# Rajasthan Marudhara Gramin Bank

Department of Planning & Development and
Risk Management
Head Office Jodhpur

# RMGB KYC POLICY

| | |
|---|---|
| Version | 4 |
| Date of Adoption | 12-01-2015 |
| Date of last Review | 13-09-2022 |
| Renewal Frequency | Annual |

**Rajasthan Marudhara Gramin Bank**
**RMGB KYC Policy**

## INDEX

# RMGB KYC Policy

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, and RBI Master Directions on KYC (updated as on 10May 2021) our Bank has to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. RMGB should take steps to implement the provisions of the aforementioned Act & Rules and Master Directions, including operational instructions issued in pursuance of such amendment(s).

2. Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act ibid, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India has issued KYC Master directions, basis which the KYC policy of the Bank is formulated, which is as above.

## CHAPTER – I

## PRELIMINARY

### 1. Short Title and Commencement.

**(a)** This policy will be called the Know Your Customer (KYC) Policy of RMGB.

**(b)** This policy shall come into effect on the day of adoption of the policy from the Board.

### 2. Applicability

**(a)** The provisions of this policy will to every branch/offices/BCs of Rajasthan Marudhara Gramin Bank where the customer on boarding and maintenance is taking place, except where specifically mentioned otherwise.

**(b)** Provided that this rule will not apply to 'small accounts' referred to in Section 23 of Chapter VI of KYC Master Direction – 2016 issued by RBI vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 and as specified in this policy document.

### 3. Definitions

In this policy 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:

The Bank means "Rajasthan Marudhara Gramin Bank" with all its branches and other offices.

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

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

iv. Beneficial Owner (BO)

a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have 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 25 per cent 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 share-holders agreements orvoting agreements.

b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

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

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

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

v. Certified Copy" - 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 RE as per the provisions contained in the Act.

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

vii. "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. A person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks. General Manager (Audit) is nominated ex officio as the Designated Director.

viii. "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 authorized officer of the bank as per the provisions contained in the Act.

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

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

xii. "Non-profit organizations" (NPO) means any entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

xiii. "Officially Valid Document" (OVD) means the passport, the driving licence, 9proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

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

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address –

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

ii. property or Municipal tax receipt;

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

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

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above.

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

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

a. an individual,

b. a Hindu undivided family,

c. a company,

d. a firm,

e. an association of persons or a body of individuals, whether incorporated or not,

f. every artificial juridical person, not falling within any one of the above persons (a to e), and

g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvi. "Principal Officer" means an officer nominated by the bank, responsible for furnishing information as per rule 8 of the Rules. Chief Compliance Officer is nominated ex officio as the Principal Officer.

xvii. "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. A 'Small Account' means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23.

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

a. opening of an account;

b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

c. the use of a safety deposit box or any other form of safe deposit;

d. entering into any fiduciary relationship;

e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or

f. establishing or creating a legal person or legal arrangement.

xx. "Video based Customer Identification Process (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorized 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 for the purpose of this policy.

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

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

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

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

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

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

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

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

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

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

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

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

xii. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions 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. "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

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

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

**(c)** All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the 14Aadhaar (Targeted Delivery

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

## CHAPTER – II

## General

**4. This policy will be presented to the Board of Directors.**

**5. This KYC policy includes following four key elements:**

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

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

(a) The Bank will carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.
The assessment process considers all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Bank will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.

(b) The risk assessment by the bank will be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the bank. Further, the periodicity of risk assessment exercise will be determined by the Board of the bank, in alignment with the outcome of the risk assessment exercise. It will be reviewed at least annually.

(c) The outcome of the exercise will be presented to the audit committee of the Board, and will be available to competent authorities and self-regulating bodies.

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

**6. Designated Director:**

**(a)** A "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 be nominated by the Board. General Manager (Audit) is nominated ex officio as the Designated Director.

**(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'.

## 7. Principal Officer:

**(a)** The Principal Officer will 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 will be communicated to the FIU-IND.

