POLICY GUIDELINES ON KNOW YOUR CUSTOMER'(KYC) NORMS AND ANTI-MONEY LAUNDERING (AML) MEASURES

Created By:	Risk
Reviewed and Approved by:	Board of Directors
Last Updated on:	February 10, 2026
Last Reviewed on:	February 10, 2026
Version:	1.4

List of Contents

Introduction:

RBI has issued Direction – Know Your Customers (KYC) Direction, on November 28, 2025, **RBI/DOR/2025-26/361, DOR.AML.REC.No.280/14.01.003/2025-26**. These directions are applicable to all kinds of NBFCs. Authum Investment & Infrastructure Limited ("Authum") being a registered NBFC, must therefore comply with these directions.

Authum shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this code to conform to the standards so prescribed. This policy is applicable across all branches / business segments of Authum, and its financial subsidiaries and is to be read in conjunction with related operational guidelines issued from time to time. The contents of the policy shall always be read in tandem/auto-corrected with the changes/modifications which shall be advised by RBI from time to time.

Authum endeavors to frame a proper policy framework on Know Your Customer (KYC) and Anti Money Laundering measures. Authum is committed to transparency and fairness in dealing with all stakeholders and in ensuring adherence to all laws and regulations.

Authum will ensure that the information collected from the customer for any purpose would be kept as confidential and not divulge any details thereof. Authum commits that information sought from the customer is relevant to the perceived risk, is not intrusive, and is inconformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with his/her consent and after effective rendering of services.

Authum shall also communicate its KYC norms to its customers. Authum shall ensure that the implementation of the KYC norms is the responsibility of the entire organization.

Authum's Board of Directors and the management team are responsible for implementing the KYC norms hereinafter detailed, and also to ensure that its operations reflect its initiatives to prevent money laundering activities.

For the purpose of KYC policy, a "Customer" shall be defined as:

A person who is engaged in a financial transaction or activity with Authum and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

Chapter I – KYC Objective of the Policy and Definition of terms.

Objective:

The objective of KYC guidelines is to prevent Authum from being used as a channel for Money Laundering (ML) / Terrorist Financing (TF) and to ensure the integrity and stability of its financial systems. The KYC procedure would also enable Authum to know/understand its customers and their financial dealings in a better manner, which in turn will help Authum manage its risks prudently.

Definitions

The terms and references used in this Policy shall bear the meanings assigned to them in Annexure III.

Chapter II – KYC Policy

Authum's KYC policy would incorporate the following four key elements:
(i) Customer Acceptance Policy;
(ii) Risk management;
(iii) Customer Identification Procedures;
(iv) Monitoring of Transactions

1. **Customer Acceptance Policy ("CAP")**
   Authum shall frame a Customer Acceptance Policy.

2. The guidelines for Customer Acceptance Policy (CAP) for the Company are given below:

a. No account is opened in anonymous or fictitious / benami name.
b. No account is opened where Authum is unable to apply appropriate CDD (Customer Due Diligence) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. Authum should consider filing a STR (Suspicious Transaction Report) if necessary, when it is unable to comply with CDD measures pertaining to the customer
c. No transaction or account based relationship is undertaken without following the CDD procedure.
d. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
e. 'Optional"/additional information is obtained with the explicit consent of the customer after the account is opened.
f. CDD Procedure is followed for all the joint account holders, while opening a joint account.
g. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
h. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by the RBI
i. It shall be ensured that customer acceptance policy and procedure shall not result in denial in financial facility to members of general public especially those who are financially or socially disadvantaged.

j. If Authum suspects any instance(s) of money laundering / terror funding, and has reason to believe that CDD could tip-off the borrower, Authum will not pursue CDD but proceed to file STR with FIU IND – Financial Intelligence Unit of India.

Authum's IT systems are currently under migration and post completion the loan records would be in a new-age Loan Management System (LMS) and new age Loan Origination System (LOS). Post this completion of the migration into a new age LOS, the system will have the capability to accommodate the following, and which will become part of this Policy document on KYC

a. Authum shall apply the CDD procedure at the UCIC (Unique Customer Identification Code) level. Thus, if an existing KYC Compliant customer of Authum desires to open another account with Authum, there shall be no need for a fresh CDD exercise
b. Authum will be able to verify the PAN of the borrower from the verification facility of the issuing authority
c. Authum will be able to verify the GST Registration Number of the borrower from the verification facility of the issuing authority
d. Perform check at system level itself to identify if customer data matches with any person/entity, whose name appears in the sanctions lists circulated by the RBI

Chapter IV – Risk Management

3. Risk Management

Authum shall have risk-based approach while complying with Know Your Customer Policy and Procedures, which includes the following:
a. Authum shall classify customers into "low" / "medium" / "high" risk categories based on risk perception and decide on acceptance criteria for each customer category.
b. Accept customers after verifying their identity as laid down in customer identification procedures.
c. For the purpose of risk categorization of customer, Authum shall obtain the relevant information from the customer at the time of account opening.
d. Risk categorization will be undertaken based on various parameters such as customer identity, social / financial status, nature of business activity, location of customer, profile of his clients, information about clients" business, mode of payments, volume of turnover, etc. While considering customers identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
e. Information called for different categories of the customers relating to the perceived risk should be non-intrusive.
f. The FATF public statement, the reports and guidance notes on AML / KYC issued by Indian Banks Association (IBA) and other agencies in risk assessments.
g. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering (PML) Act, 2002 and guidelines issued by Reserve Bank from time to time.
h. Authum shall keep the risk categorization of its customers confidential and shall not reveal this information to the customers, this would avoid any act of tipping-off.

For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. Illustrative examples of low-risk customers would be salaried employees whose salary structures are well defined, people belonging to the lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to Authum may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Authum may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive due diligence" for higher risk customers, especially those for whom the sources of funds are not clear.

Examples of customers requiring higher due diligence may include
(i) non-resident customers,
(ii) high net-worth individuals,
(iii) trusts, charities, NGOs and organizations receiving donations,
(iv) companies having close family shareholding or beneficial ownership,
(v) firms with' sleeping partners',
(vi) politically exposed persons (PEPs) of foreign origin,
(vii) non-face to face customers, and
(viii) those with dubious reputation as per public information available, etc.

