KERALA GRAMIN BANK

HEAD OFFICE: MALAPPURAM

STRATEGIC PLANNING & DEVELOPMENT WING

POLICY ON

KNOW YOUR CUSTOMER (KYC) NORMS
ANTI-MONEY LAUNDERING (AML) STANDARDS
COMBATING FINANCING OF TERRORISM (CFT) AND
OBLIGATION OF BANKS UNDER PREVENTION OF MONEY LAUNDERING ACT (PMLA), 2002
FOR THE FINANCIAL YEAR 2025-26

VERSION 9.0

Document Title	**KNOW YOUR CUSTOMER (KYC) NORMS, ANTI-MONEY LAUNDERING (AML) STANDARDS, COMBATING FINANCING OF TERRORISM (CFT) AND OBLIGATION OF BANKS UNDER PREVENTION OF MONEY LAUNDERING ACT (PMLA), 2002**
Document Classification	Internal

Version History

Version No	Board No	Date	Type of Document/ Change/Comment	Changed By
1.0	8	25-07-2014	Initial Document	SPD Wing
2.0	18	27.01.2016	Version Change	SPD Wing
3.0	31	18-01-2018	Version Change	SPD Wing
4.0	43	02.01.2020	Version Change	SPD Wing
5.0	50	29.01.2021	Version Change	SPD Wing
6.0	56	03.02.2022	Version Change	SPD Wing
7.0	63	03.02.2023	Version Change	SPD Wing
8.0	69	13.02.2024	Version Change	SPD Wing

Version Approval

Version No	Board No.	Date	Type of Document/ Change/Comment	Approved by
1.0	8	25-07-2014	Initial Document	Board of Directors
2.0	18	27.01.2016	Version Change	Board of Directors
3.0	31	18-01-2018	Version Change	Board of Directors
4.0	43	02.01.2020	Version Change	Board of Directors
5.0	50	29.01.2021	Version Change	Board of Directors
6.0	56	03.02.2022	Version Change	Board of Directors
7.0	63	03.02.2023	Version Change	Board of Directors
8.0	69	13.02.2024	Version Change	Board of Directors
9.0	76	14.02.2025	Version Change	Board of Directors

Table of Contents

Sl No	Subject
1	Chapter I - Preliminary
2	Chapter II - General
3	Chapter III – Customer Acceptance Policy
4	Chapter IV – Risk Management
5	Chapter V – Customer Identification Procedure (CIP)
6	Chapter VI – Customer Due Diligence Procedure (CDD)
7	Chapter VII – Record Management
8	Chapter VIII – Reporting Requirements to Financial Intelligence Unit India (FIU)
9	Chapter IX – Requirements/Obligations under International Agreements
10	Chapter X – Other Instructions
11	Chapter XI – Repeal Provisions
12	Chapter XII- Combating Financing of Terrorism (CFT)
13	Chapter XIII – Anti Money Laundering (AML)
14	Annexure – I - Govt. Order on Procedure for Implementation of Section 51 A of the Unlawful Activities (Prevention) Act, 1967
15	Annexure – II – KYC documents for Eligible FPIs under PIS

INTRODUCTION

The objective of KYC (Know Your Customer), AML (Anti-Money Laundering), and CFT (Combating the Financing of Terrorism) guidelines is to prevent Bank from being used as channels for money laundering (ML) and terrorist financing (TF), while ensuring the integrity and stability of the financial system through the formulation and implementation of various rules and regulations.

Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In India, the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

The Reserve Bank of India issues the Directions in accordance with the exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act ibid, Sections 45JA, 45K and 45L of the Reserve Bank of India Act, 1934, Section 10 (2) read with Section 18 of Payment and Settlement Systems Act 2007 (Act 51 of 2007), Section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws.

In accordance with the above, the Bank has formulated a comprehensive policy on the subject as enumerated below.

CHAPTER – I

PRELIMINARY

1. Short Title and Commencement.

These Directions shall be called the Kerala Gramin Bank (Know Your Customer (KYC)) policy 2025-26

2. Applicability

These directions shall apply to all branches and offices of the Bank, provided that this rule shall not apply to 'small accounts' referred to in Section 18 of Chapter VI.

