FYNX CAPITAL LIMITED
(Formerly known as Rajath Finance Limited)

Policy Guidelines on 'Know Your Customer' norms and Anti-MoneyLaundering measures

Table of Contents

1. Introduction

Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards for Non-Banking Finance Companies (NBFCs) thereby setting standardsfor prevention of money laundering activities and corporate practices while dealing with their customers vide Circular Nos.: DNBS (PD) CC No. 34/10.01/2003-04, dated 06-01-2004, DNBS (PD) CC No. 48/10.42/2004-05, dated 21-02-2005, DNBS (PD) CC No. 64/03.10.042/2005-06, dated 07-03-2006, **RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 (Updated as on November 06, 2024)**.

FYNX Capital Limited (Formerly known as Rajath Finance Limited) and herein after referred to as (FYNX or the Company), being a Non-deposit taking Non-Systemically Important Bale Level NBFC (NBFC-BL), it 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 the Company, 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.

The Company endeavors to frame a proper policy framework on 'Know Your Customer' (KYC) and Anti- Money Laundering measures. The Company is committed for transparency and fairness in dealing withall stakeholders and in ensuring adherence to alt laws and regulations. The Company ensures that the information collected from the customer for any purpose would be kept as confidential and not divulgeany details thereof for cross selling or any other purposes. The Company commits that information soughtfrom the customer is relevant to the perceived risk, is not intrusive, and is in conformity 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.

The Company shall also communicate its KYC norms to its customers. The Company shall ensure that the implementation of the KYC norms is the responsibility of the entire organisation.

The Company'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:

i) A person or entity that maintains and/or has a business relationship with the Company;

ii) One on whose behalf such relationship is maintained (i.e. the beneficial owner);

iii) Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and;

iv) Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say, a wire transfer or issue of a high value demand draft as a single transaction.

2. Objective:

A. To ensure the integrity and stability of the financial system

The objective of KYC guidelines is to ensure the integrity and stability of the financial system and to prevent the Company from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) activities. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The Company hereunder framing its KYC policies incorporating the following four key elements:

(i) Customer Acceptance Policy

(ii) Risk management.

(iii) Customer Identification Procedures (CIP);

(iv) Monitoring of Transactions; and

B. To dissociate from Money Laundering and Terrorist Financing transactions

The Company with an object to eliminate the risk of being used for Money Laundering and Terrorist Financing activities shall carryout the following Risk Assessment Exercises:

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

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

(b) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. The Company would exercise such risk assessment exercise

at least once in a year.
(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) with controls and procedures in this regard. The Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

3. Appointment of Designated Director*:*

(a) The Governing Board of the company shall nominate a "Designated Director" to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules thereunder.

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

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

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

4. Appointment of Principal Officer:

(a) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

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

(c) The name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.

5. Compliance of KYC policy

(a) The Company shall ensure compliance with KYC Policy through:

(i) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.

(ii) Allocation of responsibility for effective implementation of policies and procedures.

(iii) Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements.

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

(v) Submission of quarterly audit notes and compliance to the Audit Committee.