Chapter V - Customer Identification Procedure (CIP)

4. Authum shall undertake identification of customers in the following cases:
a. Commencement of an account-based relationship with the customer.
b. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c. When Authum has reason to believe that a customer (account-based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rupees fifty thousand.
d. Authum shall ensure that it does not seek introductions while opening accounts.

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

(a) Necessary Record/ information of such customers due diligence carried out is obtained immediately from the third party or from the Central KYC Records Registry.
(b) Adequate steps are taken by Authum to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
(d) The third party shall not be based in a country or jurisdiction assessed as high risk.
(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with Authum.

Chapter VI - Customer Due Diligence (CDD)Procedure*

Part I-CDD Procedure in case of Individuals

5. Authum shall obtain the following information 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 for undertaking CDD:

a) From an individual who is eligible for enrolment of Aadhaar, the Aadhaar number
b) The proof of possession of Aadhaar number where Authum can carry out offline verification
c) The proof of possession of Aadhaar number where Authum cannot carry out offline verification or any OVD (Officially valid document) or the equivalent e-document thereof containing the details of their identity and address
d) The KYC identifier with explicit consent to download records from CKYCR
e) The Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time
f) Any other document including in the nature of business and financial status of the customer.

In case the customer provides his/her Aadhaar
(i) the same shall be authenticated by looking up the number on the UIDAI's e-kyc portal. In case the address on the Aadhar is different from the current address provided by the customer, Authum will procure a self-declaration from the customer.
(ii) Authum will carry out off-line verification
(iii) In case offline verification cannot be carried out, Authum shall carry out digital verification – more about the steps for digital verification are mentioned hereinbelow

In case the customer provides any other OVD, Authum shall verify the digital signature as per provisions of the Information Technology Act and also take a live photo

In respect of the KYC identifier consent obtained, Authum shall retrieve the online KYC records from the online CKYCR

6. Digital KYC Process

As stated earlier, Authum's systems are being migrated to latest, high-end versions, post migrations, the Digital KYC steps mentioned hereinbelow will become part of Authum's KYC policy:

1) Authum shall develop an application for digital KYC process and make it available at customer touch points for undertaking KYC of its customers and shall undertake the KYC process only through this authenticated application
2) Authum shall control the access to this application and ensure that only authorized persons use this application, and access is controlled by issuing login ids and passwords, further the password will also be in conformity with Authum's IT policy on live OTP.
3) The customer shall visit the location of the authorized official at Authum or vice versa. The original OVD will be in possession of the customer
4) Authum shall ensure that its officer takes a live photo of the customer and embeds the same on the Customer Application Form. The application must be capable of and shall put a watermark in readable form, containing CAF number, GPS coordinates, official's name, employee code, and date and time stamp on the live photo of the customer.
5) The application must be such that only live photos are captured and no other photograph is permitted to be embedded therein. The background will be white in colour and only the customer must be in the photograph.
6) Where offline verification cannot be carried out, the authorized officer shall capture the live

photograph of the OVD or Aadhaar vertically from above and apply a watermark in readable form as mentioned above. The live photos of the original documents must be straight, i.e. the mobile device must not be a position of skew or tilted.

7) The live photos of the customer and his / her original documents must be captured in proper light, so that they are clearly identifiable and readable.
8) After the photos, the authorized officer shall fill the necessary details on the CAF as per the information and documents furnished by the customer. If documents have a Quick Response (QR) code, then information must be auto-populated by scanning the QR code, instead of manual filling-in of details. Example when there is a QR code on the Aadhar, the name, DOB, address, gender may be auto-populated by scanning the QR code
9) Once the photos are done, the authorized officer shall trigger an sms containing an OTP on the registered mobile number of the customer. The message on the sms will read "Please verify details on the form before sharing this OTP". Authum must check that the mobile number on which the OTP is messaged is not the mobile number of its own authorized officer.
10) Post the completion of the customer's Digital KYC process, Authum's authorized officer's live photo and original document shall also be captured in addition an sms will also be triggered to the mobile number of the authorized officer that is registered with Authum. Post successful registration, of the OTP, Authum will treat the signature of its authorized officer on the CAF to be complete
11) Post the above steps, Authum's authorized officer shall pass on the information to the back-office at Authum and request for generating transaction ID / LAN. The authorized officer shall communicate the transaction ID / LAN to the customer for future reference.

12) Authum's authorized officer will check and verify that:
    a) Information in the pictures on the document match with the information on the CAF
    b) Live photo of the customer matches with the photo on the CAF
    c) The CAF has been filled in full and information therein is accurate
13) On successful verification, the CAF will be digitally signed by the authorized officer of Authum, printed and hard copy is signed by the customer and upload the original on Authum's system and return the original form to the customer.

6.a The points related Video-Customer Identification Process (V-CIP) & V-CIP Records and Data Management do not apply to Authum for now since Authum does not have a system to conduct CIP via video mode.

6.b The points related to Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs), CDD Measures for Sole Proprietary firms for opening account with an NBFC & CDD Measures for Legal Entities for opening account with an NBFC does not apply for Authum for now as Authum is a non-deposit taking NBFC.

Part II-CDD Procedure in case of Sole Proprietary firms

7. While signing up with a sole proprietary for a new relationship, Authum will perform the same CDD procedures as in the case of an individual.

7.1. In line with RBI Master Direction – KYC (Dec 2025), where Authum relies on customer KYC records downloaded from CKYCR, and such records are current and compliant, Authum shall not be required to re-verify the identity and/or address of the customer. However, Authum shall remain responsible for all other aspects of Customer Due Diligence (CDD) in accordance with the PML Act and RBI Directions.

8. In addition, Authum will also obtain any 2 of the following, for checking the proof of business activity in the proprietary firm:
    (i) Registration certificate, including UDYAM issued by the government
    (ii) Shop & Establishment certificate / license issued by the municipality
    (iii) Sales & income tax returns
    (iv) GST / VAT / CST certificate
    (v) Utility bills such as electricity, water, landline telephone bill
    (vi) IEC (Importer Exporter Code) issued to the proprietary firm by the office of the DGFT
    (vii) Complete income tax return (not just the acknowledgment) in the name of the proprietor, indicating the income earned from the proprietary firm.