3. Definitions

In these Directions, 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: Aadhaar number shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. Act and Rules: 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: 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 a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

1. Controlling ownership interest means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

2. 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 10 percent of capital or profits of the partnership or who exercises control through other means.

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

c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

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

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

v. Certified Copy: Obtaining a certified copy by the Bank shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the bank.

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, 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): In terms of PML rules, "Central KYC Records Registry (CKYCR)" means an entity to receive, store, safeguard and retrieve the KYC records in digital form of a Customer.

vii. Designated Director: Designated Director means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include a person who holds the position of senior management or equivalent designated as a Designated Director. The name, designation & address of the Designated Director shall be communicated to the FIU-IND.

viii. Digital KYC: Digital KYC means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the bank as per the provisions contained in the Act.

ix. Digital Signature: Digital Signature shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

x. Equivalent e-document: Equivalent e-document means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

xi. Group: The term group shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961(43 of 1961).

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

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

xiv. Officially Valid Document (OVD):

The Officially Valid Documents are as under:

1. The Passport.
2. The Driving License.
3. Proof of possession of Aadhaar number*.
4. The Voter's Identity Card issued by Election Commission of India.
5. Job card issued by NREGA duly signed by an officer of the State Government.
6. Letter issued by the National Population Register containing details of name and address.

*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 (UIDAI) and Proof of possession of Aadhaar shall include the following:

a) Aadhaar letter issued by UIDAI which carry name, address, gender, photo and date of birth details of the Aadhaar number holder.
b) Downloaded Aadhaar (e-Aadhaar) which carries name, address, gender, photo and date of birth details of the Aadhaar number holder in similar form as in printed Aadhaar letter. This is digitally signed by UIDAI.
c) Aadhaar Secure QR code generated and digitally signed by UIDAI carries name, address, gender, photo and date of birth details of the Aadhaar number holder.
d) Aadhaar paperless offline e-KYC which is an XML document generated by UIDAI and digitally signed by UIDAI carries name, address, gender, photo and date of birth details of the Aadhaar number holder.

In case, Officially Valid Documents (OVDs) furnished by the customer does not contain updated address, the following documents or the equivalent e-documents there of shall be deemed to the 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 Department or Public Sector Undertakings, if they contain the address;
iv. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.

The Customer shall submit updated Officially Valid Document with current address within a period of three months of submitting the above document.

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.

xv. Person: Person has the same meaning assigned in the Act and includes: An individual, a Hindu undivided family, a company, a firm, an association of persons or a body of individuals, whether incorporated or not, every artificial juridical person, not falling within any one of the above persons and any agency, office or branch owned or controlled by any of the above persons.

xvi. Principal Officer: Principal Officer means an officer at the management level nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

xvii. Suspicious transaction: 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.

Xviii. Small Account means a savings account in which:

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

xix. Transaction: Transaction means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

i. Opening of an account;

ii. Deposits, 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;
iii. The use of a safety deposit box or any other form of safe deposit;
iv. Entering into any fiduciary relationship;
v. Any payment made or received in whole or in part of any contractual or other legal obligation; or
vi. Establishing or creating a legal person or legal arrangement.

(B) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. Common Reporting Standards (CRS): 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: 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: It 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):CDD means identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'proof of identity' and a 'proof of address'.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

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

taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

v. Customer identification: It means undertaking the process of CDD.

vi. Foreign Account Tax Compliance Act (FATCA): FACTA 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. Inter-Governmental Agreement (IGA): 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: It means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

ix. Non-face-to-face customers: It means customers who open accounts without visiting the branch/offices of the bank or meeting the officials of bank.

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

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

xii. Politically Exposed Persons (PEPs): 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.

xiii. Simplified procedure: It means the procedure for undertaking customer due diligence in respect of customers, who are rated as low risk by the bank and who do not possess any of the six officially valid documents, with the alternate documents prescribed under the two provisos of Section 3(a)(vi) of this Directions.

xiv. Shell Bank: It means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The

existence simply of a local agent or low-level staff does not constitute physical presence.

xv. Wire transfer: It 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.

xvi. 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.

xvii. Video based Customer Identification Process (V-CIP): V-CIP is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the bank by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to- face CIP.