(b) **The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced**

6. Customer Acceptance Policy (CAP)

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

- No account is opened in anonymous or fictitious/benami name.
- The Company shall take the mandatory information for KYC purpose while opening an account and during the periodical update of such KYC.
- PAN shall be mandatorily checked for every loan applicant. A declaration in Form No. 60 as per the provisions of Income Tax Rule 114B shall be obtained from persons [*not being a company or a firm*] who do not have PAN or equivalent e-document thereof.
- No account is opened where the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- No transaction or account-based relationship is undertaken without following the CDD procedure, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
- The Company shall open accounts of its customers using Adhar OTP based new registration. It would ensure that transaction alerts, OTP, etc. are sent only to the mobile number of the customer registered with Aadhaar. The Company shall have a robust process of due diligence for dealing with requests for change of mobile number in such accounts.
- Video based Customer Identification Process (V-CIP) shall be adopted by the Company. Further, the (i) the validity of Aadhaar XML file / Aadhaar Secure QR Code and (ii) to undertake the video process shall be 'three working days. Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, The Company shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company shall ensure that no incremental risk is added due to this.
- In case of Sole Proprietary firms, "Udyam Registration Certificate" (URC) shall be accepted as a proof of Identity of the firm. This will be in addition to the KYC of Proprietor as applicable to any individual applicant.
- Additional information, where such information requirement has not been specified in the internal KYC Policy of the Company, shall be obtained with the explicit consent of the customer.
- The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account or avail any other product or service, there shall be no need for a fresh CDD exercise by the Company as far as identification of the customer is concerned.
- KYC documents downloaded from the CKYCR, but whose validity has lapsed, shall not be used by the Company for KYC purposes. CDD Procedure is followed for all the joint account holders, while opening a joint account as well as for guarantors in the loan account (if any).
- CDD exercise shall be carried out where a change in Address is reported by the customer with regard to new proof of address verification.
- The Company shall devise a suitable system 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 indicated in Chapter IX of Master Direction - Know Your Customer (KYC) Direction, 2016 or as may be changed from time to time.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- Accounts of Politically Exposed Persons: Customer Due Diligence (CDD) measures shall be made applicable to Politically Exposed Person (PEP) and their family members or close relatives. In case of new application of any Politically Exposed Person (PEP) and their family members or close relatives or in the event ofan existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain senior management approval to make the account operational or to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.
- Where the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.
- HIRING AND TRAINING Human Resource Department, Legal & Compliance and Operations Department shall conduct an employee training program of members of staff to ensure that they are adequately trained in KYC/AML procedures. Proper staffing of the audit function with adequately trained and well-versed in AML/CFT policies shall be ensured.

7. Risk Management

- The Company shall classify customers into various risk categories and based on riskperception decide on acceptance criteria for each customer category.
- Accept customers after verifying their identity as laid down in customer identification procedures.
- While carrying out due diligence the Company shall ensure that the procedure adopted shall not result in denial of services to the genuine customers especially those, who are financially or socially disadvantaged.
- For the purpose of risk categorisation of customer, Company shall obtain the relevant information from the customer at the time of account opening. The company will include parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc.
- While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
- The risk categorization of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.
- The company shall obtain KYC Identifier with explicit customer consent to download KYC records from CKYCR, for the purpose of CDD.
- The Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar
- The company shall make a robust process of due diligence for dealing with requests

for change of mobile number in such accounts

- Parameters of risk perception for customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs – as explained in Annex II) may, if considered necessary, be categorized even higher;
- Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirementsof Prevention of Money Laundering (PML) Act, 2002 and guidelines issued by Reserve Bank from time to time;
- The Company shall not open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the Company. It shall be necessary to have suitable built-in safeguards to avoid harassment of the customer. For example, decision to
- close an account shall be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
- Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be clearly spelt out in conformity with the established law and practice
- Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
- The Company shall prepare a profile for each new customer based on risk categorisation.The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the Company. However, while preparing customer profile the Company shall take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.
- For the purpose of risk categorisation, 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 categorised as low risk.Illustrative examples of low-risk customers would be salaried employees whose salary structures are well defined, people belonging to 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 the Company 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. the Company 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
    - non-resident customers,
    - high net worth individuals,
    - trusts, charities, NGOs and organizations receiving donations,
    - companies having close family shareholding or beneficial ownership,
    - firms with 'sleeping partners',
    - politically exposed persons (PEPs) of foreign origin,
    - non-face to face customers, and
    - those with dubious reputation as per public information available, etc.

- Adoption of customer acceptance policy and its implementation shall not become too restrictive and shall not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged.