9. In cases where Authum is satisfied that it is not possible to furnish two such documents, it may, at its discretion, accept only one of those documents as proof of business/activity. Provided that Authum undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III – CDD Measures for Legal Entities (LE)

10. For opening an account of a company, certified copy of each of the following documents shall be obtained:
    i. Certificate of incorporation.
    ii. Memorandum and Articles of Association.
    iii. Permanent Account Number of the Company
    iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
    v. Documents/Identification information as mentioned in Part I (CDD Measures for individuals) in respect of beneficial owner(s), managers, officers or employees holding an attorney to transact on its behalf.
    vi. The names of the relevant persons holding senior management position
    vii. The registered office and the principal place of business, if it is different.

11. For opening an account of a partnership firm, the certified copy of each of the following documents shall be obtained:
    i. Registration certificate.
    ii. Partnership deed.
    iii. Permanent Account Number of the partnership firm
    iv. Documents/Identification information as mentioned in Part I (CDD Measures for individuals) in respect of beneficial owner(s), managers, officers or employees holding an attorney to transact on its behalf.
    v. The names and addresses of all the partners and
    vi. Address of the registered office, and the principal place of its business, if it is different

12. For opening an account of a trust, certified copy of each of the following documents shall be obtained:
    i. Registration certificate.
    ii. Trust deed.

iii. Permanent Account Number or Form 60 of the Trust
iv. The names of the beneficiaries, trustees, settlor, protector, if any, and authors of the trust
v. Documents/Identification information as mentioned in Part I (CDD Measures for individuals) in respect of trustees, beneficial owner(s), managers, officers or employees holding an attorney to transact on its behalf.
vi. The address of the registered office of the trust

13. For opening an account of an unincorporated association or a body of individuals, certified copy of each of the following documents shall be obtained:

i. Resolution of the managing body of such association or body of individuals;
ii. Permanent Account Number or Form 60 of the unincorporated association or body of individuals
iii. Power of attorney granted to transact on its behalf;
iv. Documents/Identification information as mentioned in Part I (CDD Measures for individuals) in respect of beneficial owner(s), managers, officers or employees holding an attorney to transact on its behalf.
v. Such information as maybe required by Authum 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

14. For opening accounts of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats, certified copy of the following documents shall be obtained.
    i. Document showing name of the person authorized to act on behalf of the entity;
    ii. Documents/Identification information as mentioned in Part I (CDD Measures for individuals) in respect of the person(s) holding an attorney to transact on its behalf.
    iii. Such documents as may be required by Authum to establish the legal existence of such an entity/juridical person.

Part IV-Identification of Beneficial Owner

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

1. Where the customer or the owner of the controlling interest is a company
   (i) listed on a stock exchange, or
   (ii) it is an entity resident in jurisdictions notified by the Central government and listed on stock exchanges in such jurisdictions or
   (iii) 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.

2. 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

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

17. Without prejudice to the generality of factors that call for close monitoring, Authum shall necessarily monitor the following types of transactions:
    - (i) 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.
    - (ii) Transactions which exceed the thresholds prescribed for specific categories of accounts.
    - (iii) High account turnover inconsistent with the size of the balance maintained.
    - (iv) Deposit of 3rd party cheques in the account(s)

For ongoing due diligence, Authum may consider adopting appropriate innovations including AI and Machine learning tools to support effective monitoring.

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

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

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

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

19. Updating / Periodic Updating of KYC

Authum will adopt a risk-based approach for updating KYC and ensure that the KYC collected under the CDD procedure is kept upto date and relevant particularly for high risk customers. Periodic updating 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 subject to the following procedure:

Notwithstanding the above provision, in respect of an individual, who has been categorized as “low risk”, Authum shall allow all transactions and ensure the updation of KYC within 1 year of its falling due or upto June 30, 2026, whichever is later. Authum shall monitor such accounts at regular intervals. This will also apply to low risk individuals for whom periodic updation of KYC has already fallen due.

<u>Individuals:</u>

1. No change in KYC information: In case of no change in the KYC information, Authum shall obtain a self-declaration from the customer in this regard through the customer’s email-id registered with Authum, customer’s mobile number registered with Authum, digital channels (including mobile application of NBFC) letter, etc.
2. Change in address: In case of a change only in the address details of the customer, Authum shall obtain a self-declaration of the new address from the customer through customer’s email-id registered with Authum, customer’s mobile number registered with Authum, digital channels (including mobile application of Authum), letter, etc.,

and shall verify the declared address through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

3. Further, Authum at its option, may obtain a copy of OVD (passport, driving license, Voter ID, Proof of possession of Aadhar, NREGA card issued by the State Government) or deemed OVD, or equivalent e-document (documents issued to the digilocker account of the customer) for the purpose of proof of address, declared by the customer at the time of updation / periodic updation.
   Change in address:

4. Further, the NBFC at its option, may obtain a copy of OVD or deemed OVD, as defined in sub-clause (xiv) of clause (1) of paragraph 5 or the equivalent e-documents thereof, as defined in sub-clause (x) of clause (1) of paragraph 5 for the purpose of proof of address, declared by the customer at the time of updation / periodic updation.

5. Accounts of customers, who were minor at the time of opening account, on their becoming major: In case of customers for whom Authum opened an account when they were minors, Authum shall obtain fresh photographs upon their becoming a major and, at that time, shall ensure that CDD documents as per the current CDD standards are available. Wherever required, Authum may carry out fresh KYC of such customers, i.e., customers for whom it opened account when they were minor, upon their becoming a major.