(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, and Prevention of Money Laundering (Maintenance of Records) Rules 2005, the 30Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 any statutory modification or re- enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER – II
General

4. Know Your Customer (KYC) policy is duly approved by the Board of Directors of our bank.

5. The KYC policy shall include following four key elements:

a. Customer Acceptance Policy;

b. Risk Management;

c. Customer Identification Procedures (CIP); and

d. Monitoring of Transactions

6. Designated Director:

a. A Designated Director shall be nominated by the Board.

b. The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
c. In no case, the Principal Officer shall be nominated as the Designated Director.
d. Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.

7. Principal Officer:

a) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
b) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
c) Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

8. Compliance of KYC policy

Bank shall ensure compliance with KYC Policy through:

a) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
b) Allocation of responsibility for effective implementation of policies and procedures.
c) Independent evaluation of the compliance functions of bank's policies and procedures, including legal and regulatory requirements.
d) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
e) Submission of quarterly audit notes and compliance to the Audit committee.
f) Bank shall ensure that decision making functions of determining compliance with KYC norms are not outsourced.

CHAPTER – III

Customer Acceptance Policy

9. Customer Acceptance Policy of the bank is framed as below.

10. Without prejudice to the generality of the aspect that Customer Acceptance Policy 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 CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Bank shall

consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

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

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

e) Additional information, where such information requirement has not been specified in the this policy, is obtained with the explicit consent of the customer

f) CDD Procedure is followed for all the joint account holders, while opening a joint account.

g) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

h) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

i) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

j) Where an equivalent e-document is obtained from the customer, bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

k) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority

l) At our bank, the CDD procedure shall be applied at the Unique Customer Identification Code (UCIC) level. Therefore, if an existing customer, who is already compliant with our KYC requirements, wishes to open an additional account or avail themselves of any other product or service offered by the bank, a fresh CDD process will not be required for customer identification purposes.

11. 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.

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

CHAPTER – IV

Risk Management

12. For Risk Management, bank has a risk based approach which includes the following.

a. Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception of the bank.
b. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc.
c. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive.

Chapter V

Customer Identification Procedure (CIP)

13. Bank shall undertake identification of customers in the following cases:

a. Commencement of an account-based relationship with the customer.
b. Carrying out any international money transfer operations for a person who is not an account holder of the bank.
c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
d. Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
e. Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
f. 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.
g. Bank shall ensure that introduction is not to be sought while opening accounts

14. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, bank shall , at its option, rely on customer due diligence done by a third party, subject to the following conditions:

a. Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from

the Central KYC Records Registry.

b. Adequate steps are taken by bank to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

c. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

d. The third party shall not be based in a country or jurisdiction assessed as high risk.

e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the bank.

Chapter VI

Customer Due Diligence (CDD) Procedure

Part I CDD Procedure in case of Individuals

15. Bank shall obtain the following documents from an individual while establishing an account based relationship:

a) one certified copy of an OVD as mentioned at Section **3(a)(xiv)** of Chapter I, containing details of identity and address;

b) one recent photograph;

c) Such other documents pertaining to the nature of business or financial status provided that 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.

d) The KYC Identifier with an explicit consent to download records from CKYCR.

16. The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification under the PML Rules, as

a) the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document', and

b) Transfer of KYC data, electronically to the bank from UIDAI, is accepted as valid process for KYC verification.

Provided bank/ Business Correspondents (BCs)/ Business Facilitators (BFs) shall obtain authorisation from the individual user authorising UIDAI by way of explicit consent to release his/her identity/address through biometric authentication to the bank.

Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.
ii. As a risk-mitigating measure for such accounts, transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar.
iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (vi) below is complete.
iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per paragraph 13 or as per paragraph 15 (V-CIP) is carried out. If Aadhaar details are used under paragraph 15, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
vii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non- face-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face- to-face mode.
viii. Bank has a monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

ix. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
x. Bank shall print/download directly, the prospective customer's e-Aadhaar letter from the UIDAI portal if such a customer knows only his/her Aadhaar number or if the customer has only a copy of Aadhaar downloaded from a place/source elsewhere, provided the prospective customer is physically present in the branch/ office of the bank

17. As per RBI directions, bank may undertake V-CIP to carry out:

a. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
   Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in CDD Measures for Sole Proprietary firms, apart from undertaking CDD of the proprietor.
b. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per section 14
c. Updation/Updation/ periodic updation of KYC for eligible customers.