## 8. Compliance of KYC policy

**(a)** the bank will ensure compliance with KYC Policy through:

i. General Managers & Regional Managers constitute 'Senior Management' for the purpose of KYC compliance.

ii. Effective implementation of policies and procedures is the responsibility of each RM and Branch Manager of the bank.

iii. Independent evaluation of the compliance functions of bank's KYC policy and procedures, including legal and regulatory requirements shall be done during RFIA.

iv. Concurrent/internal audit system will verify the compliance with KYC/AML policies and procedures.

v. Quarterly audit notes and compliance will be submitted to the Audit Committee.

**(b)** Decision-making functions of determining compliance with KYC norms will not outsourced.

# CHAPTER – III

## Customer Acceptance Policy

**9.** The Bank has a Customer Acceptance Policy.

**10.** Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, The Bank will 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.

**(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 periodic updation, is specified.

**(e)** 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

**(f)** The Bank will apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the bank desires to open another account with the same the bank, there shall be no need for a fresh CDD exercise.

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

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

**(i)** 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.

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

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

**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.

## CHAPTER – IV

## Risk Management

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

**(a)** Customers shall be categorised as low, medium and high risk category, based on the assessment and risk perception of the bank

**(b)** Risk categorisation will 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 etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

## CHAPTER - V

## Customer Identification Procedure (CIP)

**13.** The Bank will undertake identification of customers in the following cases

**(a)** Commencement of an account-based relationship with the customer.

**(b)** When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

**(c)** Selling third party products as agents, selling our own products.

**(d)** 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.

**(e)** When the bank has a 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.

**(f)** The Bank shall ensure that introduction is not to be sought while opening accounts.

## CHAPTER - VI

## Customer Due Diligence (CDD) Procedure

### Part I - Customer Due Diligence (CDD) Procedure in case of Individuals

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

**(a)** the Aadhaar number where,

i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

ii. he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act;

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and

**(b)** the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

**(c)** such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank:

Provided that where the customer has submitted,

i. Aadhaar number under clause (a) above to a bank notified under first proviso to sub-section (1) of section 11A of the PML Act, the bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the bank.

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

iii. an equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

iv. any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC as specified under Annex I.

Provided that for a period not beyond such date as may be notified by the Government for a class of the bank, instead of carrying out digital KYC, the bank pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other

subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. The Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Explanation 1: The Bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies

Benefits and Services) Act, 2016 and the regulations made thereunder.

**15.** Accounts opened using 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. 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 (v) below is complete.

iii. the aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.

iv. Deposit Accounts, opened using OTP based e-KYC will not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

v. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately.

vi. A declaration will 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 financial institution. Further, while uploading KYC information to CKYCR, the Bank will clearly indicate that such accounts are opened using OTP based e-KYC and other financial institution shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

vii. The Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

**16.** The Bank will undertake V-CIP to carry out:

i. 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, the Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28, apart from undertaking CDD of the proprietor.

ii. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

iii. Updation/Periodic updation of KYC for eligible customers.

The Bank will adhere to the following minimum standards:

**(a) V-CIP Infrastructure**

a) The 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. The technology infrastructure should be housed in own premises of the bank and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines.

b) The bank will ensure 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.

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

d) 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.

e) 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

f) 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.

g) 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 suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

h) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, 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**

a) Each RE shall formulate a clear 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 liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

b) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

c) 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.

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

e) 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.

f) 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 Section 56, using the KYC identifier provided by the customer
   d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

   The bank shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

   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 3 days from the date of carrying out V-CIP.

   Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, the bank shall ensure that the video process of the V-CIP is undertaken within three 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, REs shall ensure that no incremental risk is added due to this.

g) 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.

h) The 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.

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

j) The authorised official of the bank will 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.

k) 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.

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

**(c) V-CIP Records and Data Management**

a) The entire data and recordings of V-CIP will be stored in a system / systems located in India. The Bank will ensure 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 policy, will also be applicable for V-CIP.

