GODREJ FINANCE LIMITED

Know Your Customer and Anti Money Laundering Policy

Contents

1. BACKGROUND, OBJECTIVES AND SCOPE 3
2. DEFINITIONS 3
3. POLICY STANDARDS 7
3.1 Compliance of KYC policy 7
3.2 The KYC and AML Policy has the following 4 key elements: 8
3.3 Customer Acceptance Policy (CAP) and Customer Due Diligence (CDD) 8
3.4 Risk Management 10
3.5 Customer Identification 13
3.6 Customer Due Diligence (CDD) Procedures 14
3.7 Enhanced Due Diligence (EDD) Procedures 18
3.8 Monitoring of Transactions/ On-Going Due Diligence 19
3.9 Appointment of the Designated Director and the Principal Officer 19
3.10 Reporting to the Financial Intelligence Unit-India (FIU-IND) 20
3.11 Record Management 21
3.12 Selling Third Party Products 22
3.13 Quoting of Pan 22
3.14 Introduction Of New Technologies 23
3.15 Customer Education 23
3.16 Hiring of Employees and Employee Training 23
3.17 Adherence to the KYC and AML Guidelines by the Company's Agents 23
3.18 Sharing KYC Information with Central KYC Records Registry (CKYCR) 24
3.19 Reporting Requirement Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS) 24
3.20 Compliance with Section 51A of Unlawful Activities (Prevention) Act, 1967 ("UAPA ACT") and Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD ACT") 24
3.21 Secrecy Obligations and Sharing of Information 24
4. Approval and Review of the KYC and AML Policy 25
Annexure 1 26

1. BACKGROUND, OBJECTIVES AND SCOPE

1.1 Background

The Prevention of Money Laundering Act, 2002 **("PMLA")** and the Rules notified thereunder impose several obligation on Banks, Non-Banking Financial Companies **("NBFC"),** Housing Finance Companies **("HFCs")**, Chit Fund Company and other defined intermediaries to inter alia verify identity of clients, maintain records and furnish requisite information to Financial Intelligence Unit- India **("FIU-IND").**

The Reserve Bank of India **("RBI")** has issued Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 on November 28, 2025 **("RBI KYC Directions")** applicable to all categories of Non-Banking Financial Company (hereinafter collectively referred to as 'NBFCs' and individually as an 'NBFC'), for all layers, unless specified otherwise.

In accordance with the PMLA and the RBI KYC Directions as amended from time to time, **Godrej Finance Limited ("GFL"** or **"the Company")**, has adopted Board approved 'Know Your Customer **("KYC")** and Anti-Money Laundering **("AML")** Policy **("KYC and AML Policy").**

1.2 Policy Objective

Key objectives of the KYC and AML Policy are as under:

(a) To establish regulatorily compliant KYC mechanism to on-board customers;

(b) To ensure compliance throughout the life cycle of customers as per the laid down norms;

(c) To prevent the Company's business channels/ products/ services from being used as a channel for Money Laundering **("ML")**/ Terrorist Financing **("TF")**;

(d) To establish a framework for adopting appropriate AML procedures and controls in the operations/ business processes of the Company;

(e) To ensure compliance with the laws and regulations in force from time to time;

(f) To protect the Company's reputation;

(g) To lay down KYC-AML compliance norms for the employees of the Company.

1.3 Applicability

This policy is applicable to all categories of products and services offered by the Company. All the employees of the Company, while dealing with its customers, will have to ensure adherence with the KYC and AML Policy.

2. DEFINITIONS

2.1 **"Aadhaar number"** means an identification number issued to an individual under sub-section (3) of Section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under said Act.

2.2 **"Aadhaar Act"** means Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016.

2.3 **"Authentication",** in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar Act.

2.4 "Beneficial Owner (BO)" means:

(a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/ have a controlling ownership interest *(means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company)* or who exercise control *(right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.)* through other means.

(b) In case of a partnership firm, the BO is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/ have ownership of/ entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation - "Control" shall include the right to control the management or policy decision.

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

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

(d) In case of a trust, the identification of BO shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

2.5 "Cash Transaction Report (CTR)" - CTR will include the following:

(a) all cash transactions of the value of more than Rs. 10 lakh or its equivalent in foreign currency;

(b) all series of cash transactions integrally connected to each other which have been individually valued below Rs. 10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency.

2.6 "Certified Copy of Officially Valid Document (OVD)" shall mean comparing the copy of Officially Valid Document with the original and recording the same as per the extant law and guidelines / directions.

2.7 "Central KYC Records Registry (CKYCR)" means an entity defined under Rule 2(1)(aag) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

2.8 "Counterfeit Currency Transaction" means Cash transactions where forged or counterfeit Indian currency notes have been used as genuine. These transactions should also include transactions where forgery of valuable security or documents has taken place.

2.9 "Counterfeit Currency Note Report" means Quarterly Report on status of receipt of counterfeit note received by any NBFC to RBI.

