ACHIIEVERS FINANCE INDIA LMTD

(FORMERLY KNOWN AS ACHIIEVERS FINANCE INDIA (P) LTD)

KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML) POLICY

1. INTRODUCTION

This KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML) POLICY has been approved by the Board of Directors of the Company at its meeting held on 01ST DAY OF FEBRUARY, 2021 and supercedes all earlier KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML) POLICY approved by the Board of Directors of the Company .The said Policy will come into effect on and from 01ST DAY OF FEBRUARY, 2021.

The Reserve Bank of India vide its circular no. RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No. 81/14.01.001/2015-16 dated 25 February, 2016 has made changes to the existing KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML) POLICY for better identification of customers and for prevention of money laundering. The Company has accordingly put in place 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards, covering KYC Standards and AML standards.

This policy document is prepared in line with the RBI guidelines.

2. POLICY OBJECTIVES

It is the Policy of Company that statutory and regulatory obligations to prevent money laundering are to be met in full.

The Company will exercise due care in order to minimize the risk of its services being abused for the purposes of laundering funds associated with drug trafficking, terrorism and other serious crime.

The objectives of the Policy are as follows:

i. To prevent criminal elements from using the Company as terminal for money laundering activities;

ii. To enable the Company to know/understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently;

iii. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;

iv. To comply with applicable laws and regulatory guidelines;

v. To take necessary steps to ensure that the concerned staffs are adequately trained in KYC/AML procedures.

3. SCOPE OF THE POLICY

This policy is applicable to all the offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time.

4. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

Money laundering is a process to make illegitimate money appear legitimate. It involves cleansing of dirty money engaging in a series of financial transactions. It is called 'dirty money' because it originates from criminal activities like drug trafficking, embezzlement, tax evasion, corruption, illegal gambling, smuggling, arson racketeering, illegal prostitution, fraud or any other illegal activity, with the objective of hiding their true source and making them legally usable.

Section 3 of the Prevention of Money Laundering Act, 2002 defines offence of money laundering as under:

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering."

The Company being a financial institution may be used at any point in the money laundering process. All financial centers are vulnerable and all financial institutions within those centers need to play their part in preventing the criminals from successfully laundering their criminal money.

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

5. OBLIGATTIONS UNDER THE PML ACT 2002

Section 12 of PML Act, 2002 places certain obligations on every banking company, financial institution and intermediary which include

i. Maintaining a record of prescribed transactions
ii. Furnishing information of prescribed transactions to the specified authority
iii. Verifying and maintaining records of the identity of its clients
iv. Preserving records in respect of (i), (ii), (iii) above for a period of 10 years from the date of cessation of transactions with the clients

6. COMPANY'S ROLE IN PREVENTING MONEY LAUNDERING

The prevention of money laundering has three objectives:

- **Ethical** - taking part in the fight against crime.
- **Professional** – ensuring that Company is not involved in recycling the proceeds of crime that would call into question its reputation, integrity and, if fraud is involved, its solvency.
- **Legal** - complying with RBI Regulations that impose a series of specific obligations on financial institutions and their employees.

The management and staff of the Company are expected to be aware of their personal legal obligations and the legal obligations of the Company, be alert for anything suspicious, and report suspicions in line with internal procedures

7. DEFINITION OF CUSTOMER

A Customer for the purpose of this policy is defined as:

i. A person or an entity that maintains an account and/or has a business relationship with the Company
ii. One on whose behalf the account 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.

8. DESIGNATED DIRECTOR

A "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 be nominated by the Board.

In the Company, Mr. Suman Chakrbarty is nominated as "Designated Director" and it is also informed to FIU IND.

9. PRINCIPAL OFFICER

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

Mr. Pankaj Kumar Das is designated as Principal Officer and it is informed to FIU IND.

10. KEY ELEMENTS OF THE POLICY

The KYC policy shall include following four key elements:

(a) Customer Acceptance Policy;

(b) Risk Management;

(c) Customer Identification Procedures (CIP); and

(d) Monitoring of Transactions

11. CUSTOMER ACCEPTANCE POLICY (CAP)

The Customer Acceptance Policy ensures that explicit guidelines are in place on the following aspects of customer relationship in the Company:

i. No accounts is to be opened in anonymous or fictitious/ benami name(s);

ii. No account is opened where the Company is unable to apply appropriate Customer Due Diligence ("CDD") measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

iii. No transaction or account-based relationship is undertaken without following the CDD procedure.

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

v. 'Optional'/additional information, is obtained with the explicit consent of the customer after the account is opened.

vi. 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 with the same Company, there shall be no need for a fresh CDD exercise.

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

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

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

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

xi. 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).

xii. Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

12. RISK MANAGEMENT

For Risk Management, the Company shall have a risk based approach which includes the following-

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

(b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity and information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy. Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

CUSTOMERS REQUIRING HIGH LEVEL OF MONITORING:

High Risk	*Low Risk*
Non Resident Accounts	Salaried Employees
High Net worth individuals	People belonging to lower economic Group with low turn over
Trust, Charities, etc.	Government Departments
Companies having close family shareholding	
Firms with sleeping partners	
Politically Exposed Persons (PEP)	

13. CUSTOMER IDENTIFICATION PROCEDURES (CIP)

This policy spells out the Customer Identification Procedure to be carried out at different stages. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. The Company needs to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship.