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

**17.** Notwithstanding anything contained in Section 16 and as an alternative thereto, in case an individual who desires to open a bank account, the bank will open a 'Small Account', which entails the following limitations:

i. the aggregate of all credits in a financial year does not exceed rupees one lakh;

ii. the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

iii. the balance at any point of time does not exceed rupees fifty thousand.

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

Further, small accounts are subject to the following conditions:

i. The bank shall obtain a self-attested photograph from the customer.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. The entire relaxation provisions shall be reviewed after twenty-four months.

vii. Notwithstanding anything contained in clauses (e) and (f) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.

viii. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established as per Section 16.

ix. Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 16.

**18.** KYC verification once done by one branch/office of the bank shall be valid for transfer of the account to any other branch/office of the same bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

## Part II - CDD Measures for Sole Proprietary firms

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

**20.** 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

**(b)** Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

**(c)** Sales and income tax returns.

**(d)** CST/VAT/ GST certificate (provisional/final).

**(e)** Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

**(f)** IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/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, landline telephone bills, etc.

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

Provided REs undertake 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

**22.** 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)** Permanent Account Number of the company

**(d)** A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

**(e)** Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

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

**(a)** Registration certificate

**(b)** Partnership deed

**(c)** Permanent Account Number of the partnership firm and

**(d)** Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

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

**(a)** Registration certificate

**(b)** Trust deed

**(c)** Permanent Account Number or Form No.60 of the trust

**(d)** Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

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

**(a)** Resolution of the managing body of such association or body of individuals

**(b)** Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals

**(c)** Power of attorney granted to transact on its behalf

**(d)** Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and

**(e)** Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

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

Explanation: Term 'body of individuals' includes societies.

**25. B** For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:

(a) Document showing name of the person authorised to act on behalf of the entity;

(b) Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and

(c) Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

## Part IV - Identification of Beneficial Owner

**26.** 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 sub-rule (3) of Rule 9 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

**27.** The Bank will 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.

**28.** 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. Threshold will as per IBA parameters for suspicious transactions.

(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.

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

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

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

**30. Periodic Updation**

The Bank shall adopt a risk-based approach for periodic updation of KYC. However, 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. Policy in this regard is documented as part of this KYC policy duly approved by the Board of Directors.

**(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 with the RE, customer's mobile number registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of RE), 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 will be obtained from the customer through customer's email-id registered with the bank, customer's mobile number

registered with the bank, and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, the bank will obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation.

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 it shall be ensured that CDD documents as per the current CDD standards are available with the bank. Wherever required, the bank will carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

**(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, letter from an official authorized by the LE in this regard, board resolution etc. Further, bank will 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, the Bank will undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

(c) **Additional measures:** In addition to the above, the Bank will 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 with the bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the bank has expired at the time of periodic updation of KYC, the bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

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

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

iv. In order to ensure customer convenience, the facility of periodic updation of KYC at any branch is extended, in terms of their internal KYC policy duly approved by the Board of Directors.

v. The Bank will adopt a risk-based approach with respect to periodic updation of KYC. No exception shall be allowed in the above rekyc guidelines.

vi. The Bank will ensure that their internal KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

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

Provided that before temporarily ceasing operations for an account, the bank will give the customers an accessible notice and a reasonable opportunity to be heard. The customercan have the relaxation to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes Such accounts shall, however, be subject to enhanced monitoring

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

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

## Part VI - Enhanced and Simplified Due Diligence Procedure

### A. Enhanced Due Diligence

**32. Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):** the bank shall ensure that the first payment is to be effected through the customer's KYC-complied account with another bank, for enhanced due diligence of non-face-to-face customers.

**33. Accounts of Politically Exposed Persons (PEPs)**

A. the Bank shall have the option of establishing a relationship with PEPs provided that:

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

(b) the identity of the person shall have been verified before accepting the PEP as acustomer;

(c) the decision to open an account for a PEP is taken by the Regional Manager inaccordance with the Customer Acceptance Policy;

(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, Regional Manager's approval is obtained to continue the business relationship;

(f) the CDD measures as applicable to PEPs including enhanced monitoring on an on- going basis are applicable.