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

2.11 "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:
(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
(c) Determining whether a customer is acting on behalf of a beneficial owner and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

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

2.13 "Designated Director" means the Managing Director or a whole-time Director designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the Rules.

2.14 "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the Company as per the provisions contained in the PMLA. The Company will adhere to the applicable requirements in this regard which may be prescribed by the Government/ the RBI from time to time.

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

2.16 "Group" – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961). The definition reads as below:
"group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes:

(i) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or

(ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident;

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

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

2.19 "Non-face-to-face customers" - Customers who open accounts without visiting the branch/ offices of the Company or meeting its officials but will not include customers whose account has been opened as per Video Customer Identification Procedure.

2.20 "Officially Valid document (OVD)" - Any document defined as OVD under rule 2(1)(d) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and the amendments thereto ("**PML Rules**") or any document as may be specifically prescribed by the RBI as per the applicable regulations. Such OVD will be considered valid for verifying identity and proof of address of individual customer/ beneficial owner/ authorized signatory/ power of attorney holder.

Please refer to ***Annexure 1*** for list of OVDs and other documents which are currently considered valid for verifying identity and proof of address of customers.

2.21 "Offline Verification" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

2.22 "On-going Due Diligence" - Regular monitoring of transactions in accounts to ensure that they are consistent with RE's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

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

2.24 "Person" shall have the meaning as defined under RBI KYC Directions (and any amendment from time to time by RBI) which at present is as follows:
'Person' shall include:
(a) an Individual;
(b) a Hindu Undivided Family;
(c) a Company;
(d) a Firm;
(e) an association of persons or a body of individuals, whether incorporated or not;
(f) every artificial juridical person, not falling within any one of the above person (a to e);
(g) any agency, office or branch owned or controlled by any one of the above persons (a to f)

2.25 "Politically Exposed Persons (PEPs)" are individuals who are or have been entrusted with prominent public functions by a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

2.26 "Principal Officer (PO)" means a senior official at management level designated by the Board of Directors of the Company for overseeing and managing the KYC & AML policies and processes. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

2.27 "Suspicious transaction" means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

(a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime, regardless of the value involved; *or*

(b) appears to be made in circumstances of unusual or unjustified complexity; *or*

(c) appears to have no economic rationale or bona fide purpose; *or*

(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation - Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

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

(a) opening of an account;

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

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

(d) entering into any fiduciary relationship;

(e) any payment made or received in whole or in part of any contractual or other legal obligation;

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

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

3. POLICY STANDARDS

3.1 Compliance of KYC policy

(a) Senior Management for the purpose of KYC Compliance shall mean Designated Director and Principal Officer

(b) Designated Director on recommendation of Principal Officer shall be responsible for setting up the policies which will be approved by the Board on recommendation of Audit Committee

(c) Principal Officer with support of Compliance Team be responsible for overseeing the KYC operations of the Company

(d) Field Sales, operations and credit team shall be responsible for ensuring that policy is followed
(e) Internal Audit function will review the KYC operations as mentioned in paragraph 3.4.3 of the Policy
(f) Quarterly audit notes and compliance shall be submitted to the Audit Committee
(g) Decision-making functions of determining compliance with KYC norms shall not be outsourced

3.2 The KYC and AML Policy has the following 4 key elements:

(a) Policy for Customer Acceptance (CAP).
(b) Risk Management from money laundering risk perspective.
(c) Customer Identification Procedures (CIP).
(d) Procedures for monitoring of transactions, as applicable.

3.3 Customer Acceptance Policy (CAP) and Customer Due Diligence (CDD)

The Company will adhere to the following criteria for acceptance of customers:

(a) The Company will not open any account(s) in anonymous, fictitious or 'benami' name(s) and where proper due diligence cannot be applied.

(b) No account will be opened where the Company is unable to apply required 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 a Suspicious Transaction Report (STR), if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

(c) No transaction or account-based relationship will be undertaken without following appropriate CDD procedure.

(d) The mandatory information to be sought for KYC purpose at the time of login of loan / credit facility and during the periodic updation is being specified.

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.

(e) A Customer Identification File (CIF) number which is a Unique Customer Identification Code (UCIC) is being allotted while entering into new relationships with individual customers

(f) CDD procedure is being applied at the UCIC level & thus, if an existing KYC compliant customer of GFL desires to open another account or avail any other product or service from GFL, there shall be no need for a fresh CDD exercise as far as identification of the customer is concerned

(g) Additional information, if any as per internal policy, will be obtained with consent of the customer.

(h) CDD Procedure is being followed for all joint account holders also.

(i) A customer will be permitted to act on behalf of another person/ entity in accordance with the legal requirements.

(j) Identity of the customer shall not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. For this purpose, the Company will maintain lists of individuals or entities issued by RBI, United Nations Security Council, UAPA other regulatory & enforcement agencies etc. Details of accounts/ customers bearing resemblance with any of the individuals/ entities in such list shall be treated as suspicious and reported.