For customers that are natural persons, we have to obtain sufficient identification data to verify the identity of the customer, his/her address/location and also his recent photograph.

For customers that are legal persons or entities, we have to (i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identity and verify the identity of that person (iii) understand the ownership and control structure of the customer and determine who are the natural person who ultimately control the legal person.

The Customer Identification Procedures are to be carried out at the following stages:

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

(b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.

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

(d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(f) When 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.

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

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

(b) Adequate steps are taken 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.

14. CLIENT DUE DILIGENCE (CDD) PROCEDURE

In case of Individual

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

(a) the Aadhaar number where,

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

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

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.

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

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise and similar causes, the Company shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Company and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. The Company shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection and shall be available for supervisory review.

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

i. There must be a specific consent from the customer for authentication through OTP.

ii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

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

iv. 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.

v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification as per Section 16 is to be carried out.

vi. 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.

vii. 21A 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 Company. Further, while uploading KYC information to CKYCR, the Company shall clearly indicate that such accounts are opened using OTP based e-KYC and other companies shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode. viii. 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.

The Company may undertake live V-CIP, to be carried out by an official, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the Company performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information by carrying out Offline Verification of Aadhaar.

ii. A clear image of PAN card is captured 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.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India.

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

v. The official shall also ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

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

viii. The Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt.

ix. To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audiovisual interaction shall be triggered from the domain of the Company. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. It shall be ensured that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. The Company takes assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer.

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

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 Section 16, the Company, being a NBFC, may at their discretion open accounts subject to the following conditions:

(a) The Company shall obtain a self-attested photograph from the customer.

(b) The designated officer certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

(c) The account shall remain operational initially for a period of twelve months, within which CDD as per Section 16 shall be carried out.

(d) Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.

(e) The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.

(f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.

(g) 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 (d) and (e) above.

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

In case of Sole Proprietory Firm

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

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

(a) Registration certificate

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

(c) Sales and income tax returns.

(d) CST/VAT/ GST certificate (Provisional/ final)

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

(f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

(g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

(h) Utility bills such as electricity, water, landline telephone bills, etc.

In cases where the Company 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.

In case of Legal Entity

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

(a) Certificate of incorporation

(b) Memorandum and Articles of Association

(c) Permanent Account Number of the company

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

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

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

(a) Registration certificate

(b) Partnership deed

(c) Permanent Account Number of the partnership firm

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

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

(a) Registration certificate

(b) Trust deed

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

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

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

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

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

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

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

(e)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.

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

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

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

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

15. 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)Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

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

16. On Going Due Diligence

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; and the source of funds.

17. PERIODIC UPDATION

The policy will reviewed be at yearly intervals or as and when considered necessary by the Board.

18. ENHANCED DUE DILIGENCE

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

b. **Accounts of Politically Exposed Persons (PEPs):** The identity of the person shall be verified before accepting him as a client and sufficient information including source of funds, accounts of family members and close relatives are collected.

   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. The CDD measures includes enhanced monitoring ongoing basis.

c. **Client accounts opened by professional intermediaries:**

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

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

   (b) It 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) It 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.

   (d) All the beneficial owners shall be identified.

   (e) The Company 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.

   (f) The ultimate responsibility for knowing the customer lies with the Company.

d. Foreign Portfolio Investors (FPI)

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

19. RECORD MANAGEMENT

As per the RBI regulations, the Company is required to keep records of account opening forms, vouchers, ledgers, registers etc pertaining to transactions for 10 years. In addition, the Company should maintain the following documents, like, Customer Profile, Reports made to Government authorities concerning suspicious activities with supporting documentation, records of all money laundering training, nature of transactions, amount of the transaction and the currency in which it was denominated, date on which transaction was conducted and parties to the transaction etc.

20. REPORTING REQUIREMENTS TO FIU-IND

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.

21. JURISDICTIONS THAT DO NOT OR INSUFFICIENTLY APPLY THE FATF RECOMMENDATIONS

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

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

(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.

22. CDD PROCEDURE AND SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

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

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

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

(d) The Company 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.

23. HIRING OF EMPLOYEES AND EMPLOYEE TRAINING

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

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

24. ADHERENCE TO KNOW YOUR CUSTOMER (KYC) GUIDELINES BY NBFCS

(a) Persons authorised by the Company for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to the Company.

(b) All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by the Company including brokers/agents etc. who are operating on their behalf.

(c) The books of accounts of person authorised by the Company including brokers/agents, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

Digital KYC Process

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

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

C. The client, for the purpose of KYC, shall visit the location of the authorized official of the Reporting Entity or vice-versa. The original Officially Valid Document (OVD) shall be in possession of the client.

D. The Reporting Entity must ensure that the Live photograph of the client is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Reporting Entity shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Reporting Entities) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the client.

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

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

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

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

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

used for client signature. The Reporting Entity must check that the mobile number used in client signature shall not be the mobile number of the authorized officer.

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

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

L. The authorized officer of the Reporting Entity shall check and verify that: -

(i) information available in the picture of document is matching with the information entered by authorized officer in CAF.

(ii) live photograph of the client matches with the photo available in the document.; and

(iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF shall be digitally signed by authorized representative of the Reporting Entity who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.