- As advised by RBI under Circular No. DNBS(PD)CC.No.193/03.10.42/2010-11, the Company shall not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits the Company's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

8. Customer Identification Procedure (CIP)

In order to eliminate risk envisaged under AML/TF, the policy clearly spells out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a business relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

The Company shall undertake identification of customers in the following cases:

a. At the commencement of an account-based relationship with the customer.
b. When the Customer is carrying out any international money transfer operations for a person who is not an account holder of the Company.
c. The Company has a doubt about the authenticity or adequacy of the customer identification data it has obtained.
d. While Selling third party products as agents, selling their own products, payment of dues of any other product having value of more than rupees fifty thousand.
e. At the time of carrying out transactions for any non-account-based walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
f. When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold

of rupees fifty thousand.

g. The Company shall ensure that introduction is not to be sought while opening accounts.

9. Video based Customer Identification Process

(a) V-CIP Infrastructure

i. The Company shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with relevant RBI guidelines. 60Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

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

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

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

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

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

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

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

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

conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

i. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official will carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

ii. Disruption of any sort including pausing of video, reconnecting calls, etc., will not result in creation of multiple video files. In case of call drop / disconnection, fresh session shall be initiated.

iii. The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded. iv) Any prompting observed at end of customer shall lead to rejection of the account opening process.

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

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

a. OTP based Aadhaar e-KYC authentication
b. Offline Verification of Aadhaar for identification
c. KYC records downloaded from CKYCR, in accordance with paragraph 56, using the KYC identifier provided by the customer
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi-Locker.

vi. The Company shall ensure to redact or blackout the Aadhaar number in terms of paragraph 16 of MD- Know Your Customer (KYC) Direction, 2016.

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

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

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

viii. The Company shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN

details shall be verified from the database of the issuing authority including through DigiLocker.

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

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

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

xii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process and its acceptability of the outcome.

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

(c) V-CIP Records and Data Management

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

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

10. Identification of Beneficial Owner

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

(a) 104Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

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

11. Due Diligence for all the customers will be made as per the Company's "Customer Due Diligence Policy"

A. Due Diligence by the Company:

The Company exercise due diligence in accordance with its Due Diligence Policy and if needed, may take the assistance of third parties for the purpose.

B. Due Diligence through third party:

For the purpose of verifying the identity of customers at the time of commencement of an

account-based relationship, the Company shall at rely on customer due diligence done by a third party, subject to the following conditions:

(a) Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

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

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

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

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

C. Due Diligence for individuals:

The following documents/certified copies shall be collected from an individual for establishing an account-based relationship or while dealing as a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where,

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

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

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

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

(ac) the KYC Identifier with an explicit consent to download records from CKYCR; and

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

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

Provided that where the customer has submitted,

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

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

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

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline

verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under Annex I.
v) KYC Identifier under clause (ac) above, the Company shall retrieve the KYC records online from the CKYCR.

D. The Company shall undertake opening Accounts using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

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

E. The Company may undertake V-CIP to carry out:

i. CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.
ii. In case of CDD of a proprietorship firm, the Company shall also obtain the equivalent e-document
iii. of the activity proofs with respect to the proprietorship firm, as mentioned in paragraph 28 and paragraph 29, apart from undertaking CDD of the proprietor.
iv. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication.
v. Updation/ Periodic updation of KYC for eligible customers.

12. Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs):

In case a person who desires to open an account is not able to produce documents, as specified in paragraph 16 of MD Know Your Customer (KYC) Direction, 2016, the Company

may at its discretion open accounts subject to the following conditions:

i. The NBFC shall obtain a self-attested photograph from the customer.
ii. The designated officer of the NBFC certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
iii. CDD as per paragraph 16 or paragraph 18 of MD Know Your Customer (KYC) Direction, 2016 shall be carried out. The account shall remain operational initially for a period of twelve months, within which CDD as per paragraph 16 or paragraph 18 of MD Know Your Customer (KYC) Direction, 2016 shall be carried out.
iv. Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.
v. The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
vi. The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (iv) and (v) above are breached by him.
vii. The customer shall be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (iv) and (v) above.
viii. The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established through Adhar Card Verification or shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.
ix. KYC verification once done by one branch/office of the company shall be valid for transfer of the account to any other branch/office, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

13. For opening an account in the name of a sole proprietary firm, certified copies any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

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

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

14. **For opening an account of a company**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    i. Certificate of incorporation
    ii. Memorandum and Articles of Association
    iii. 84Permanent Account Number of the company
    iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
    v. Documents, as specified in paragraph16, relating to beneficial owner, the managers, officers or employees, as the case may be holding an attorney to transaction the company's behalf
    vi. the names of the relevant persons holding senior management position; and
    vii. the registered office and the principal place of its business, if it is different.