(a) V-CIP Infrastructure

i) Bank has complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. Bank has ensured that the technology infrastructure housed in our own premises and the V-CIP connection and interaction originate from our own secured network domain. All technology related outsourcing for the process be complied with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Bank only and all the data including video recording is transferred to the Bank's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Bank.

ii) Bank ensured that end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

iv) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Bank.

   Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP

shall be reported as a cyber-event under extant regulatory guidelines.

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

i) Bank has formulated a work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the RE specially trained for this purpose. The official should be capable to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the bank. However, in case of call drop / disconnection, fresh session shall be initiated.

iii) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

iv) Any prompting observed at end of customer shall lead to rejection of the account opening process.

v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work-flow.

vi) The authorised official of the Bank performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

(a) OTP based Aadhaar e-KYC authentication

(b) Offline Verification of Aadhaar for identification

(c) KYC records downloaded from CKYCR, in accordance with CDD Procedure and sharing KYC information with Central KYC Records Registry, using the KYC identifier provided by the customer.

(d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker Bank shall ensure to redact or blackout the Aadhaar Number

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, Bank ensured that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However Bank ensured that no incremental risk is added due to this.

vii) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

viii) Bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through DigiLocker.

ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

x) The authorised official of the Bank shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

xi) Assisted V-CIP shall be permissible when banks take help of Business Correspondents (BCs) facilitating the process only at the customer end. Banks shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the bank.

xii) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of

process and its acceptability of the outcome.

xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the RE.

(c) V-CIP Records and Data Management

i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. Bank ensured that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this MD, shall also be applicable for V-CIP.

ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

18. A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

a. In case the person who proposes to open an account does not have an OVD as 'proof of address', such person shall provide OVD of the relative as provided at sub-section 77 of Section 2 of the Companies Act, 2013, read with Rule 4 of Companies (Specification of definitions details) Rules, 2014, with whom the person is staying, as the 'proof of address'.

Explanation: A declaration from the relative that the said person is a relative and is staying with him/her shall be obtained

19. In cases where a customer categorised as 'low risk', expresses inability to complete the documentation requirements on account of any reason that the bank consider to be genuine, and where it is essential not to interrupt the normal conduct of business, bank shall, at its option, complete the verification of identity of the customer within a period of six months from the date of establishment of the relationship.

20. In case an individual customer who does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at Section OVD) and desires to open a bank account, banks shall open a 'Small Account',.

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 designated 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) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and 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) 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 mentioned in OVDs and VCIP**.**

h) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per OVDs and VCIP**.**

21. KYC verification once done by one branch/office shall be valid for transfer of the account to any other branch/office, provided full KYC verification has already been done for the concerned account and the same is not due for updation/ periodic updation and a self-declaration from the account holder about his/her current address is obtained in such cases.

Part II - CDD Measures for Sole Proprietary firms

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

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

a. Registration certificate including Udyam Registration Certificate (URC) issued by the Government
b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
c. Sales and income tax returns.
d. CST/VAT /GST certificate
e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / License / Certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. 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.
h. Utility bills such as electricity, water, and landline telephone bills.

24. In cases where the bank is satisfied that it is not possible to furnish two such documents, bank may, at its 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

25. For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
a. Certificate of incorporation.
b. Memorandum and Articles of Association.
c. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
d. Officially valid documents in relating to beneficial owner, managers, officers or employees holding an attorney to transact on the company's behalf.
e. Permanent Account Number of the company
f. The names of the relevant persons holding senior management position; and
g. The registered office and the principal place of its business, if it is different.

26. For opening an account of a partnership firm, one certified copy of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Registration certificate.

b. Partnership deed.

c. Officially valid documents in relating to beneficial owner, managers, officers or employees holding an attorney to transact on the its behalf

d. Permanent Account Number of the partnership firm

e. the names of all the partners and

f. Address of the registered office, and the principal place of its business, if it is different.