B. These instructions shall also be applicable to accounts where a PEP is the beneficial owner

**B. Simplified Due Diligence**

**34. Simplified norms for Self Help Groups (SHGs)**

(a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.

(b) CDD of all the office bearers shall suffice.

(c) Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

## CHAPTER - VII
## Record Management

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

(a) maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction;

(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.

## CHAPTER - VIII

## Reporting Requirements to Financial Intelligence Unit – India

**36.** The Bank will 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.

**37.** The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of.

**38.** While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Bank will not put any restriction on operations in the accounts where an STR has been filed. The Bank will 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.

**39.** 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 –

**40.** The Bank will ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, 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", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl {Every update in this list is circulated by the Bank}

(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 https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl. {Every update in this list is circulated by the Bank}

**41.** Details of accounts resembling any of the individuals/entities in the lists will be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated 55February 2, 2021 (Annex II of RBI master directions) as per prevalent instructions.

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.

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

The procedure laid down in the UAPA Order dated 56February 2, 2021 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

**43. 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

**44. Secrecy Obligations and Sharing of Information:**

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

(b) 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.

(c) 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.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. the interest of bank requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

**45. 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 PML Rules, the Bank 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 which has been issued as circular in our Bank.

(d) The Bank Will 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) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Scheduled Commercial Banks (SCBs) are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. SCBs were initially allowed time up-to February 1, 2017, for uploading data in respect of accounts opened during January 2017.

REs other than SCBs were required to 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) REs shall upload 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, the Bank shall ensure that the 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, the Bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (e) and (f) respectively at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer

(i) The Bank will ensure that during periodic updation, the customers are migrated to the current CDD standard.

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

i. there is a change in the information of the customer as existing in the records of CKYCR;
ii. the current address of the customer is required to be verified;
iii. the bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client

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

Under FATCA and CRS, the bank shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as definedin 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: the 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 procedure and for recording and maintaining the same, as provided in Rule 114H.

(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. The Bank has to take note of the following:
   i. updated Guidance Note on FATCA and CRS
   ii. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

**47. 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.

**48. 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, it shall be deemed that the bank has not complied with these directions.

**49. Collection of Account Payee Cheques**

Account payee cheques for any person other than the payee constituent shall not be collected. Banks shall, at their 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.

**50.**

(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 and NBFCs.
(b) The banks/NBFCs shall, at their 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.

**51. Introduction of New Technologies /Debit Cards / Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc**

Adequate attention shall be paid by the 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.

**52. Wire transfer**

The Bank shall ensure the following while effecting wire transfer:

(a) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.
(b) Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.
(c) Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

**53. Issue and Payment of Demand Drafts, etc.,**

Any remittance of funds by way of demand draft, mail/ /NEFT/IMPS or any other mode value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.
Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

**54. Quoting of PAN**

Permanent account number (PAN) or equivalent e-document thereof of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax

Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

**55. Selling Third party products**

The bank 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 as required under Section 13(e) of this Directions.

(b) transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

(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.

**56. Hiring of Employees and Employee training**

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

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues shall be ensured.

## Annex I

## Digital KYC Process

A. The Bank shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of The Bank

B. The access of the Application shall be controlled by the Bank and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by the Bank to its authorized officials.

C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Bank or vice-versa. The original OVD shall be in possession of the customer.

D. The Bank must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Bank shall put a water-mark in

readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by The Bank) and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the customer.

E. The Application of the Bank shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the bank shall not be used for customer signature. The Bank must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Bank. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the bank, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the bank shall check and verify that: - (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized officer of the bank who will take a print of CAF, get signatures/thumb-impression of customer at

appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

**Annex II**
**File No. 14014/01/2019/CFT**
**Government of India**
**Ministry of Home Affairs**
**CTCR Division**

North Block, New Delhi.

Dated: the 2nd February, 2021

**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.

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

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

3.5 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.

3.6 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.

ii. The CBIC shall advise the dealers of precious metals/stones (DPMS) that if any designated individual/entity approaches them for sale/purchase of precious metals/stones or attempts to undertake such transactions the dealer should not

carry out such transaction and without delay inform the CBIC, who in turn follow the similar procedure as laid down in the paragraphs 6.2 to 6.5 above.