(k) PAN number/ Goods and Services Tax Number will be verified from the verification facility of the issuing authority.

(l) 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).

(m) In order to avoid fictitious and fraudulent applications of the customers and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company will conduct appropriate due diligence. Beneficiary of the relationship/ account shall also be identified.

(n) The nature and extent of basic due diligence measures to be conducted at the time of establishment of account opening/ relationship, will depend upon the risk category of the customers and involve collection and recording of information by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the risks posed by the applicant and the applicant's expected use of the Company's products and services from an AML perspective.

(o) The Company may rely on third party verification subject to the conditions prescribed by the RBI or the PMLA and the Rules thereunder in this regard.

(p) For non-face-to-face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised for identification and verification of such customers.

(q) The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without expressed consent of the customer.

(r) Appropriate Enhanced Due Diligence ("EDD") measures shall be adopted for high risk customers from AML perspective, especially those for whom the sources of funds are not clear and customers who are Politically Exposed Persons ("PEPs").

(s) In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate EDD measures shall be adopted.

(t) Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at the Principal Officer's level, after giving due notice to the customer explaining the reasons for such a decision.

(u) Suitable system as contained in Chapter XI of RBI KYC Directions shall be put in place/ to ensure that the identity of the customer which does not match with any person or entity, whose name appears in the sanctions lists If Company is suspicious 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.

The aspects mentioned in the CAP would be reckoned while evolving the KYC/AML procedures for various types of customers and products. However, while developing the KYC/CDD procedures, the Company will ensure that its procedures do not become too restrictive or pose significant difficulties in availing its services by deserving general public, especially the financially and socially disadvantaged sections of society, including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind (i.e. the process shall be more inclusive and accessible to all Persons with Disabilities, particularly acid attack survivors suffering from permanent facial or eye disfigurement and similarly placed individuals, including persons with blindness and low vision). In case the application or period updation of KYC of any customer is rejected, the reason(s) for such rejection shall be duly recorded by the Company's employee.

3.4 Risk Management

The Company will ensure that it has effective and appropriate KYC procedures. The overall KYC/ AML program will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibilities will be explicitly allocated within the Company to ensure that the Company's policies and procedures are implemented effectively.

3.4.1 Risk Categorization

The Company will categorize its customers into low, medium and high-risk category based on the assessment, profiling and perceived money laundering risk. Principles for risk-categorisation of customers are being laid down by the Company.

Risk categorisation is being undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. 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 categorisation of a customer and the specific reasons (including non-intrusive information) for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

3.4.2 Updation/Periodic Updation

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 will conduct periodic updation of KYC documents at least once in every 2 years for high risk customers, once in every 8 years for medium risk customers and once in every 10 years for low risk customers in any of the following manner:

(a) PAN verification from the verification facility available with the issuing authority.

(b) GST verification from the verification facility available with the issuing authority.

(c) Authentication of Aadhaar Number already available with the Company with the explicit consent of the customer in applicable cases.

(d) In case of individuals except low-risk customers, certified copy of OVD containing identity and address shall be obtained at the time of updation/periodic updation. In

case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

In case of change only in address, a self-declaration of the new address shall be obtained from the customer the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. Company may also obtain a copy of OVD for the purpose of proof of updated address.

In case of change in any other KYC information, Company shall undertake the KYC process equivalent to that applicable for onboarding a new individual customer.

(e) In case of Legal entities ("LE"), the Company shall review the documents sought at the time of grant of loan / credit facility and obtain fresh certified copies, incase of no change. However, in case of change in any KYC information, Company shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer

(f) The Company shall provide facility for of updation/ periodic updation of KYC at any branch for convenience of the customer.

(g) The Company will not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the borrower is required to establish their bona-fides. Normally, OVD/ Consent forwarded by the customer through mail/ post, etc., shall be acceptable.

(h) The Company shall send advance intimation to its customers to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including one intimation by letter, at appropriate intervals to its customers through Email, SMS, etc. for complying with the requirement of periodic updation of KYC. Further, after the due date, the Company shall give at least three reminders, including one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. Such letter of intimation/ reminder may, inter alia, contain instructions for updating KYC, customer escalation matrix, and such other information as the Company may deem fit. The Company shall record and maintain trail of issue of such advance intimation/ reminder against each customer for audit trail.

(i) The Company will provide an acknowledgment of following to the customer:
- receipt of the relevant document(s), including self-declaration for carrying out updation/periodic updation
- date on which periodic KYC updation was conducted

Note:

- The frequency for periodic updation prescribed above would apply from the date of disbursement of loan / last verification of KYC.
- Company shall advise the customers that in order to comply with the Prevention of Money Laundering Rules, in case of any update in the documents submitted by the customer at the time of establishment of relationship with the Company and thereafter, as necessary; customers shall submit to the Company the updated document within 30 days of the update to the documents for the purpose of updating the records with the Company.

