am not the beneficial owner of the customer for this account

Complete identifying information of all beneficial owners that own or control 10% or more of the customer's equity, beneficial owners on whose behalf the account is being operated and persons who exercises effective control of the legal entity.

Name	**PAN/AADHAR or Passport (country of issue and citizenship)**	**Date of Birth**	**Current Address**	**Source of Beneficial Ownership 1=Equity (indicate%) 2=Effective Control 3=Person on whose behalf account is operated**	**PEP status**
					☐
					☐

1 beneficial owner as "a natural person who ultimately owns 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 politically exposed person "means an individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government of autonomous body but does not include middle rank or junior rank individual.

					☐
					☐
					☐
					☐
					☐
					☐
					☐
					☐

Details of the Customer authorized to act on behalf of entity

Name	
AADHAR/Passport	
Date of Birth	
Signature	
Verification of Beneficial Ownership	
For Office use only	
Name	
PF Number	
Date	

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.

Signature :

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 (iii) 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.
Location of Customer	Developing Countries, African Countries, South American Countries	Asian Countries, Russia and China	United States and European Countries
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

	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	One time transaction Less than Rs.20,000/- Cash Less than Rs.1 lacs non cash
Business Activity	(1) Jewellery (2) Chit Funds (3) Finance Companies (4) Foreign Exchange, Money Market Brokers (5) Travel Agencies (6) Export / Import Trade (7) S M Es with annual turnover xceeding Rs. 25 Crores and above	(i) Commodity Trade (ii) S M Es with annual turnover Rs. 10 Crores and above, but < Rs.25 Crores	(i) Industry (ii) Hotel (iii) Plantations (iv) S M Es 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

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