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

iv. The UAPA Nodal Officer of the State/UT shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino and/ or if any assets of such designated individual/ entity is with the Casino operator, and of the particulars of any client matches with the particulars of designated individuals/ entities, the Casino owner shall inform the UAPA Nodal Officer of the State/UT without delay, who shall in turn follow the procedure laid down in paragraph 6.2 to 6.5 above.

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

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

vii. In addition, the member of the ICSI be sensitized that if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person then the member should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate

Affairs who shall in turn follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

viii. The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraph 8 to 10 above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms. Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraph 6.2 to 6.5 above.

**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.

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

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

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

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

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

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

**(Ashutosh Agnihotri)**
**Joint Secretary to the Government of India**

To,

1) Governor, Reserve Bank of India, Mumbai
2) Chairman, Securities & Exchange Board of India, Mumbai
3) Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4) Foreign Secretary, Ministry of External Affairs, New Delhi.
5) Finance Secretary, Ministry of Finance, New Delhi.
6) Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7) Secretary, Ministry of Corporate Affairs, New Delhi
8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9) Director, Intelligence Bureau, New Delhi.
10) Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
11) Chief Secretaries of all States/Union Territories
12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13) Directors General of Police of all States & Union Territories
14) Director General of Police, National Investigation Agency, New Delhi.
15) Commissioner of Police, Delhi.
16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.

17) Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.
18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
19) Director (FIU-IND), New Delhi.

Copy for information to: -

1. Sr. PPS to HS
2. PS to SS (IS)

## Annex III
## Indicative Risk Categorization of Customers

| Particulars | High Risk | Medium Risk | Low Risk |
|---|---|---|---|
| Type of Customer | (i) Private Ltd. Com.<br>(ii) Public Ltd Company (Closely held)<br>(iii) Trusts<br>(iv) Charities<br>(vi) Politically Exposed Persons<br>(vii) Non-Face to face customers with aggregate deposit of Rs.10 lakhs and above.<br>(viii) Customers having adverse publicity.<br>(ix) Firms with operative transactions authorized by sleeping partner. | (i) Public Ltd companies (widely held)<br>(ii) Firms with sleeping partners. | (i) Salaried persons.<br>(ii) Pensioners<br>(iii) Professional & Self employed persons.<br>(iv) Agriculturist<br>(v) Self Help Groups<br>(vi) Government companies.<br>(vii) Public Sector companies.<br>(viii) Government Departments |
| Quantum of Transaction | Cash transaction of Rs. 5 lac and above Non cash transactions of Rs.10 lacs and above One time transaction Rs. 1 lac and above (cash.) Rs.5 lac and above (non cash) | Cash transaction of Rs. 1 lac & above but less than 5 lacs. Non cash transactions of Rs.2 lacs & above but below Rs.10 lac One time transaction Rs. 20,000 and above but below 1 lac cash Rs.1 lac and above but less than Rs.5 lacs non cash | Cash transactions less than Rs. 1 lac Non cash transactions Less than Rs.2.00 lacs One time transaction Less than Rs.20,000/- Cash Less than Rs.1 lacs non cash |
| Business Activity | (1) Jewellery<br>(2) Chit Funds<br>(3) Finance Companies<br>(4) Foreign Exchange, Money Market Brokers<br>(5) Travel Agencies<br>(6) Export / Import Trade<br>(7) S M Es with annual turnover exceeding Rs. 25 Cr. and above | (i) Commodity Trade<br>(ii) S M Es with annual turnover Rs. 10 Crores and above, but3 < Rs.25 Crores | (i) Industry<br>(ii) Hotel<br>(iii) Plantations<br>(iv) S M Es with turnover less than Rs. 10 Crores.<br>(v) Retail Trade |
| Composition of partners, directors | Entirely Foreign nationality | A mix of Indian and Foreign nationals | Exclusively Indian Nationals |