- High risk accounts shall be subjected to more intensified monitoring. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

3.4.3 Internal Audit and Assurance

To provide reasonable assurance that its KYC and AML procedures are functioning effectively, audit of its KYC and AML processes will also be covered under the scope of Internal Audit of the Company. The audit findings and compliance thereof will be put up before the Audit Committee of the Board till closure of audit findings.

3.4.4 Money Laundering ("ML") and Terrorist Financing ("TF") Risk Assessment

It is understood that the ML and TF risks for the Company are likely to be low due to the following reasons:

(a) The Company does not operate in other countries/ geographies;

(b) The Company does not source/ originate loans from other countries/ geographies and its customer base consists of Indian nationals only;

(c) The Company extends loans to identified borrowers for which rigorous KYC checks have been put in place

(d) The Company does not offer banking, liabilities and insurance products; and

(e) The Company offers loans/ credit facilities with defined end-use and verifies the same.

However, in accordance with the regulatory requirements, the Company is carrying out ML and TF Internal Risk Assessment (IRA) exercise periodically to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels etc.

Such assessment process will consider various 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, Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share.

The Company may refer to Internal Risk Assessment Guidance for Money Laundering/ Terrorist Financing Risks issued by RBI and involve officials from various teams such as Product, Customer service and Internal audit.

The Internal risk assessment exercise and the methodology by the Company will be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company.

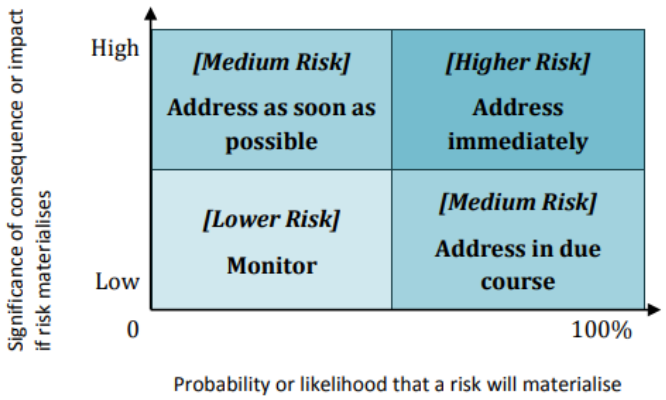
The risk assessment shall involve relevant functions and have the following stages:

(a) **Identification**- Development of list of potential risks or risk factors drawn from known/ suspected threats or vulnerabilities. For this purpose, various important aspects of the KYC Policy (non-compliance of which may pose threat to the Company) will be identified along with the risks which the Company may be exposed to due to the same.

(b) **Analysis**- Implementation of key requirements under the KYC Policy should be analyzed. This stage should analyse the likelihood and the impact of each of the identified risks. It will help in assigning priority/ importance to each of the risks.

(c) **Evaluation-** It should involve taking the results found during the analysis process to determine priorities for addressing the risks. These priorities should contribute to

development of a strategy for their mitigation. A typical Risk Evaluation matrix would be as under:



The Company shall conduct the ML and TF IRA based on Risk based approach (RBA) covering Business Level IRA and individual (Customer) Level IRA on half-yearly frequency. The outcome of the ML and TF IRA will be put up to the Audit Committee. The IRA report may include the following details:

(a) Brief profile of the Company
(b) Executive summary;
(c) Threats of ML/TF faced;
(d) Inherent ML/TF risks and vulnerabilities assessed;
(e) Methodology applied for the assessment;
(f) ML/TF risk-factors assessed;
(g) Controls applied;
(h) Residual risk identified;
(i) Outcomes;
(j) Mitigating measures proposed;
(k) Enforcement actions taken by supervisors, LEAs, etc., during the last five years;
(l) Observations and findings of internal audit regarding AML/CFT measures;
(m) Case studies or illustrations may be included, wherever appropriate.

The Company is committed to ensuring that it is not made a vehicle for any kind of money laundering or terror financing. For this purpose, Company will, if required, share information with its group entities while maintaining confidentiality of information with confirmation that such information will not be used for any tip-off.

3.5 Customer Identification

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

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

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

(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 or any other product for more than Rs. 50,000/-.

(e) Carrying out transactions for a non-account-based customer where the amount involved is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.

(f) When it has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

3.5.2 Reliance on customer due diligence done by third party

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, the Company may at their option, rely on customer due diligence done by a domestic 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) 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 PMLA;

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

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

3.6 Customer Due Diligence (CDD) Procedures

The Company will ensure compliance with the regulatory/ statutory requirements with respect to the Customer Identification Procedure to be carried out at different stages, i.e. while establishing a 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 etc.

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company will obtain sufficient information necessary to establish, identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship.