6. Authum may use Aadhaar OTP based e-KYC in non-face-to-face mode for updation / periodic updation.

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

19.A Re-KYC:

As per the directions of the regulator to conduct periodic re-kyc of its customers Authum has adopted a step-by-step approach to ensure fullest compliance.

a: Risk categorization of the customer shall be conducted in accordance with the Authum's board approved credit policy which entails the criteria and parameters for risk classification of customers.

b: As per Authum's board approved credit policy and in line with regulatory requirements below shall be the periodicity for conducting Re-KYC post risk classification:

Customer Classification Type	Low Risk	Medium Risk	High Risk*
Re-KYC Periodicity	Once every 10 years	Once every 8 years	Once every 2 years

*As per the RBI circular dated June 12th 2025 below exercise shall be conducted as an exception:

"*In respect of an individual customer who is categorized as low risk, the RE shall allow all* *transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. The RE shall subject accounts of such customers to regular monitoring. This shall also be applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.*"

<u>Customers other than Individuals:</u>

1. No change in KYC information: In case there is no change in the KYC information of a legal entity (LE), Authum shall obtain a self-declaration in this regard from the customer through its email id registered with Authum, digital channels (including mobile application of Authum), letter from an official authorised by the LE in this regard, board resolution, etc. Further, Authum shall ensure during this process that Beneficial Ownership (BO) information available with it is accurate and shall update the same, if required, to keep it as up-to-date as possible.

2. Change in KYC information: In case of change in KYC information, Authum shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer

In addition to the above, Authum shall ensure that:

i. Authum has customer's KYC document as per the current CDD standards available with it. This is applicable even if there is no change in customer information but the documents available with Authum are not as per the current CDD standards. Further, in case the validity of the CDD documents available with Authum has expired at the time of periodic updation of KYC, Authum shall undertake the KYC process equivalent to that applicable for onboarding a new customer.
ii. Authum verifies the Customer's PAN details, if available, from the database of the issuing authority at the time of periodic updation of KYC
iii. Authum provides an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation. Further, Authum shall ensure that it promptly updates the information / documents obtained from the customers at the time of updation / periodic updation of KYC in its records / database and provide an intimation, mentioning the date of updation of KYC details, to the customer.
iv. In order to ensure customer convenience, Authum may consider making available the facility of updation / periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Authum or any committee of the Board to which power has been delegated.
v. Authum shall adopt a risk-based approach with respect to periodic updation of KYC. Authum shall clearly specify in its internal policy, duly approved by the Board of Directors of Authum or any committee of the Board to which power has been delegated, any additional and exceptional measures, it adopts that are not otherwise mandated under the above instructions, such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of Authum where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc

Authum shall advise its customers, that in order to comply with PML rules, they would need to update their KYC in case of any changes in their KYC. The customers should share new KYC documents, so that the same are updated within 30 days of change.

Prior to the date of updation of KYC, Authum shall give at least 3 advance intimations including at least one intimation by letter for complying with the requirement of periodic updation of KYC. Subsequent to the due date, Authum shall give at least 3 reminders including at least reminder by letter, to such customers who have still not complied with the requirements, despite advance intimations. Issue of intimations shall be recorded for audits.

i. PAN verification from the verification facility available with the issuing authority and
ii. Authentication of Aadhaar Number already available with Authum with the explicit consent of the customer in applicable cases.
iii. In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.
iv. Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorised as "low risk". In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.
v. In case of Legal entities, Authum shall review the documents sought at the time of opening of account and obtain fresh certified copies.

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

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

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

Part VI- Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

20. **Accounts of non-face-to-face customers:** Authum shall ensure that

(a) If Authum were to establish a Video Customer Identification Process (V-CIP), then this should be the first option that should be offered to the customer for remote onboarding.
(b) the first payment is to be effected through the customer's KYC-complied account with another RE, for enhanced due diligence of non-face to face customers
(c) PAN is obtained from the customer and the PAN is verified from the verification facility of the issuing authority
(d) Not only is the current address obtained, it must also be verified through positive confirmation before allowing operations. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables etc
(e) In order to prevent frauds, alternate mobile numbers will not be linked post CDD with such accounts for OTPs for transaction updates. There should be a board approved policy for changing registered mobile numbers.

(f) Such customers are categorized as “high risk” and their accounts shall be subjected to enhanced monitoring until the identity of the customer is verified in face to face manner or through V-CIP

21. Accounts of Politically Exposed Persons (PEPs)

Authum shall have the option of establishing a relationship with PEPs provided that apart from performing normal customer due diligence:

i. Authum must ensure that it has appropriate systems in place to determine whether the customer or the beneficial owner is a PEP
ii. Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
iii. The decision to open an account for a PEP is taken at a senior level in accordance with the Company‟ Customer Acceptance Policy;
iv. All such accounts are subjected to enhanced monitoring on a non-going basis;
v. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management’s approval is obtained to continue the business relationship; and

The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable to family members or close associates of PEP

22. Client accounts opened by professional intermediaries:

Authum shall ensure while opening client accounts through professional intermediaries, that:

a) Authum identifies the clients when an account is opened by a professional intermediary on behalf of a single client.
b) Authum shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
c) Authum shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to Authum.
d) All beneficial owners are identified where funds held by the intermediaries are not co-mingled at the level of Authum, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Authum, then Authum shall look for the beneficial owners
e) Authum shall, at its discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

The ultimate responsibility for knowing the customer lies with Authum.

23. Record Management

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

(a) maintain all necessary records of transactions between Authum 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

(g) manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities; and

(h) 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.

24. Authum shall ensure that in case the customer is a not for profit organization, the details of such customers are registered on the DARPAN portal of the NITI Ayog. These records will also be maintained for a period of 5 years from the date of closure of account.

Reporting Requirements to Financial Intelligence Unit–India

25. Authum shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

26. 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. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Authum for extracting CTR/STR from their live transaction data.

27. 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 misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Authum shall not put any restriction on operations in the accounts where an STR has been filed.

28. Authum, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005, and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information of any analysis of transactions and activities which appear unusual, if Authum has done any such analysis

29. 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.

For determining integrally connected cash transactions, Authum shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month.

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND immediately. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

"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 are as on able 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 on 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.

Requirements/obligations under International Agreements Communications from International Agencies –

30. **Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:**

1. Authum shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

(b) The 'Taliban Sanctions List' established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://www.un.org/securitycouncil/sanctions/1988/materials

- Authum shall share a report of updated lists to stakeholders to have a de-dupe check of existing as well as new cases prior to going ahead with the transaction.

2. Authum shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any

modifications to the lists in terms of additions, deletions or other changes shall be taken into account by Authum for meticulous compliance.

3. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

4. Freezing of Assets under section 51A of UAPA, 1967: Authum shall strictly follow the procedure laid down in the UAPA Order dated February 2, 2021 (Annexure – I of this Policy which is based on RBI's Directions), and shall ensure the meticulous compliance with the Order issued by the Government.

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

(a) Authum shall ensure meticulous compliance with "Procedure for Implementation of Section 12A of the WMD Act, 2005" and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005' laid down in terms of section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (Annex – II of this Policy Document, which is based on RBI's Directions)
(b) Authum shall ensure not to carry out transactions in case the particulars of the individual/entity match with the particulars in the designated list.
(c) Further, Authum shall run a check, on the given parameters, at the time establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any financial asset.
(d) In case of matches in the above cases, Authum shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI.
(e) It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.
(f) Authum should refer to the designated list, as amended from time to time, available on the portal of FIU-India.
(g) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of section 12A of the WMD Act, 2005, Authum shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email and by post, without delay.
(h) In case an order to freeze assets under section 12A is received by Authum from the CNO, Authum shall, without delay, take necessary action to comply with the Order.
(i) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by Authum along with full details of the asset frozen, as given by the applicant, to the CNO by email and by post, within two working days.

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

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

34. Authum shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

35. 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. Authum shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF
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.
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.

36. Authum shall deploy latest technology and tools for effective implementation of name screening to meet the sanctions requirements

Other Instructions

37. Secrecy Obligations and Sharing of Information

(a) Authum 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 an 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, Authum shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the 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 Authum requires disclosure; and
   iv. Where the disclosure is made with the express or implied consent of the customer.

38. **Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010**: The NBFC shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010, and Rules made thereunder. Further, the NBFC shall also

ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the RBI based on advice received from the Ministry of Home Affairs, Government of India.

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

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.

1. In terms of provision of Rule 9(1A) of the PML Rules, Authum shall capture the KYC information and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
2. Operational Guidelines for uploading the KYC data have been released by CERSAI
3. Authum shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI
4. The "live run" of the CKYCR would start with effect from July 15, 2016 in phased manner beginning with new "individual accounts".

Authum is currently transitioning from an old application to a modern application that can handle CKYC related compliance, once the migration has been completed, Authum shall take the following steps: ensure that the same is communicated to the individual/LE as the case may be

5. it shall take steps to prepare their systems for uploading the KYC data in respect of new individual as well as Legal entity accounts so that the same is complete as soon as possible in a time-bound manner. Authum shall prepare a plan for uploading the data in respect of existing individual accounts and include the same in their KYC Policy.
6. ensure that the CKYC identifier is communicated to the individual/LE as the case may be
7. in order to ensure that all KYC records are incrementally uploaded on to CKYCR, Authum shall upload the KYC pertaining to accounts of individual customers and LEs opened prior to dated mentioned in (4) and (5) above at the time of periodic updates. Also, whenever Authum obtains additional or updated information from any customer it shall within 7 days submit this information to CERSAI for updating the CKYCR. Post receipt of the updated information the CKYCR will get updated and the CERSAI will inform all REs who have dealt with this customer about the updated in his/their KYC. Once an update is received from the CKYCR, Authum shall retrieve the updated KYC records from CKYCR and update the KYC maintained by Authum.
8. Authum will ensure that during periodic update, the customers are migrated to the current CDD Standard
9. For the purpose of establishing an account-based relationship, updation / periodic updation or verification of identity of a customer, Authum shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available from the CKYCR and proceed to obtain KYC records online by using KYC Identifier and shall not require the customer to submit the same KYC records or information or any other additional identification documents or details, unless

(i) There is a change in the information of the customer as existing in the records of the CKYCR; OR
(ii) The KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; OR
(iii) The validity period of downloaded documents has lapsed; OR
(iv) Authum considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer

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

Under FATCA and CRS, Authum shall adhere to the provisions of Income Tax rules 114F, 114G, and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements.

(a) Register on the related e-filing 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 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
(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. Authum may take note of the following:
   i. updated Guidance Note on FATCA and CRS
   ii. a press release on ‘Closure of Financial Accounts’ under Rule 114H (8).

41. **Operation of accounts and 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 accounts by recruiting third parties which act as “money mules.” Authum shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if it is established that an account opened and operated is that of a Money Mule, but no STR was filed Authum, it shall then be deemed that Authum has not complied with these directions.

42. Unique Customer Identification Code (UCIC)

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

(b) This UCIC will be used to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable Authum to have a better approach to risk profiling of customers.

43. Introduction of New Technologies

Authum shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, Authum shall ensure:

a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

44. Wire Transfers – where Authum is the beneficiary

Authum shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers that lack required originator information

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

Full records of such wire transfers will be maintained by Authum for 5 at least years post completion of the transaction or end of relationship whichever is later.

45. Quoting of Permanent Account Number ("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.

46. Selling Third Party Products

If Authum chooses to act as an agent while selling third party products as per regulations in force from time to time, it shall comply with the following aspects for the purpose of these directions:

1. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand.
2. transaction details of sale of third-party products and related records shall be maintained.
3. AML software capable of capturing, generating and analyzing 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.

4. transactions involving rupees fifty thousand and above shall be undertaken only by:
   (i) against cheques; and
   (ii) obtaining and verifying the PAN given by the account-based as well as walk-in customers.
5. Instruction at ‘4’ above shall also apply to sale of Authum’ own products.

47. 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) Authum shall endeavor to ensure that the staff dealing with / being deployed for KYC / AML / CFT standards, effective communication skills & ability to keep up the changing KYC / AML / CFT landscape nationally & internationally. Authum shall strive to develop an environment which fosters open communication & high integrity amongst the staff.

On-going employee training program 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 Authum, regulation and related issues shall be ensured.

Annexure-I

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

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

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

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

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

c) prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

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

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

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

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

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

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

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

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

3.5 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) and any other person:**

(i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned

Regulators without delay.