15. **For opening an account of a partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    i. Registration certificate
    ii. Partnership deed
    iii. Permanent Account Number of the partnership firm
    iv. Documents, as specified in paragraph16 of MD, Know Your Customer (KYC) Direction, 2016, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
    v. the names of all the partners and
    vi. address of the registered office, and the principal place of its business, if it is different.

16. **For opening an account of a trust**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    i. Registration certificate
    ii. Trust deed
    iii. Permanent Account Number or Form No.60 of the trust
    iv. Documents, as specified in paragraph16, relating to beneficial owner, managers, officers or employees, as the case may be holding an attorney to transact on its behalf
    v. the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust
    vi. address of the registered office of the trust; and
    vii. the list of trustees and documents, as specified in paragraph 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

17. **For opening an account of an unincorporated association or a body of individuals,** certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
    i. Resolution of the managing body of such association or body of individuals
    ii. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
    iii. Power of attorney granted to transact on its behalf
    iv. Documents, as specified in paragraph 16 of Know Your Customer (KYC) Direction, 2016, relating to beneficial owner, managers, officers or

employees, as the case may be, holding an attorney to transact on its behalf and

v. Such information as may be required by the Company 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.

18. For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust,

i. certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

ii. Document showing name of the person authorised to act on behalf of the entity

iii. Documents, as specified in paragraph 16 of Know Your Customer (KYC) Direction, 2016, of the person holding an attorney to transact on its behalf and

iv. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Provided that in case of a trust, the Company shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (e) and (f) of paragraph 13 of MD Know Your Customer (KYC) Direction, 2016.

19. Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

i. Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of paragraph 17): Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by the Company for non-face-to-face customer onboarding (other than customer onboarding in terms of paragraph 17 of Know Your Customer (KYC) Direction, 2016):

ii. The Company shall introduce the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

iii. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. The Company shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

iv. Apart from obtaining the current address proof, The Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

v. The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

vi. First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

vii. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

B. Business Relationship with "Politically Exposed Persons" (PEP)

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

i. The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

ii. Reasonable measures are taken by the Company for establishing the source of funds / wealth;

iii. the approval to open an account for a PEP shall be obtained from the senior management;

iv. all such accounts are subjected to enhanced monitoring on an on-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;

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

Explanation: For the purpose of this paragraph, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country,

20. Client accounts opened by professional intermediaries:

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

i. Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.

ii. The Company 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.

iii. The Company shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Company.

iv. All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of the Company, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled, the Company shall look for the beneficial owners.

v. The Company shall, at their 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.

vi. The ultimate responsibility for knowing the customer lies with the Company.

21. On-going Due Diligence/Monitoring of Transactions

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

The Company shall prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits, Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attentionof the Company.

The Company does not accept any deposits. Further, there are no operative accounts where in the need for fixing the threshold limits for individual transactions and aggregate is more relevant and necessary. Most of the Company's loans are EMI based loans on all categories of borrowers. Hence the transactions with the Company are purely shall be restricted to the EMI/loan repayable over the tenor of the loan. Hence while the threshold limit for transactional basis is restricted to the EMI/loan payable, the threshold for turnover shall be restricted to the aggregate EMIs payable year after year. No other transactions what so ever nature other than repayment of loan with interest is carried out by the customer with the Company. Therefore, there shall be no occasion of

i. **High account turnover inconsistent with the size of the balance maintained.**

ii. **Deposit of third-party cheques, drafts, etc. in the existing or newly opened accounts followed by cash withdrawals for large amounts.**

In view of the risks involved in cash intensive businesses, the Company shall discourage its customers against transactions in cash as repayment in their loan accounts and all cash transactions would be monitored on daily basis. Further the accounts of bullion dealers (including sub-dealers) and jewelers, who normally transact in cash, should also be categorized as 'high risk' requiring enhanced due diligence. The Company shall classify such bullion dealers and jewelers under "high risk" category and any transactions in their loan accounts would be monitored on daily basis.