27. **For opening an account of a trust**, one certified copy of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Registration certificate.

b. Trust deed.

c. Officially valid documents in relating to beneficial owner, managers, officers or employees holding an attorney to transact on the its behalf.

d. Permanent Account Number or Form No.60 of the trust

e. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust

f. The address of the registered office of the trust; and

g. list of trustees and documents, as specified in Section CDD procedure, for those discharging the role as trustee and authorised to transact on behalf of the trust.

h. Provided that in case of a trust, the branch shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of Customer Identification Procedure**.**

27 A. For opening an account of an unincorporated association or a body of individuals, one certified copy of each of the following documents or the equivalent e-documents thereof shall be obtained:

a. Resolution of the managing body of such association or body of individuals.

b. Power of attorney granted to transact on its behalf;

c. Officially valid documents in relating to beneficial owner, managers, officers or employees holding an attorney to transact on the its behalf

d. Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.

e. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals.

Explanation: Unregistered trusts/partnership firms shall be included under the term ‘unincorporated association’.

"Explanation: Term 'body of individuals' includes societies".

27 B. For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

i. Document showing name of the person authorized to act on behalf of the entity;
ii. Officially valid documents for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf and
iii. Such documents as may be required to establish the legal existence of such an entity/juridical person.

Part IV - Identification of Beneficial Owner

28. 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. Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
b. In cases of 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 - On-going Due Diligence

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

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

(a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

(b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
(c) High account turnover inconsistent with the size of the balance maintained.
(d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

31. The extent of monitoring shall be aligned with the risk category of the customer.

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.
b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

32. Updation/ periodic updation of KYC

Bank shall adopt a risk-based approach for updation/ periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant. updation/ periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

a. Individual Customers:

i. No change in KYC information**:** In case of no change in the KYC information, a self- declaration from the customer in this regard shall be obtained through customer's email-id registered, customer's mobile number registered, ATMs, digital channels (such as online banking / internet banking, mobile application), letter etc.
ii. Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered, customer's mobile number registered, ATMs, digital channels (such as online banking / internet banking, mobile application), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.
Bank must obtain a copy of OVD or deemed OVD or the equivalent e- documents thereof, as defined in Section **1(a)(xiv),** for the

purpose of proof of address, declared by the customer at the time of updation/ periodic updation.

iii. Accounts of customers who were minor at the time of opening account on their becoming major**:** In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time its shall be ensured that CDD documents as per the current CDD standards are available. Wherever required, bank must carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

iv. On- going Due Diligence – Updation/periodic Updation of KYC:

Aadhaar OTP based e-KYC in non-face to face mode may be used for Updation/ periodic updation. To clarify, conditions stipulated in Section 14 are not applicable in case of updation / updation/ periodic updation of KYC through Aadhaar OTP based e-KYC in non- face to face mode.

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

b. Customers other than individuals:

i. **No change in KYC information**: In case of no change in the KYC information of the LE customer, a self-declaration in this regard shall be obtained from the LE customer through its email id registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application), letter from an official authorized by the LE in this regard, board resolution etc. Further, banks shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to- date as possible.

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

c. Additional measures: In addition to the above, banks shall ensure that

i. The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available are not as per the current CDD standards. Further, in case the validity of the CDD documents available has expired at the time of updation/ periodic updation of KYC, bank shall undertake the KYC process

equivalent to that applicable for on-boarding a new customer.

ii. Customer's PAN details, if available, is verified from the database of the issuing authority at the time of updation/ periodic updation of KYC.

iii. An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation/ periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation/ periodic updation of KYC are promptly updated in the Records / database of bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. Bank adopts a risk-based approach with respect to updation/ periodic updation of KYC**.** In order to ensure customer convenience, the facility of updation/ periodic updation of KYC of a customer should be made available at any of our branch.

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

Partial freezing and closure of accounts

(a) Where bank is unable to comply with the CDD requirements mentioned at Part I to V above, bank shall not open accounts, commence business relations or perform transactions. In case of existing business relationship which is not KYC compliant, bank shall ordinarily take step to terminate the existing business relationship after giving due notice.

(b) As an exception to the Rule, instead of terminating business relationship straight away an option for a phased closure of operations in this account as explained below:

i. The option of 'partial freezing' shall be exercised after giving due notice of **30** days to the customers to comply with ongoing CDD.

ii. Thereafter, 'partial freezing' shall be imposed by allowing all credits and disallowing all debits with the freedom to close the accounts in case of the account being non-compliant to KYC and CDD after **30** days of issuing first notice.

iii. All debits and credits from/to the accounts shall be disallowed, in case of the account being KYC non-compliant after **30** days of imposing 'partial freezing',

iv. The account holders shall have the option, to revive their accounts by submitting the KYC documents and along with

complying CDD procedure.