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

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

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

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

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

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

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

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

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

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

8.1 The U.N. Security Council Resolution No.1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

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

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

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

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

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

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

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

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

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

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

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

10.3 (a): The designated individual or organization may submit a request to the Central [Designated] Nodal Officer for UAPA under the provisions of Para 10.1 above. The Central [Designated] Nodal Officer for UAPA may be approached by post at "Joint Secretary (CTCR), North Block, New Delhi – 110001" or through email to jsctcrmha@gov.in"

(b): The Central [Designated] Nodal Officer for UAPA shall examine such requests, in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence

Agencies and, if accepted, communicate the same, if applicable, to the Ministry of External Affairs, Government of India for notifying the committee established pursuant to UNSC Resolution 1267 (1999) of the intention to authorize, access to such funds, assets or resources in terms of Para 10.1 above.

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

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

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

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

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

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

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

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

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

13. **Procedure for communication of compliance of action taken under Section 51A:** The Central [designated] Nodal Officer for the UAPA and the Nodal

Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

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

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

Annexure - II

Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005"

Section 12A of The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [hereinafter referred to as 'the Act'] reads as under: -

"*12A. (1) No person shall finance any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.*

(2) For prevention of financing by any person of any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

a) freeze, seize or attach funds or other financial assets or economic resources—

i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or

ii. held by or on behalf of, or at the direction of, such person; or

iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

II In order to ensure expeditious and effective implementation of the provisions of Section 12A of the Act, the procedure is outlined below.

1. Appointment and communication details of Section 12A Nodal Officers:

1.1 In exercise of the powers conferred under Section 7(1) of the Act, the Central Government assigns Director, FIU-India, Department of Revenue, Ministry of Finance, as the authority to exercise powers under Section 12A of the Act. The Director, FIU-India shall be hereby referred to as the Central Nodal Officer (CNO) for the purpose of this order. **[Telephone Number: 011-23314458, 011- 23314435, 011- 23314459 (FAX), email address: dir@fiuindia.gov.in].**

1.2 **Regulator** under this order shall have the same meaning as defined in Rule 2(fa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. **Reporting Entity (RE)** shall have the same meaning as defined in Section 2 (1) (wa) of Prevention of Money-Laundering Act, 2002. DNFPBs is as defined in section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.

1.3 The Regulators, Ministry of Corporate Affairs and Foreigners Division of MHA shall notify a Nodal Officer for implementation of provisions of Section 12A of the Act. The Regulator may notify the Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act. All the States and UTs shall notify a State Nodal officer for implementation of Section 12A of the Act. A State/UT may notify the State Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

1.4 The CNO shall maintain an updated list of all Nodal Officers, and share the updated list with all Nodal Officers periodically. The CNO shall forward the updated list of all Nodal Officers to all REs.

2. Communication of the lists of designated individuals/entities:

2.1 The Ministry of External Affairs will electronically communicate, without delay, the changes made in the list of designated individuals and entities (hereinafter referred to as ‘designated list’) in line with section 12A (1) to the CNO and Nodal officers.

2.1.1 Further, the CNO shall maintain the Designated list on the portal of FIU-India. The list would be updated by the CNO, as and when it is updated, as per para 2.1 above, without delay. It shall make available for all Nodal officers, the State Nodal Officers, and to the Registrars performing the work of registration of immovable properties, either directly or through State Nodal Officers, without delay.

2.1.2 The Ministry of External Affairs may also share other information relating to prohibition / prevention of financing of prohibited activity under Section 12A (after its initial assessment of the relevant factors in the case) with the CNO and other organizations concerned, for initiating verification and suitable action.

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The REs will maintain the designated list and update it, without delay, whenever changes are made as per para 2.1 above.

2.2 The Nodal Officer for Section 12A in Foreigners Division of MHA shall forward the updated designated list to the immigration authorities and security agencies, without delay.

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

3.1 All Financial Institutions shall –

i. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of designated list and in case of match, REs shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved *to* the CNO by email, FAX and by post, without delay.

ii. Run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, Insurance policies etc. In case, the particulars of any of their customers match with the particulars of designated list, REs 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 on their books *to* the CNO by email, FAX and by post, without delay.

iii. The REs shall also send a copy of the communication, mentioned in 3.1 (i) and (ii) above, *to* State Nodal Officer, where the account/transaction is held, and to their Regulator, as the case may be, without delay.

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

3.2 On receipt of the particulars, as referred to in Paragraph 3.1 above, the CNO 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 REs are the ones in designated list and the funds, financial assets or economic resources or related services, reported by REs are in respect of the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

3.3 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned RE under intimation to respective Regulators. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

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

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

4.1 The Registrars performing work of registration of immovable properties shall --

i. Verify if the particulars of the entities/individual, party to the transactions, match with the particulars of the designated list, and, in case of match, shall not carry out such transaction and immediately inform the details with full particulars of the assets or economic resources involved *to* the State Nodal Officer, without delay.

ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. 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 Registrar shall immediately inform the details with full particulars of the assets or economic resources involved *to* the State Nodal Officer, without delay.

iii. In case there are reasons to believe beyond doubt that assets that are held by an individual/entity would fall under the purview of clause (a) or (b) of sub- section (2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post , without delay.

4.2 the State Nodal Officer would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources to the CNO without delay by email, FAX and by post.

4.3 The State Nodal Officer may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent 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 CNO without delay by email, FAX and by post.

4.4 The CNO may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

4.5 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Registrar performing the work of registering immovable properties, and to FIU under intimation to the concerned State Nodal Officer. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

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

5. **Regarding the real-estate agents, dealers of precious metals/stones (DPMS), Registrar of Societies/ Firms/ non-profit organizations, The Ministry of Corporate Affairs and Designated Non-Financial Businesses and Professions (DNFBPs):**

(i) The dealers of precious metals/stones (DPMS) as notified under PML (Maintenance of Records) Rules, 2005 and Real Estate Agents, as notified under clause (vi) of Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002, are required to ensure that if any designated individual/entity approaches them for sale/purchase of precious metals/stones/Real Estate Assets or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Nodal officer in the Central Board of Indirect Taxes and Customs (CBIC). Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Nodal officer in the CBIC, who will, in turn, follow procedure similar to as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6.

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensure 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 shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure 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 State Nodal Officer, without delay.

(iii) The State Nodal Officer 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 or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

(iv) 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 12A, 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 Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.

(v) The members of these institutes should also be sensitized by the Institute of Chartered Accountants of India, Institute of Cost and Work Accountants of India and Institute of Company Secretaries of India (ICSI) 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 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 Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(vi) In addition, a member of the ICSI shall, 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, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.