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

The Company shall put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation of customers shall be carried out at a periodicity of not less than once in six months.

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

22. Periodic Updation of KYC: The Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. The Company shall introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened.

S.NO	Basis Risk category	Frequency
1	High risk customers	Once in every two years from the date of opening of the account / last KYC updation
2	Medium risk customers	Once in every eight years from the date of opening of the account / last KYC updation
3	Low risk customers	Once in every ten years from the date of opening of the account / last KYC updation

a. In case of Individual Customer

iii. Where there is no change in the KYC information: a self-declaration from the customer in this regard shall be obtained through customer's registered email-id, customer's mobile number registered with the Company, mobile application of the Company), letter, etc.

iv. Where there is change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's registered email-id or customer's mobile number registered with the Company or through digital channels like mobile application of the Company), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc.

v. The Company, may obtain a copy of OVD or deemed OVD, or the equivalent e-documents thereof (as defined in Master Direction DBR.AML.BC.No.81 /14.01.001/2015-16), for the purpose of proof of address, declared by the customer at the time of updation/ periodic updation.

vi. The Company may use Aadhaar OTP based e-KYC in non-face to face mode for periodic updation. To clarify, conditions stipulated in paragraph 17 are not applicable in case of updation/ periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

vii. Declaration of current address, where the current address is different from the address in Aadhaar, the Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b. In case of Customer other than individuals:

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

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

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

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

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

x. Acknowledgment is provided to the customer mentioning the date of receipt of

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

xi. In order to ensure customer convenience, The Company will have the facility of periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of the Company s or any committee of the Board to which power has been delegated.

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

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

f. The Company shall give the customer an accessible notice and a reasonable opportunity to be heard before temporarily ceasing operations for an account, Further, for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, appropriate relaxation(s) would be given for continued operation of their accounts for a reasonable time. Till such time, such accounts shall be subject to enhanced monitoring.

g. In case any customer having an existing account-based relationship does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60 and gives it in writing, the Company shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

23. Record Management

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

(a) maintain all necessary records of transactions between the Company 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 swiftly, the identification records and transaction data to the competent authorities upon request;

(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so

as to permit reconstruction of individual transaction, including the following:
(i) the nature of the transactions;
(ii) the amount of the transaction and the currency in which it was denominated;
(iii) the date on which the transaction was conducted; and
(iv) the parties to the transaction.
(f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

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

24. Reporting Requirements to Financial Intelligence Unit - India

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

Explanation: *In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.*

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 the Company which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of the Company, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

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

The Company, 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 under paragraph 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

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.

25. Requirements/obligations under International Agreements –

(a) **Communications from International Agencies**

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

B. The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at **www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list**

C. 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**

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

(c) 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 (MHA) as required under UAPA notification dated 128(Annex II of this Master Direction). February 2, 2021

(d) Freezing of Assets under section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated 129February 2, 2021 (Annex II of this Master Direction), shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

(e) **Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)**:

i. The Company shall ensure meticulous compliance with the "Procedure for Implementation of section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of

section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

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

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

iv. In case of match in the above cases, the Company 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.

v. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

vi. The Company shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.

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

viii. In case an order to freeze assets under section 12A is received by the Company from the CNO, the Company shall, without delay, take necessary action to comply with the Order.

ix. 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 the Company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

x. The Company 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.

xi. In addition to the above, the Company 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.

xii. The Company 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.

(f) Jurisdictions that do not or insufficiently apply the FATF Recommendations

i. 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. REs 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.

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

Explanation: The processes referred to in (i) & (ii) above do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(g) 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.