(c) When an account is closed without 'partial freezing' or after 'partial freezing', the reason for that shall be communicated to account holder.

(d) For all newly opened accounts, branches must invariably send a thank-you letter to the customer for the completion of Customer Due Diligence (CDD) process. This requirement applies to all account types, including those opened under various schemes. If the thank-you letter is not accepted by the customer, the branch must conduct a Contact Point Verification (CPV) to confirm the authenticity of the customer. If the CPV fails, the account may be partially frozen immediately, and a letter of intimation regarding the partial freeze must be sent to the account holder(s). If the account holder(s) fail to provide a valid justification for the discrepancies within 30 days of receiving the intimation letter, the account may be closed.

Part VI - Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

33. Accounts of non-face-to-face customers:

Bank shall undertake additional procedures i.e., certification of all the documents presented, calling for additional documents and the first payment to be effected through the customer's KYC complied account with any another bank, for enhanced due diligence of non-face to face customers.

34. Accounts of Politically Exposed Persons (PEPs)

A. Bank has the option of establishing a relationship with PEPs provided that that, apart from performing normal customer due diligence bank has to ensure:

(a) the identity of the person shall have been verified before accepting the PEP as a customer;

(b) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

(c) the decision to open an account for a PEP is taken at a senior level

(d) all such accounts are subjected to enhanced monitoring on an on-going basis;

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

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

35. Client accounts opened by professional intermediaries:

Bank shall ensure while opening client accounts through professional intermediaries, that: CDD is carried out as per the guidelines and bank may rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. Bank does not normally open accounts in this manner.

B. Simplified Due Diligence

36. Simplified norms for Self Help Groups (SHGs)

CDD of all the members of SHG may be undertaken at the time of credit linking of SHGs.

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

a. Bank 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.

38. Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex II, subject to Income Tax (FATCA/CRS) Rules.

Chapter VII
Record Management

39. 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, for at least five years from the date of transaction

(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.

Explanation. –the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

39A. Bank shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

Chapter VIII

Reporting Requirements to Financial Intelligence Unit - India

40. 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.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule

(1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

41. The reporting is done as per the formats and comprehensive reporting format guide, prescribed/ released by FIU-IND , continuation missing

42. 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. 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.

43. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

Chapter IX

Requirements/obligations under International Agreements Communications from International Agencies

44. Bank shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, they 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"**, established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/ohz5jen- al-qaida.html

b. The **"Taliban Sanctions List"**, established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.html

Bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the bank for meticulous compliance.

45. 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 August 27, 2009.

46. 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.

47. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967.

The procedure laid down in the UAPA Order dated Feb 2, 2021 (Annex I) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

48. 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 in Section 55 a & b do not preclude REs 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.

Chapter X

Other Instructions

49. 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, banks 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:

   i. Where there is a duty to the public to disclose,

   ii. the interest of bank requires disclosure,

   iii. Where the disclosure is made with the express or implied consent of the customer and,

   iv. Where disclosure is under compulsion of law.

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

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

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

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

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

e. Being a nonscheduled commercial Bank, Bank shall start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.

f. KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

g. Once KYC Identifier is generated by CKYCR, same is communicated to the individual/LE as the case may be.

h. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per clauses (e) and (f), respectively, at the time of periodic updation, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the Bank obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs Bank regarding an update in the KYC record of an existing customer, Bank shall retrieve the updated KYC records

from CKYCR and update the KYC record maintained by Bank.

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

j. For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the Bank shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

(i) there is a change in the information of the customer as existing in the records of CKYCR; or

(ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or

(iii) the validity period of downloaded documents has lapsed; or

(iv) the bank considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

51. 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. Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login - -> My Account --> Register as Reporting Financial Institution,

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

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

c. Develop Information Technology (IT) framework for carrying out due diligence

d. Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

e. Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

f. 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. REs may take note of the following:

a) updated Guidance Note on FATCA and CRS

b) a press release on 'Closure of Financial Accounts' under Rule 114H (8).

52. Period for presenting payment instruments

Payment of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

53. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." If it is established that an account opened and operated is that of a Money Mule, but no STR it shall be deemed that the bank has not complied with these directions.

54. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituent shall not be collected. Bank shall, at its option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of their customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co- operative credit societies.