(vii)In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure 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 is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(viii) All communications to Nodal officer as enunciated in subclauses (i) to (vii) above should, inter alia, include the details of funds and assets held and the details of transaction.

(ix) The Other DNBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Central Nodal officer. The communication to the Central Nodal Officer would include the details of funds and assets held and the details of the transaction. Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Central Nodal officer.

(DNFBPs shall have the same meaning as the definition in Section 2(1) (sa) of Prevention of Money-Laundering Act,2002.)

5.1. All Natural and legal persons holding any funds or other assets of designated persons and entities, shall, without delay and without prior notice, freeze any transaction in relation to such funds or assets and shall immediately inform the State Nodal officer along with details of the funds/assets held, who in turn would follow the same procedure as in para 4.2 to 4.6 above for State Nodal Officer. This obligation should extend to all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

5.2 No person shall finance any activity related to the 'designated list' referred to in Para 2.1, except in cases where exemption has been granted as per Para 6 of this Order.

5.3. Further, the State Nodal Officer 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 in the designated list. The State Nodal Officer shall, upon becoming aware of any transactions and attempts by third party, without delay, bring the incidence to the notice of the CNO and the DGP/Commissioner of Police of the State/UT for initiating suitable action.

5.4 Where the CNO has reasons to believe that any funds or assets are violative of Section 12A (1) or Section 12A (2)(b) of the Act, he shall, by order, freeze such funds or Assets, without any delay, and make such order available to authorities, Financial Institutions, DNFBPs and other entities concerned.

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including Fls and DNFBPs obligated to carry out sanctions screening. The concerned Regulators shall take suitable action under their relevant laws, rules or regulations for each violation of sanction screening obligations under section 12A of the WMD Act.

6. **Regarding exemption, to be granted to the above orders**

6.1. The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the CNO 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, consequent to notification by the MEA authorizing access to such funds, assets or resources.

This shall be consequent to notification by the MEA to the UNSC or its Committee, of the intention to authorize access to such funds, assets or resources, and in the absence of a negative decision by the UNSC or its Committee within 5 working days of such notification.

(b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA to the UNSC or its Committee, and has been approved by the UNSC or its Committee;

6.2. The accounts of the designated individuals/ entities may be allowed to be credited with:

(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 section 12A of the Act.

Provided that any such interest, other earnings and payments continue to be subject to those provisions under para 3.3;

6.3 Any freezing action taken related to the designated list under this Order should not prevent a designated individual or entity from making any payment due under a contract entered into prior to the listing of such individual or entity, provided that:
(i) the CNO has determined that the contract is not related to any of the prohibited goods, services, technologies, or activities, under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems;
(ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and
(iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, he unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization

7. **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 individual or entity is not a designated person or no longer meet the criteria for designation:**

7.1 Any individual/entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held has been inadvertently frozen, an application may be moved giving the requisite evidence, in writing, to the relevant RE/Registrar of Immovable Properties/ ROC/Regulators and the State.

7.2 The RE/Registrar of Immovable Properties/ROC/Regulator and the State Nodal Officer shall inform, and forward a copy of the application, together with full details of the asset frozen, as given by applicant to the CNO by email, FAX and by Post, within two working days. Also, listed persons and entities may petition a request for delisting at the Focal Point Mechanism established under UNSC Resolution.

7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it 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 all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

7.4 The CNO shall, based on de-listing of individual and entity under UN Security Council Resolutions, shall pass an order, if not required to be designated in any other order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer.

8. **Procedure for communication of compliance of action taken under Section 12A:** The CNO 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.

9. **Communication of the Order issued under Section 12A:** The Order issued under Section 12A of the Act by the CNO relating to funds, financial assets or economic resources or related services, shall be communicated to all nodal officers in the country.

10. This order is issued in suppression of F.No.P-12011/14/2022-ES Cell-DOR, dated 30th January 2023.

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

Annexure–III Definitions

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

i. "Aadhaar number", as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, henceforth "The Aadhaar Act", means an identification number issued to an individual by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

   Explanation 1: In terms of the Aadhaar Act, every resident shall be eligible to obtain an Aadhaar number.

   Explanation 2: Aadhaar will be the document for identity and address

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", as defined under sub-section (c) of section 2 of the Aadhaar Act, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

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 person, has/have a controlling ownership interest or who exercise control through other means.

      Explanation-For the purpose of this sub-clause-

      1. "Controlling ownership interest" means ownership of/entitlement to more than 10 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 shareholders agreements or voting agreements.

   b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 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 10% 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. “Biometric information”, as defined in the Section 2(g) of the Aadhaar Act, means photograph, fingerprint, Iris scan, or such other biological attributes of an individual as maybe specified by Aadhaar (authentication) regulations.

vi. “Central Identities Data Repository” (CIDR), as defined in Section 2(h) of the Aadhaar Act, means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic in- formation and biometric information of such individuals and other information related thereto.

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

viii. “Demographic information”, as defined in Section 2(k) of the Aadhaar Act, includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history

ix. “Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:-

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

b. the Managing Partner, if the RE is a partnership firm,

c. the Proprietor, if the RE is a proprietorship concern,

d. the Managing Trustee, if the RE is a trust,

e. a person or individual, as the case maybe, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. 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.

Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

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

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

xii. 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.

xiii. Enrolment number means “Enrolment ID” as defined in section 2(1) (j) of the Aadhaar (Enrolment and update) Regulation, 2016 which means a 28 digit Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar.

xiv. “E-KYC authentication facility” as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the biometric information and /or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e- KYC data along with other technical details related to the authentication transaction.

xii “ Identity information”, as defined in sub-section (n) of section 2 of the Aadhaar Act, in respect of an individual, includes individual’s Aadhaar number, biometric information and demographic information.

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

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

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

Explanation 1: For the purpose of this clause, a document shall be deemed to be an OVD even if there is change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

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

xiv. Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar Act

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

AUTHUM

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

xvi. “Principal Officer” means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

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 in which:

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

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

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

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

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. Yes/No authentication facility”, as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing “ Yes” or “No”, along with other technical details related to the authentication transaction, but no identity information.