3.6.1 CDD Procedure in case of Individuals

3.6.1.1 Documents/ Information to be collected

From an individual (who is prospective customer OR a Beneficial Owner/ Authorised Signatory/ Power of Attorney Holder related to any legal entity) the following documents/ information will be obtained:

(a) Recent photograph;

(b) Certified copy of Permanent Account Number (PAN) OR the equivalent e-document thereof;

(c) Certified copy of one of the OVDs as defined above to be taken for verification of the identity and the address OR the equivalent e-document thereof; and

(d) Other documents including in respect of the nature of business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company.

Note:

- If PAN is not availed then Form No. 97 - may be taken;
- Aadhaar Offline Verification - The Company, being a non-bank, may carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purpose. However, where a customer submits his Aadhaar number, the Company will ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under the Aadhaar Act.
- Authentication using e-KYC authentication facility provided by the UIDAI - As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI, it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the PMLA/ the Aadhaar Act/ the KYC & AML Guidelines.
- Aadhaar number is not mandatory for purposes of KYC - In case the customer 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), the customer shall provide the Aadhaar number to the Company. However, in other cases, customers may provide the Aadhaar number voluntarily.
- If the customer provides an equivalent e-document of any OVD, the Company should 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 Digital KYC Process defined below (at sub-para 3.6.1.3).

  The Company may also carry-out KYC verification under Digital KYC Process defined below (at sub-para 3.6.1.3).
- The KYC Identifier with an explicit consent to download records from CKYCR shall be considered as sufficient for CDD for individuals.

3.6.1.2 Video based Customer Identification Process ("V-CIP")

The Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account-based relationship with an individual customer, after obtaining his informed consent. The Company, if implements V-CIP, will adhere to the extant applicable requirements.

3.6.1.3 Digital KYC Process

In case Digital KYC Process is adopted by the Company, it will ensure compliance with the following requirements:

(a) It will use an Application to 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 Company.

(b) The access of such Application should be controlled by the authorized persons of the Company. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism defined by the Company.

(c) The customer, for the purpose of KYC, shall visit the location of the Authorized Official of the Company **("Authorized Official")** vice-versa. The original OVD should be in possession of the customer.

(d) It should be ensured that the Live photograph of the customer is taken by the Authorized Official and the same photograph is embedded in the Customer Application Form (CAF). Further, a water-mark in readable form having CAF number, GPS coordinates, Authorized Official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) should be put on the captured live photograph of the customer.

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

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

(g) The live photograph of the customer and his original documents shall be captured in proper light so that they are clear.

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

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

(j) The Authorized Official should provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his official mobile number. Upon successful OTP validation, it shall be treated as the Authorized Official'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 should give information about the completion of the process and submission of activation request to activation officer of the Company and also generate the transaction-id/reference-id number of the process. The Authorized Official shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

(l) The Authorized Official should check and verify that: (i) information available in the picture of document is matching with the information entered by the Authorized Official in CAF. (ii) live photograph of the customer matches with the photo available in the document. and (iii) all of the necessary details in CAF including mandatory field are filled properly. However, the Company shall ensure that the liveness check does not result in exclusion of person with special needs.

(m) On successful verification, the CAF shall be digitally signed by the Authorized Official 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.

3.6.1.4 Simplified procedure for opening accounts of Individuals

In case a person who desires to open an account is not able to produce any of the OVDs, the Company may at its discretion open accounts subject to the following conditions:

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

(b) The authorized officer of the Company should certify 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 12 months, within which CDD as prescribed above should be carried out.

(d) Balances in all their accounts taken together shall not exceed Rs. 50,000/- at any point of time.

(e) The total credit in all the accounts taken together shall not exceed Rs. 1,00,000/- 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) When the balance reaches Rs. 40,000/- or the total credit in a year reaches Rs. 80,000/- , the customer shall be notified 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.

(h) 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 as per para 3.6.1.1 to 3.6.1.3 above.

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

3.6.2 On-boarding the Borrowers through Central KYC Registry

Company shall endeavor to provide option to the applicants to be on-boarded through verifying their antecedents through Central KYC Registry.

3.6.3 CDD Measures for Legal Entities

For due diligence with respect to legal entities, the Company will obtain the documents listed in ***Annexure 1***.

3.6.4 Identification of Beneficial Owner

For opening an account of an entity who is not a natural person, the beneficial owner(s) (as defined above) shall be identified and all reasonable steps to verify his/her identity shall be undertaken. While doing so, the Company will keep the following in view:

(a) Where 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, where it is determined that the customer is acting on behalf of another person as trustee/ nominee or so, identity of the intermediaries and of the persons on whose behalf he is acting, as also details of the nature of the trust or other arrangements in place will be obtained.

3.7 Enhanced Due Diligence (EDD) Procedures

3.7.1 Accounts of non-face-to-face customers:

Non-face-to-face onboarding is where the Company establishes relationship with the customer without meeting the customer physically or through V-CIP or by use of digital channels such as CKYCR, DigiLocker, 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.