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

(b) The bank shall, at its option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

56. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS 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. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

57. Issue and Payment of Demand Drafts, etc.

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

58. Quoting of PAN

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

59. Selling Third party products

Bank acting as agent while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

a. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand.
b. transaction details of sale of third party products and related records shall be maintained.
c. AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
d. transactions involving rupees fifty thousand and above shall be undertaken only by:
    i. debit to customers' account or against cheques; and
    ii. obtaining and verifying the PAN given by the account based as well as walk-in customers.
e. Instruction 'a' to 'd' above shall also apply to sale of banks own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

Chapter XI

Repeal Provisions

60. With the issue of these directions, the instructions / guidelines contained in the circulars mentioned in the Appendix, issued by the Reserve Bank stand repealed.

61. All approvals / acknowledgements given under the above circulars shall be deemed as given under these directions.

62. All the repealed circulars are deemed to have been in force prior to the coming into effect of these directions.

Chapter XII

Combating Financing of Terrorism (CFT)

63. The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC).

Name screening is done during opening of accounts for screening of individuals and entities, suspected of having terrorist links, and as approved by Security Council (UNSC). The list circulated by UNSC is periodically updated in the system.

-

(a) **The "Al-Qaida Sanctions List",** includes names of individuals and entities associated with the Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml.

(b) The **"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at http://www.un.org/sc/committees/ 1988/list.shtml.

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Banks are required to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, discussed below. Banks should ensure that they do not have any account in the name of individuals/entities appearing in the above lists. Details of accounts resembling any of the individuals/entities in the list should be reported to FIU-IND.

64. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

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

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

b. Bank is required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex II of this Master Circular) and ensure meticulous compliance to the Order issued by the Government.

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

a. Bank is required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, Bank should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that Bank should also give special attention 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.

b. Bank should examine 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. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

Chapter XIII

ANTI MONEY LAUNDERING (AML)

Anti-Money Laundering (AML) refers to a set of procedures, laws and regulations designed to eliminate the practice of generating income through illegal actions. AML regulations requires institutions issuing credit or allowing customers to open accounts to complete due-diligence procedures to ensure they are not aiding in money- laundering activities. Anti-money-laundering laws and regulations target activities that include market manipulation, trade of illegal goods, corruption of public funds and tax evasion, as well as the activities that aim to conceal these deeds. Fighting money laundering is a highly effective way to reduce overall

crime.

66. Reporting Requirements- General Guidelines to banks furnished below

Maintenance of the records of the identity of clients;

i. Every reporting entity shall maintain the physical copy of records of the identity of its clients obtained in accordance with rule 9, after filing the electronic copy of such records with the Central KYC Records Registry.
ii. The record of the identity of clients shall be maintained by a reporting entity in the manner as may be specified by the Regulator from time to time.
iii. Where the reporting entity does not have records of the identity of its existing clients, it shall obtain the records within the period specified by the regulator, failing which the reporting entity shall close the account of the clients after giving due notice to the client.

Explanation: For the purpose of this rule, the expression records of the identity of clients shall updated records of the identification data, account files and business correspondence and result of any analysis undertaken under maintenance of record transaction and Client due Diligence

a) Reporting to Financial Intelligence Unit – India

(i) In terms of the Rule 3 of the PML (Maintenance of Records) Rules, 2005, Banks are required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations (NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (erstwhile Section 25 of Companies Act, 1956) under Section 8 of the Companies Act, 2013), cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi-110021 Website - http://fiuindia.gov.in/

(ii) FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website. Banks should carefully go through all the reporting formats prescribed by FIU-IND.

(iii) FIU-IND have placed on their website editable electronic utilities to file

electronic Cash Transactions Report (CTR)/ Suspicious Transactions Report (STR) to enable Banks which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of those Banks, where all the branches are not fully computerized, the Principal Officer of the Bank should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in

(iv) In terms of Rule 8, 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 constitute a separate violation. Banks are advised to take note of the timeliness of the reporting requirements.

In terms of instructions contained in paragraph 3.4 (b) of this Master Circular, Banks are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 3.2.2. (III), the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that, as a part of their transaction monitoring mechanism, Banks are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

b) Reports to be furnished to FIU-IND

1. Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, Banks should scrupulously adhere to the following:

(i) The CTR for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis and Banks should ensure to submit CTR for every month to FIU- IND within the prescribed time schedule.