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

i. “Common Reporting Standards” (CRS) 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 a Regulated Entity (RE) 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 RE, but undertakes transactions with the RE.

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

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

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

Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

v. “Customer identification” 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 REs or meeting the officials of REs.

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. "Regulated Entities"(REs)means

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co- operative Banks (SCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as banks.

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFC)s, Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

d. All Payment System Providers (PSPs)/System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xiv. "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.

xv. Video based Customer Identification Process (V-CIP): an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE 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 Master Direction

xvi. "Wire transfer" means a transaction carried out, directly or through a chain of transfers, on behalf of an origin at or 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.

xvii. "Domestic and cross-border wire transfer": When the original 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

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

Sr.No.	A. List of KYC documents - For Individual applicants (As per RBI policy) wherein Permanent address is same as Current address(any one)	ID proof	Approved KYC as Address proof	Signature proof
1	Voter's Identify Card issued by Election Commission of India	Yes	Yes	
2	Valid Passport	Yes	Yes	
3	Valid Driving License. Learning License Not permitted.	Yes	Yes	
4	PAN Card (additional address proof to Be collected).	Yes	No	
5	Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhar number or Aadhar card. Acknowledgement receipt is not Acceptable	Yes	Yes	
6	Job card (with photo) issued under Mahatma Gandhi National Rural Employment Guarantee Act (NREGA) duly signed by an authorized officer of The State Government.	Yes	Yes (if it is with address)	
Note: As per RBI Circular RBI/2015-16/213 (DBR.AML.BC. No. 46/14.01.001 /2015-16) dated October 29, 2015, we may accept a copy (which is self-certified and OSV done) of marriage certificate issued by the State Government or Gazette notification indicating change in name together with a self-certified copy of the 'officially valid document' in the existing name of the person.				
Incase of Low Risk Customers				
7	Identity card with applicant's photograph issued by Central / State Government Departments (like Photo Ration card), Statutory / Regulatory Authorities (like ICAI, ICSI, ICWAI member ID card), Public Sector Undertakings (IOC, BPCL, HPCL employee ID card), Scheduled Commercial Banks (Banks like SBI, PNB, ICICI, etc..) and Public Financial Institutions	Yes	Yes (if it is with address)	

AUTHUM

8	Letter issued by a gazette officer, with a duly attested photograph of the person Only acceptable with photograph.	Ye s	Yes (if it is with address)	
9	Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);	No	Yes	
10	Property Tax or Municipal Tax receipt for the owned accommodation;	No	Yes	
11	Bank account or Post Office savings Bank account statement; (can be Accepted as ID proof if photo attested)	Ye s	Yes	
12	Pension or family pension payment orders (PPOs) is-sued to retired employees by Government Departments or Public Sector Undertakings, if they contain the Address	No	Yes	
13	Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such Employers allotting official Accommodation	No	Yes	
14	Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India (Work/Resident Permit, Social Security Card, Green Card etc.)	No	Yes	

Sr.No.	B. List of KYC documents - For Individual applicants wherein Permanent address is different from Current address	ID proof	Address proof	Signature proof
	Note: In addition to above KYC documents for both ID & address, we need to collect any ONE of the following address documents as proof for current address.			
1	Voter's Id	Yes	Yes	NO
2	Utility Bills - Telephone (land or Mobile) / Electricity (in applicant's name). Not greater than 3 full calendar months old. Example: If file log in has been done on 20th April 2010 then last three months would imply Jan 2010 onwards.–		Yes	NO
	PAN Card	Yes	NO	Yes
3	Passport	Yes	Yes	Yes
4	Valid Driving License. Learning License not permitted.	Yes	Yes	Yes
5	Life Insurance Policy. If the address has changed since then. The applicant needs to provide the latest Renewal premium paid receipt reflecting the New address, along with policy.	NO	Yes	NO
6	Municipal/Corporation tax/ Corporation Water tax / Water charges payment voucher or bill. Not more than 3 full calendar months old.	NO	Yes	NO
7	Printed Gas bill/ Gas receipt with the addressed early mentioned. Not more than 3 full calendar months old. Gas Book not accepted.	NO	Yes	NO
8	Printed Bank statement having the customer's current residential address. E-statements are also acceptable (along with a ATM generated mini statement with overlapping transactions with the E-statements). Bank passbooks (with entries more than 6 month old).	Yes (if photo affixed)	Yes	NO

	Above documents can be accepted as ID proof if it has photo affixed with Bank manager sign and seal			
9	Registered sale deed or sale agreement.	Yes (if photo affixed)	Yes	NO
10	Registered lease deed or leave and license agreement (rent agreement). At least 6 months old document either franked or on stamp paper. The stamp paper date / franking date should confirm the age of the document.	NO	Yes	NO
11	RC copy of 4 wheeler.	NO	Yes	NO
12	Ration card. (if the photo ration card has a family photo and the applicant's part of the family photo, then the document is a valid ID proof)	Yes (if photo affixed)	Yes	NO
13	Allotment letter issued from Gov- Government departments for government employees can betaken as address proof. Should have name and sign of issuing authority	Yes (if photo affixed)	Yes	NO
14	Employee ID card (For government employees & CAT-A Company only).	Yes	NO	NO
15	Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhar number or Aadhar card. Acknowledgement receipt is not acceptable	Yes	Yes	NO
16	Government Medical insurance card	Yes	NO	NO
I.	In cases where any of the above listed valid address proof documents are NOT available (section B). Address proof in the name of PARENT/CHILDREN/SPOUSE together with a relationship proof document establishing the relationship may be accepted. Acceptable Relation- ship Proof for applicant staying in the residence of a relative (Parent/Child / Spouse); Marriage Certificate, Birth Certificate, Passport, PAN Card, Voter's Id, Ration Card.			
II.	In the above situation, it is mandatory to collect the KYC of the person whose address proof is being taken.			

III.	A declaration from the address proof holder that he is aware that his relatives (exact relation) have applied for a loan and he has no objection.
Note:	
1	The above list is applicable to all new borrower segments.
2	KYC documents are not required to be collected for existing borrower segment in case there is no change in address. In case of change of address or change in name/surname above KYC policy will apply.
3	In case the existing borrower segment, new KYC documents will have to be collected if the loan is tagged as PEP.

****