The Company shall ensure following EDD measures are undertaken for all non-face-to-face customers onboarded except for customers onboarded using Aadhaar OTP based e-KYC:

(a) Whenever the Company introduces the process of V-CIP, the same shall be provided as first option to the customer for remote onboarding and the 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 KYC Directions.

(b) 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 at the time of login.

(c) Company shall develop and implement robust process of due diligence for dealing with requests for change of registered mobile number.

(d) 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.

(e) Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

(f) Transaction with customers shall be from existing KYC-complied bank account of the customer.

(g) Such non-face-to-face 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.

3.7.2 Accounts of Politically Exposed Persons (PEPs): If the Company decides to establish a business relationship with PEPs (whether as customer or beneficial owner), it will ensure the following:

(a) appropriate risk management system is in place to determine whether the customer or the beneficial owner is a PEP

(b) sufficient information including information about the sources of funds of PEPs is gathered;

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

(d) the decision to open an account for a PEP is taken at a senior management level in accordance with the Company's procedures;

(e) all such accounts will be classified as High Risk and will be subjected to required due diligence and monitoring, as applicable;

(f) if it gets confirmed to the Company that an existing customer or the beneficial owner of an existing account has subsequently become a PEP, an approval from a senior management of the Company will be obtained to continue the business relationship;

Further, such existing accounts which get classified PEPs subsequently will be subjected to enhanced due diligence, as applicable.

The above will also be applicable to accounts where a PEP is the beneficial owner or the family members or close associates of PEPs.

3.8 Monitoring of Transactions/ On-Going Due Diligence

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. The Company will put in place a process to identify and review complex and unusual transactions/ patterns which have no apparent economic or visible lawful purpose, or transactions that involve large amounts of cash or are inconsistent with the normal and expected activity of the customer.

3.9 Appointment of the Designated Director and the Principal Officer

(a) **Designated Director -** The Company has nominated a "Designated Director" to ensure compliance with the obligations prescribed by the PMLA and the Rules thereunder.

(b) **Principal Officer -** The Company has designated one of its senior officials as the 'Principal Officer' who will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

The name, designation, address and contact details of Designated Director and Principal Officer shall be communicated to FIU-IND and RBI and shall also be informed in case of any change.

3.10 Reporting to the Financial Intelligence Unit-India (FIU-IND)

The Company will report information of transaction referred to in clause (a) of sub-section (1) of section 12 of PMLA read with Rule 3 of the PML Rules relating to cash and suspicious transactions, etc., to the Director, Financial Intelligence Unit-India (FIU-IND). The Principal officer shall furnish information, where the principal officer of the Company has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of this section, in respect of such transactions to the Director of FIU-IND within the prescribed time.

The formats for reporting the requisite information in respect of cash transactions and suspicious transactions as provided by FIU-IND shall be followed as prescribed from time to time.

For determining integrally connected cash transactions, the Company shall take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rs. 10 lakh during the month.

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

The Company will pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. These records are required to be preserved for five years as is required under PMLA, 2002. Such records and related documents shall be made available to help auditors in their work relating to scrutiny of transactions and also to RBI/other relevant authorities.

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

The Company shall make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall ensure that there is no tipping off to the customer at any level.

In accordance with the requirements under the PMLA, the Company will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND):

(a) **Cash Transaction Report (CTR) -** If any such transactions are detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.

(b) **Counterfeit Currency Report (CCR) -** All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.

(c) **Suspicious Transactions Reporting (STR) -** The Company will monitor transactions to identify potentially suspicious activity. Such triggers will be investigated, and any suspicious activity will be reported to FIU-IND. The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed. The Company shall also consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer

The Company, its directors, officers, and all employees will maintain confidentiality in investigating suspicious activities and while reporting CTR/ CCR/ STR to the FIU-IND/ higher authorities. However, the Company may share information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local govt. authorities etc.

3.11 Record Management

(a) **Record-keeping requirements-** The Company shall ensure maintenance of proper record of transactions required under PMLA read with rules as mentioned below:

(i) 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;

(ii) preserve the records pertaining to the identification of the customers and their addresses obtained while sanction of loan / credit facility and during the course of business relationship, for at least five years after the business relationship is ended;

(iii) make available the identification records and transaction data to the competent authorities upon request;

(iv) 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);

(v) all cash transactions of the value of more than Rs. 10 lakh or its equivalent in foreign currency;

(vi) all series of cash transactions integrally connected to each other which have been individually valued below Rs. 10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs. 10 lakh or its equivalent in foreign currency;

(vii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions;

(viii) all suspicious transactions whether or not made in cash;

(ix) records pertaining to identification of the customer and his/her address; and

(x) 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.

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

(b) **The records should contain the following information:**

(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.

(c) **Maintenance and Preservation of records -** The Company will:

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

(ii) 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.