The Company shall endeavour to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

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

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

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

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

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

C. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

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

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

F. Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site **http://www.incometaxindia.gov.in/Pages/default.aspx**. The Company shall refer to the following:

i. updated **Guidance Note** on FATCA and CRS

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

Annexure — I

Customer Identification Procedure Features to be verified and documents that shall be obtainedfrom customers

KYC CHECKLIST	
Features to be verified and documents that shall be obtained from customers	
Features	**Documents**
Identity Proof (Individual)	Passport
	Photo PAN card
	Voter's Identity Card / UID Aadhar Card
	Laminated Driving license - Permanent. For a Driving license coming in abooklet form (Not laminated) to be acceptable as KYC document, an OSVdone by the Company (RFL) employee on the photocopy of the Driving license would be mandatory.
	Employee ID card (MNCs / PSUs / Public Limited Companies/Other Government companies and not Pvt. Ltd. Co)
	Photo Ration Card
	Photo Debit Card
	Bankers' verification/passbook with stamp on photograph along with applicant's signature. This can be accepted provided it contains customer's photo and signature, a/c number, date of opening, branch name, address andit shall be certified only by the Branch Manager or Operations Head with theirname & designation.
	Defence ID Card
	Photo credit Card - provided the card is valid & current and is at least 3 months old
Address Proof (Individual)	Telephone Bill
	Life Insurance Premium receipt of any insurer (Policy shall be minimum 12 months in force)
	Post paid Piped gas connection bill showing consumption and full address
	Electricity Bill
	Ration Card
	Voter's Identity Card
	Laminated Driving license - Permanent. For a Driving license coming in a booklet form (Not laminated) to be acceptable as KYC document, an OSVdone by the Company (RFL) employee on the photocopy of the Driving license would be mandatory.

KYC Docs for Entities (Self Proprietorship / Partnership / Companies)

a) Proof of Legal Existence and Registered Office Address	For Partnership firms, Partnership Deed or Certificate of Registration fromRegistrar of firms in case the firm is registered
	For Companies, MOA & AOA along with Certificate of Incorporation. In case ofPublic Limited Company, Certificate of Commencement of Business also to be taken.
	PAN Card of partnership firm or companies can be taken as proof of existence. (In this case separate proof of registered address needs to be taken)
	Sales tax registration Certificate
	Shop & Establishment Certificate
	Factory Registration Certificate
	SSI Registration Certificate
	Importer - Exporter Code Certificate
	GST Registration Certificate.
	Latest Bank Account Statement in the name of the Entity with full address mentioned which matches with the entity's address as per the Application form along with Banker's Verification of the Authorized Signatory of the entity
b) Proof of Operating Address	Telephone Bill / Electricity Bill in the name of the entity
	Leave & License agreement in the name of the entity if the entity is operating its business from a rented premises & the agreement is registered / notarized. Wherever notarized Leave & License agreement is taken, the notarization shallbe in original & the agreement shall be executed on a stamp paper as per the respective State Stamp Act (mail already circulated to all in the past on the same)
	IT Assessment Order
	Pan Intimation letter
	Acknowledged ITR of the entity
	Latest Bank Account Statement in the name of the Entity with full address mentioned which matches with the entity's address as per the Application form along with Banker's Verification of the Authorized Signatory of the entity
	In case of Self Proprietorship concerns, proof of the operating address couldbe taken in the individual's name as long as the Office FI is positive at the address from where the individual is operating his business. This shall matchwith the office address given by the individual as per the Application form. Office FI in this case shall not be negative on account of applicant not