(ii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

(iii) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

(iv) A summary of cash transaction reports for the bank as a whole should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU- IND. In case of CTRs compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre,

banks may generate centralised CTRs in respect of the branches under core banking solution at one point for onward transmission to FIU-IND, provided the CTR is to be generated in the format prescribed by FIU-IND;

(v) A copy of the monthly CTR submitted to FIU-India in respect of the branches should be available at the branches for production to auditors/inspectors, when asked for.

(vi) The instruction on 'Maintenance of records of transactions'; and 'Preservation of records' as contained above in this Master Circular at Para 6.1 and 6.2 respectively should be scrupulously followed by the branches.

(vii) However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU- IND.

2.Suspicious Transaction Reports (STR)

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

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

(ii) Banks should make STRs if they have 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.

(iii) The STR should be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

(iv) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in 'IBA's Guidance Note for Banks, January 2012'.

(v) Banks should not put any restrictions on operations in the accounts where an STR has been filed. Banks and their employees should keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

3. Non - Profit Organisation Transaction Reports (NTR)

The report of all transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency should be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

4. Counterfeit Currency Report (CCR)

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer of the bank to FIU- IND in the specified format(Counterfeit Currency Report – CCR), by 15thday of the next month. These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

5. Cross-border Wire Transfer

Cross-border Wire Transfer Report (CWTR) is required to be filed with FIU-IND by 15^{the} of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India

Annex I

File No. 14014/01/2019/CFT

Government of India
Ministry of Home Affairs
CTCR Division

North Block, New Delhi.
Dated: the 2nd February, 2021

ORDER

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

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

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

a. freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
b. prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
c. Prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under: -

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

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

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

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA **[Telephone Number: 011-23092548, 011-23092551 (Fax), email address: jsctcr-mha@gov.in].**

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a

UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

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

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

3.6 The Financial Regulators shall forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies.

3.7 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the consolidated list of UAPA Nodal Officers to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs.

4. Communication of the list of designated individuals/entities:

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3 In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an orders to freeze these assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer

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

The order shall be issued without prior notice to the designated individual/entity.

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

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

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

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

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

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

The order shall be issued without prior notice to the designated individual/entity.

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

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

(i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.

(a) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above. Further, if the dealers hold any assets or funds of the designated individual/entity, either directly or indirectly, they shall freeze the same without delay and inform the UAPA Nodal officer of the State/UT.

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

(iii) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above.

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

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

owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

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

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

9. Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs 5 and 6 above shall be followed.

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

10. Regarding exemption, to be granted to the above orders in accordance with UNSCR 1452.

10.1 The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the Central [designated] nodal officer of the UAPA to be:-

(a) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

(b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA;

10.2. The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 10 of:

(a) Interest or other earnings due on those accounts, or

(b) Payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of resolutions 1267 (1999), 1333 (2000), or 1390 (2002),

Provided that any such interest, other earnings and payments continue to be subject to those provisions;

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

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

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

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

11. (A) **Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/organisations in the event of delisting by the UNSCR 1267 (1999), 1988 (2011) and 1989 (2011) Committee**

Upon making an application in writing by the concerned individual/organisation, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs., who in turn shall forward the application along with the full details of the assets frozen to the Central [Designated] Nodal Officer for UAPA within two working days. The Central [Designated]

Nodal Officer for UAPA shall examine the request in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and cause such verification as may be required and if satisfied, shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services owned or held by the applicant under intimation to concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs.

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

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

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

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

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

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

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

Annex II

KYC documents for eligible FPIs under PIS

		FPI Type		
Document Type		**Category I**	**Category II**	**Category III**
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN Card	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution	Exempted *	Mandatory	Mandatory
	List	Mandatory	Mandatory	Mandatory

	Proof of Identity	Exempted *	Exempted *	Entity
Senior Management (Whole Time Directors/ Partners/ Trustees/ etc.)				declares* on letter head full name, nationality, date of birth or submits photo identity
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

Authorized Signatories	List and Signatures	Mandatory – list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

	List	Exempted *	Mandatory (can declare “no UBO	Mandatory

			over 25%")	
Ultimate Beneficial Owner (UBO)	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

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

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