(iii) maintain and preserve the following records for the required time-period as prescribed under the PMLA, either in hard or soft format:

- all necessary records of transactions referred above; which will permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity;
- records pertaining to the identification of the customer and his address obtained while opening the account and during the course of business relationship.

(iv) make available the identification records and transaction data to the competent authorities upon request.

(v) 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).

3.12 Selling Third Party Products

The Company, if acting as agent while selling third party products as per regulations in force from time to time, will comply with the following aspects:

(a) The identity and address of the walk-in customer shall be verified for the transactions as required under the CIP prescribed above;

(b) Transaction details of sale of third-party products and related records shall be maintained.

(c) Monitoring of transactions for any suspicious activity will be done.

3.13 Quoting of Pan

As applicable, Permanent Account Number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B, as amended from time to time. Form 97 (previously Form 60) shall be obtained from persons who do not have PAN.

3.14 Introduction Of New Technologies

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

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures.

(c) to undertake Transaction Monitoring through in-house/third-party software to track suspicious transactions.

3.15 Customer Education

Seeking certain KYC information from customers can sometimes lead to queries from the customer as to the motive and purpose of collecting such information. In this regard, the Company will take appropriate steps to educate customers on the objectives of the KYC measures.

3.16 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) Company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally.

Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

(c) On-going employee training programme shall be put in place so that the members of staff are adequately trained in the KYC Policy. The focus of the training will be different for frontline staff, compliance staff and staff dealing with new customers.

(d) The front desk staff shall be specially trained to handle issues arising from lack of customer education.

(e) Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.

3.17 Adherence to the KYC and AML Guidelines by the Company's Agents

(a) The Company's agents or persons authorized by it, for its business, will be required to be compliant with the applicable KYC & AML Guidelines.

(b) All requisite information shall be made available to the RBI to verify the compliance with the applicable KYC & AML Guidelines.

(c) The books of accounts of persons authorized by the Company including agents etc., so far as they relate to business of the company, shall be made available for audit and inspection whenever required.

3.18 Sharing KYC Information with Central KYC Records Registry (CKYCR)

The Company will capture the KYC information/ details as the KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and KYC Directions. The Company shall also update information CKYC pursuant to updation/period updation of KYC records within timelines prescribed.

The Company shall carry out updation of KYC information of existing customer in case any update in CKYC of customer is informed by CKYCR.

The Company shall communicate the CKYCR number to the customer upon generation of the same.

In case Company downloads and relies on such records from the CKCYR, it shall not be required to re-verify the authenticity of the customer's identity and / or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005. However, the Company shall continue to remain responsible for all other aspects of CDD procedure and provisions under RBI KYC Directions.

3.19 Reporting Requirement Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

The Company, if applicable, will adhere to the provisions of Income Tax Rules 114F, 114G and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take requisite steps for complying with the reporting requirements in this regard.

3.20 Compliance with Section 51A of Unlawful Activities (Prevention) Act, 1967 ("UAPA ACT") and Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD ACT")

The company will ensure compliance with Section 51A of UAPA Act, 1987 and Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 by periodic screening the prospective and existing borrowers for UN Sanction List or any other list as per UAPA Act, 1987 and WMD Act, 2005.

In event, any account holder resembles the name of as per the list it will be reported to FIU-IND (including Central Nodal Officer), Ministry of Home Affairs, State Nodal Officer and RBI, as prescribed under KYC Directions.

Further, other requirements including freezing of assets shall be followed by company.

3.21 Secrecy Obligations and Sharing of Information

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

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(d) The exceptions to the said rule shall be as under:
- Where disclosure is under compulsion of law
- Where there is a duty to the public to disclose,
- the interest of RE requires disclosure and
- Where the disclosure is made with the express or implied consent of the customer.

(e) Company shall maintain confidentiality of information as provided in Section 45NB of RBI Act, 1934.

4. Approval and Review of the KYC and AML Policy

(a) There shall be an annual review of the Policy by the Board of Directors

(b) Board of Directors can at any time modify or amend, either the whole or any part of Policy

-X-

Annexure 1

List of Documents considered valid for verifying identity and proof of address of prospective customers

SN	Type of customer	Documents
1)	**Individual- Resident Indian** *(as a Customer/ Beneficial Owner/ Authorized Signatory/ Power of Attorney holder for another individual/ entity)*	(a) Recent photograph; (b) Certified copy of Permanent Account Number (PAN) OR the equivalent e-document thereof; (c) Certified copy of one of the OVDs to be taken for verification of the identity and the address OR the equivalent e-document thereof; and (d) Other document including in respect of the nature of business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company. **OVD** shall mean the following: (i) Proof of possession of Aadhaar number, in such form as issued by the Unique Identification Authority of India (UIDAI) (ii) Passport (iii) Driving License (iv) Voter's Identity Card issued by the Election Commission of India (v) Job Card issued by NREGA duly signed by an officer of the State Government (vi) Letter issued by the National Population Register containing details of name and address. **Provided that in case the OVD furnished by the customer does not contain updated address**, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: (i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (ii) property or Municipal tax receipt; (iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave & license agreements with such employers allotting official accommodation. Provided, the customer shall submit OVD with current address within a period of three months of submitting the alternate documents specified above. **Explanation:** For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued

		by the State Government or Gazette notification, indicating such a change of name.
2)	**Individual- Non-Resident Indian (NRI)/ Persons of Indian Origin (PIOs)**	(a) Recent photograph; (b) Certified copy of Permanent Account Number (PAN) OR the equivalent e-document thereof; (c) In case of Indian Passport Holder- Certified copy of Valid Indian Passport along with copy of valid Employment/ Residence/ Student/ Dependent visa copy or work/ Residence Permit copy; (d) In case of Foreign Passport holder Certified copy of valid Foreign Passport along with OCI (Overseas Citizen if India) card / PIO (Person of Indian Origin) card; (e) Certified copy of one of the OVDs to be taken for verification of the address OR the equivalent e-document thereof, if additionally required; (f) Valid KYC for the Power of Attorney holder as detailed in the previous para; and (g) Other document including in respect of the nature of business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company. Further**,** the original certified copy of OVD, certified by any one of the following, may be obtained: (i) Authorized officials of overseas branches of Scheduled Commercial Banks registered in India; (ii) Branches of overseas banks with whom the Company may have relationships; (iii) Notary Public abroad; (iv) Court Magistrate; (v) Judge; (vi) Indian Embassy/ Consulate General in the country where the non-resident customer resides. **Note:** Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.
3)	**Sole Proprietary firms**	In addition to OVD, PAN and photograph for the proprietor as an individual, <u>any two of the following documents</u> OR the equivalent e-document thereof, as a proof of business/ activity in the name of the proprietary firm shall also be obtained: (a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government; (b) Certificate/ License issued by the municipal authorities under Shop and Establishment Act; (c) GST and income tax returns; (d) CST/VAT/GST certificate, whenever applicable Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities / GST authorities;

		(e) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute; (f) License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute; (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax authorities; (h) Utility bills such as electricity, water, landline telephone bills etc. (not older than 2 months). **Note:** In cases where the Company is satisfied that it is not possible to furnish two such documents as mentioned above, it may accept only one of those documents as proof of business/ activity, subject to contact point verification and collection of such other information and clarification as would be required to establish the existence of such firm. Further, it should be satisfied that the business activity has been verified from the address of the proprietary concern.
4)	**Company**	In addition to OVD, PAN and photograph of the director/ manager/ employee (as an individual) holding authority to transact on the applicant company's behalf; certified copies of the following documents OR the equivalent e-document thereof: (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) the names of the relevant persons holding senior management position; and (f) the registered office and the principal place of its business, if it is different.
5)	**Partnership Firm**	In addition to OVD, PAN and photograph of the partner/ manager/ employee (as an individual) holding authority to transact on the applicant firm's behalf; certified copies of the following documents OR the equivalent e-document thereof: (a) Document evidencing authority of the person to act on behalf of the entity; (b) Registration Certificate, if registered; (c) Partnership Deed; (d) Permanent Account Number of the partnership firm; (e) the names of all the partners; and (f) address of the registered office, and the principal place of its business, if it is different.

6)	**Trust**	In addition to OVD, PAN and photograph of the trustee/ beneficiary/ person (as an individual) holding an attorney to transact on the trust's behalf; certified copies of the following documents OR the equivalent e-document thereof: (a) Document evidencing authority of the person to act on behalf of the Trust; (b) Registration Certificate, if registered; (c) Trust Deed; (d) Permanent Account Number or Form No.97 of the trust. (e) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust; (f) the address of the registered office of the trust; and (g) list of trustees and documents, as specified in Paragraph 23, for those discharging the role as trustee and authorised to transact on behalf of the trust. **Note:** In case of non-profit organisations, the details as registered on the DARPAN Portal of NITI Aayog.
7)	**Unincorporated Association or a Body of Individuals**	In addition to OVD, PAN and photograph of the person (as an individual) holding an attorney to transact on the entity's behalf; certified copies of the following documents OR the equivalent e-document thereof: (a) Resolution of the managing body of such association or body of individuals; (b) Power of attorney granted to him to transact on its behalf; (c) Permanent Account Number or Form No. 97 of the unincorporated association or a body of individuals; and (d) Such information as may be required by the Company to collectively establish the legal existence of such an association or body of individuals.
8)	**Other entities not specifically covered above, such as societies, universities and local bodies like village panchayats**	In addition to OVD, PAN and photograph of the person (as an individual) holding an attorney to transact on the entity's behalf; certified copies of the following documents OR the equivalent e-document thereof: (a) Document evidencing authority of the person to act on behalf of the entity; and (b) Such documents as may be required by the Company to establish the legal existence of such an entity/ juridical person.

---XXX---