	running business from the same premises.
c) Trust/Society	Certificate of registration, if registered
	Trust Deed/ Constitutional Documents of the trust / Society
d) Signature verification of the Authorized Signatory of the Entity	ECS mandate with the signatures of authorized signatories and with the stamp of entity - Verified and acknowledged by the banker pre-disbursement.
	Clearance of Initial payment cheque equal to an amount of the EMI and confirmed by local ops
	Certain companies have GPAs for signing PDCs. The GPA can be an SV subject to the GPA carrying the signature of the auth signatories along with their names & certified only by the Branch Manager or Operations Head with their name & designation. Care must be taken to verify the GPA for any specific covenants such as (a) If GPA is applicable for a particular bank account, and then PDCs must be from the same bank account (b) Whether GPA is valid indefinitely or has an expiry date. In a case where there is an expiry date then the validity of GPA shall be > contract tenure otherwise such GPA becomes invalid
	Documents which would have been submitted to banker at time of opening of account by the entity stating the authorised signatories of the bank account. These documents again shall be certified by the Branch Manager or Operations Head with their name & designation
	Bankers Verification of the Entity's Authorised Signatory from where the PDCs are issued.
Proprietary Concerns (Care: As per Circular No. RBI/2011-12/579 DNBS (PD).CC. No 275	i) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc

/03.10.42 /2011-12 dated May 29, 2012 any two of the documents listed should be obtained foridentity of the proprietory concern. These documents should be in the nameof the proprietory concern.)	ii) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. NBFCs/RNBCs may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.
	iii) The complete Income Tax return (not just the acknowledgement) in thename of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities.
	iv) Utility bills such as electricity, water, and landline telephone bills in thename of the proprietary concern.
	Two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Annexure - II

Customer Identification Requirements – Indicative

GuidelinesTrust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The Company shall determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, the Company shall take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', steps shall be taken to verify the founder managers/ directors and the beneficiaries, if defined.

Accounts of companies and firms

the Company need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the Company. The Company shall examine the control structure of the entity, determine the source offunds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public Company it shall not be necessary to identify all the shareholders.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The Company shall gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. The Company shall verify the identify of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP shall be taken at a senior level which shall be clearly spelt out in Customer Acceptance policy. The Company shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened for customers without the need for the customer to visit the Company branch. In the case of non-face- to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the company may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

Beneficial Ownership

As per Rule 9(IA) of the Prevention of Money Laundering Rules, 2005 the Company shall identify the beneficial owner and take all reasonable steps to verify his identity.

Beneficial Ownership has been defined in RBI Circular No. RBI/2012-13/422 DNBS (PD).CC. No 321
/03.10.42 /2012-13 dated February 27, 2013 as given below.

The term 'beneficial owner'; has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership.

The procedure as advised by the Government of India is as under:

A. Where the client is a person other than an individual or trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

(i) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to more than 25 percent of shares or capital or profits of the juridical person, where the juridical person is a company; ownership of/entitlement to more than 15% of the capital or profits of the juridical person where the juridical person is a partnership; or, ownership

of/entitlement to more than 15% of the property or capital or profits of the juridical person where the juridical person is an unincorporated association or body of individuals.

(ii) In cases where there exists doubt under (i) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements, etc.

(iii) Where no natural person is identified under (i) or (ii) above, the identity of the relevant natural person who holds the position of senior managing official.

B. Where the client is a trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify theidentity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

C. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Annexure -III

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash

Company transactions, that are denominated by unusually large amounts of cash, rather than normallyassociated with the normal commercial operations of the Company, e.g. cheques,

Transactions that do not make Economic Sense

Transactions in which assets are withdrawn immediately after being deposited unless the businessactivities of the customer's furnishes a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

Accounts with large volume of credits whereas the nature of business does not justify such credits.

Attempts to avoid Reporting/Record-keeping Requirements

(i) A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

(ii) Any individual or group that coerces/induces or attempts to coerce/induce a NBFC employee not to file any reports or any other forms.

(iii) An account where there are several cash transactions below a specified threshold level to a avoidfiling of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

(i) A customer/Company who is reluctant to provide complete information regarding the purpose ofthe business, prior business relationships, officers or directors, or its locations.

(ii) A customer/Company who is reluctant to reveal details about its activities or to provide financialstatements.

(iii) A customer who has no record of past or present employment but makes frequent large transactions.

Certain NBFC Employees arousing Suspicion

(i) An employee whose lavish lifestyle cannot be supported by his or her salary.

(ii) Negligence of employees/willful blindness is reported repeatedly.